01 용어 정리

용어 정리

ClusterXL은 게이트웨이 여러 대를 묶어 한 대가 죽어도 서비스가 끊기지 않게 하는 기술입니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

클러스터의 기본 개념

ClusterXL 은 동일한 게이트웨이 여러 대를 묶는 소프트웨어 기반 클러스터 솔루션입니다. 묶인 한 대 한 대가 **Cluster Member(클러스터 멤버)** 이고, 그 묶음 전체가 **Security Cluster** 입니다.

클러스터의 두 가지 목적이 곧 두 가지 모드입니다. **High Availability(HA, 고가용성)** 는 한 멤버만 Active이고 장애 시 백업으로 투명하게 페일오버 하며, **Load Sharing(부하 분산)** 은 모든 멤버가 Active로 트래픽을 나눠 처리해 성능까지 높입니다(HA·Load Sharing 모드).

장애가 나서 다른 멤버가 역할을 넘겨받는 것이 **Failover(페일오버)** 입니다.

IP·MAC 주소 구조

클러스터의 주소 체계가 핵심입니다. **Virtual IP(VIP, 가상 IP)** 는 클러스터 자체의 주소 로 물리 인터페이스에 속하지 않고, 각 멤버는 자기만의 고유 물리 IP·MAC 을 따로 가집니다. 외부에서는 VIP 하나로 접속하고, 내부에서 어느 멤버가 처리할지가 갈립니다. 페일오버가 일어나면 새 Active 멤버가 **Gratuitous ARP(GARP)** 를 뿌려 VIP를 자기 MAC에 다시 연결 합니다. 전환을 더 빠르게 하려고 모든 멤버가 같은 **VMAC(Virtual MAC)** 을 VIP에 연결 하는 모드도 있습니다(요구사항·호환성).

멤버를 잇는 통신과 동기화

멤버들을 하나로 묶는 접착제가 **CCP(Cluster Control Protocol)** 입니다. 멤버 사이에서 UDP 8116 포트로 동작 하며, 서로 살아 있음을 알리는 keep-alive와 상태 동기화 를 나릅니다 (정책에 CCP 허용 규칙을 따로 넣을 필요 없음).

연결을 잃지 않는 비결이 **State Synchronization(상태 동기화)** 입니다. 각 멤버가 다른 멤버를 지나는 연결을 알게 해 페일오버 때도 데이터를 잃지 않습니다. 처음 합류할 때 모든 커널 테이블을 옮기는 **Full Sync**, 이후 변경분만 옮기는 **Delta Sync** 로 나뉩니다 (연결 동기화).

멤버 상태를 판정하는 것이 **Critical Device(중요 장치)** 입니다. 하나라도 "problem"을 보고하면 페일오버 가 일어납니다(모니터링·문제 해결).

멤버의 상태와 역할

멤버는 상황에 따라 상태가 바뀝니다 — **Active**(트래픽 처리), **Standby**(HA에서 대기), **Down**(문제 발생) 이 기본이고, 모든 멤버가 문제일 때 하나만 골라 살리는 **Active(!)** 상태도 있습니다. HA에서는 멤버마다 우선순위(priority) 가 있어 가장 높은 멤버가 Active가 되며, Load Sharing Unicast 모드에서는 패킷을 받아 분배하는 단일 멤버인 **Pivot** 이 있습니다.

02 ClusterXL 소개

ClusterXL 소개

게이트웨이는 조직과 바깥 세상 사이를 잇는 길목 이라, 한 대가 죽으면 활성 연결과 중요 데이터 접근이 한꺼번에 끊깁니다. **ClusterXL** 은 게이트웨이를 여러 대 묶어 그 길목이 어떤 상황에서도 열려 있게 하는 솔루션입니다.

ClusterXL이 하는 일

ClusterXL은 동일한 게이트웨이 여러 대를 묶는 소프트웨어 클러스터 입니다. 두 가지 방식으로 안정성을 줍니다 — **High Availability(고가용성)** 는 한 대가 죽으면 백업으로 투명하게 페일오버 해 연결·VPN을 지키고, **Load Sharing(부하 분산)** 은 모든 멤버가 Active로 트래픽을 나눠 처리해 성능 까지 끌어올립니다(HA·Load Sharing 모드).

!ClusterXL 구성 *① 내부 네트워크 ② 내부망 스위치 ③ ClusterXL을 켠 Security Gateway들 ④ 외부망 스위치 ⑤ 인터넷*

어떻게 동작하나

핵심 비결은 **State Synchronization(상태 동기화)** 입니다. 각 멤버가 다른 멤버를 지나는 연결을 모두 "알고" 있어, 한 멤버가 죽어도 그 연결을 다른 멤버가 끊김 없이 이어받습니다 (연결 동기화).

주소 구조도 한몫합니다. 클러스터 자체는 **Virtual IP**(VIP)를 쓰고, 각 멤버는 고유한 물리 IP·MAC 을 가집니다. VIP는 물리 인터페이스에 속하지 않는 가상 주소라, 외부에서는 VIP 하나만 보면 됩니다.

> 참 고
>
> 이 가이드는 Security Gateway 클러스터 를 다룹니다. VSX와 함께 쓰는 ClusterXL은 R82 VSX 관리자 가이드를 참고하세요.

멤버를 잇는 접착제 — CCP

멤버들을 하나로 묶는 것이 **CCP(Cluster Control Protocol)** 입니다. 일반 트래픽과 구별되는 별도 트래픽으로, 멤버 사이에서 UDP 8116 포트로 동작 합니다. CCP는 두 가지 일을 합니다 — 멤버들이 keep-alive 패킷으로 서로의 상태를 알리고 배우는 일, 그리고 상태 동기화(Delta Sync) 입니다. 모든 ClusterXL 모드가 CCP를 씁니다.

> 중 요
>
> CCP 패킷을 허용하는 규칙을 정책에 따로 넣을 필요가 없 습니다.

CCP 설정은 ClusterXL 구성 명령에서 다룹니다.

03 요구사항·호환성

요구사항·호환성

ClusterXL을 세우기 전에 무엇이 똑같아야 하고 몇 대까지 묶을 수 있는지 를 알아야 합니다. 이 장은 멤버를 묶기 위한 전제 조건과 동기화 네트워크 토폴로지를 정리합니다.

설치 형태와 멤버 수

ClusterXL은 **Distributed**(멤버와 관리 서버를 다른 컴퓨터에) 또는 **Full High Availability**(멤버와 관리 서버를 같은 컴퓨터에, 각자 Standalone) 로 설치합니다(Open Server는 Distributed만 가능).

멤버 수는 모드별로 다릅니다 — HA·Load Sharing 모드는 최대 5대(단 4대 초과 시 Delta Sync 부담으로 성능 저하), Gaia VRRP 클러스터는 2대, VSLS(Virtual System Load Sharing)는 최대 13대 입니다.

"똑같아야 한다" — 하드웨어·소프트웨어 요구사항

ClusterXL의 핵심 전제는 멤버들이 동일해야 한다 는 것입니다. ClusterXL은 하드웨어 클록 틱 기반의 내부 타이머에 의존 하므로 CPU 특성이 같은 장비끼리만 지원됩니다. 또 CCP 문제로 인한 예기치 않은 페일오버를 막기 위해 동일한 물리 인터페이스끼리 짝지을 것 이 강력히 권장됩니다.

소프트웨어도 마찬가지입니다 — 운영체제·Check Point 버전(OS 빌드·핫픽스 포함)이 동일해야 하고, 켜진 Software Blade·기능, SecureXL 상태, CoreXL Firewall 인스턴스 수, Advanced Dynamic Routing 설정이 모두 같아야 합니다. 다르면 트래픽 처리가 어긋나거나 상태가 예기치 않게 바뀌고 Full Sync가 실패합니다(예: CoreXL 인스턴스가 더 많은 멤버는 DOWN 상태가 됨).

VMAC 모드 — 페일오버를 매끄럽게

HA나 Load Sharing Unicast 모드에서는 단일 멤버(Active 또는 Pivot)가 VIP와 연결됩니다. 페일오버 후 새 Active가 GARP를 뿌려 VIP를 자기 MAC에 다시 연결하는데, Static NAT 항목이 많으면 GARP가 너무 많아 스위치가 ARP 테이블을 못 따라가 거나, VoIP 전화 같은 장비가 GARP를 무시 해 죽은 멤버로 계속 트래픽을 보내는 일이 생깁니다.

이를 막는 것이 **VMAC(Virtual MAC)** 입니다. 모든 멤버가 같은 Virtual MAC을 VIP에 연결하면, 페일오버 때 MAC이 바뀌지 않으니 스위치·장비가 ARP를 갱신할 필요가 없 어 전환이 더 빠르고 매끄럽습니다(설정은 고급 기능 참고).

동기화 네트워크 토폴로지

동기화 네트워크는 여러 토폴로지로 구성할 수 있습니다. Sync 인터페이스를 여러 물리 인터페이스의 Bond로 묶 어, 같은 스위치에 연결하거나(Topology 1·2) Active-Backup Bond로 서로 다른 스위치에 연결(Topology 3·4, Enhanced Active/Backup) 합니다. Enhanced 방식에서는 멤버들이 링크 상태뿐 아니라 멤버 간 경로까지 감시해 어느 subordinate 인터페이스를 쓸지 합의 하고, 모든 subordinate가 다 죽어야 페일오버 합니다.

그 밖의 요구사항

몇 가지 더 챙길 점이 있습니다. 모든 멤버의 클록을 (수동 또는 NTP로) 동기화 해야 VPN 등이 제대로 동작합니다. IPv6는 HA 클러스터만 지원(Load Sharing은 미지원, Sync 인터페이스에는 IPv6 불가)하며, "Cluster"·"Sync"·"Cluster+Sync" 타입 인터페이스에는 IPv4 주소를 반드시 설정해야 합니다.

동기화에는 제약도 있습니다 — 동기화 중복용으로 전용 물리 인터페이스를 둘 이상 쓰는 건 미지원(대신 Bonding 사용), 한 멤버가 죽으면 그 멤버를 지나던 user-authenticated 연결은 복구 불가(user space 프로세스가 인증 상태를 보관하기 때문), 페일오버 시 관리 서버로 아직 안 보낸 어카운팅 정보는 유실 됩니다.

04 HA·Load Sharing 모드

HA·Load Sharing 모드

ClusterXL의 핵심은 어떤 모드로 묶느냐 입니다. 이 장은 High Availability와 Load Sharing의 동작 원리, 예제 토폴로지, 모드 비교, 그리고 페일오버를 정리합니다.

High Availability — 한 대만 Active

High Availability 클러스터에서는 한 멤버만 Active이고 나머지는 Standby 입니다 (Active/Standby). 멤버마다 우선순위가 있어 가장 높은 멤버가 평소 게이트웨이 역할 을 하고, 그 멤버가 죽으면 다음 우선순위 멤버로 제어가 넘어갑니다. State Synchronization을 켜면 Standby가 Active의 연결 상태를 늘 갱신받아, 페일오버 때도 연결이 끊기지 않 습니다.

동작 원리는 이렇습니다. 클러스터가 VIP를 Active 멤버의 물리 인터페이스 MAC에 연결 하므로, VIP로 오는 모든 트래픽이 실제로는 Active 멤버로 라우팅·필터링 됩니다. Active는 방화벽 역할에 더해 자기 상태·커널 테이블 변화를 Standby들에게 알려 줍니다. 페일오버가 나면 다음 우선순위 Standby가 Active가 되어 GARP를 뿌려 VIP를 자기 MAC에 다시 연결 합니다.

복구 후 동작은 설정에 달렸습니다 — **Maintain current active**(복구된 멤버는 Standby로 남음) 또는 **Switch to higher priority**(우선순위 높은 멤버가 다시 Active) 입니다. HA 모드는 IPv4·IPv6를 모두 지원합니다.

!두 멤버 ClusterXL 예제 토폴로지 *① 내부 네트워크 ② 내부 스위치(내부 클러스터 IP 10.10.0.100) ③ Cluster Member A(내부 가상 10.10.0.1 · Sync 10.0.10.1 · 외부 가상 192.168.10.1) ④ Cluster Member B(내부 가상 10.10.0.2 · Sync 10.0.10.2 · 외부 가상 192.168.10.2) ⑤ 외부 스위치(외부 클러스터 IP 192.168.10.100) ⑥ 인터넷*

위 예제처럼 각 멤버는 외부·내부·동기화 세 인터페이스 를 갖고, 같은 방향 인터페이스는 모두 같은 네트워크 에 있어야 합니다(멤버 사이에 라우터가 있으면 안 됨). 클러스터는 외부·내부 각각 하나의 VIP 를 가지며, 인터넷을 향한 가상 인터페이스에만 공인 IP가 필요 하고 멤버들의 물리 IP는 사설이어도 됩니다(공인 IP 절약).

Load Sharing — 모두 Active

Load Sharing 은 모든 멤버가 Active로 트래픽을 나눠 처리 해 총 처리량을 높입니다(Active/Active). 클러스터의 **결정 함수(decision function)** 가 각 패킷을 어느 멤버가 처리할지 정해, 적어도 한 멤버는 처리하되(차단 방지) 두 멤버가 같은 패킷을 처리하지 않게(중복 방지) 합니다. 한 멤버가 죽으면 그 멤버가 처리하던 연결을 나머지가 즉시 넘겨받 으므로 HA도 함께 제공하는 셈입니다.

받는 방식에 따라 두 가지로 나뉩니다. **Multicast 모드** 는 VIP를 멀티캐스트 MAC에 연결해 모든 멤버가 패킷을 받 고 각자 처리 여부를 결정합니다 — 부하 분산이 최적이지만 일부 스위치가 멀티캐스트 MAC의 ARP 응답을 받아들이지 못 합니다. **Unicast 모드** 는 단일 멤버인 **Pivot** 만 패킷을 받아 다른 멤버에 분배 합니다 — 멀티캐스트가 안 되는 환경에 맞고, Pivot은 분배 부담 때문에 보통 더 적은 몫을 맡습니다(non-Pivot 멤버도 받은 패킷을 처리하므로 여전히 Active). Load Sharing 모드는 State Synchronization이 필수 이고 IPv6를 지원하지 않 습니다.

> 권 장
>
> 기존 게이트웨이에 HA·Load Sharing을 도입할 때는, 가능하면 Active 게이트웨이의 기존 IP를 클러스터 VIP로 삼으세요. IPsec 엔드포인트 식별자나 Hide NAT 설정을 그대로 둘 수 있습니다.

모드 비교

어떤 모드를 고를지는 조직의 필요에 달렸습니다. HA는 안전한 연결성, Load Sharing은 안전한 연결성 + 성능 향상, Active-Active는 서로 다른 지역(네트워크)에 멤버 배치 가 필요할 때입니다(Active-Active 모드).

항목	High Availability	Load Sharing Multicast	Load Sharing Unicast	Active-Activ
고가용성	O	O	O	O
부하 분산	X	O	O	X
성능	Good	Excellent	Very Good	Good
State Sync	선택	필수	필수	선택
하드웨어 지원	모든 라우터	일부 스위치만	모든 라우터	모든 라우터
트래픽 처리 멤버 수	1	N	N	N

페일오버

Failover(페일오버) 는 멤버가 제대로 동작하지 못할 때 다른 멤버가 자동으로 넘겨받는 동작입니다. Critical Device가 "problem"을 보고하거나(예: fwd 프로세스 실패, 정책 미설치), 멤버가 동료의 CCP 패킷을 못 받으면 페일오버가 일어납니다. CCP는 멤버 간 heartbeat를 유지해, 정해진 시간 동안 CCP가 안 오면 그 멤버를 down으로 간주 합니다.

HA에서는 State Sync가 없으면 페일오버 시 기존 연결이 끊기 지만, Load Sharing에서는 모든 멤버가 늘 동기화되어 있어 연결이 끊기지 않 습니다. 모든 멤버가 문제일 때는(예: sync 크로스 케이블 고장) ClusterXL이 하나만 골라 Active(!) 상태로 살려 둡니다.

복구된 멤버는 먼저 동료 Active 멤버에서 정책을 가져오려 시도 하고(더 최신이라 가정), 실패하면 자기 정책과 관리 서버 정책을 비교해 최신을 가져옵니다 — 이렇게 모든 멤버가 늘 같은 정책 을 쓰게 합니다. 다만 Security Server 연결, 멤버 자신이 시작한 연결, CPAS/PSL TCP 연결 등 일부 연결은 페일오버를 못 넘길 수 있습니다.

05 Active-Active 모드·Geo Cluster

Active-Active 모드·Geo Cluster

앞 장의 HA·Load Sharing은 멤버들이 같은 네트워크에 있다 고 전제했습니다. 하지만 멤버를 서로 다른 지역·사이트·클라우드 가용 영역 에 두고 싶을 때가 있습니다. 이를 위한 것이 **Active-Active 모드** 와 **Geo Cluster** 입니다.

Active-Active 모드

Active-Active(R80.40 도입) 모드는 멤버들이 서로 다른 지리적 위치에 있고, 각 멤버의 인터페이스 IP가 서로 다른 네트워크(Sync 인터페이스 포함)에 있는 클러스터를 위한 것입니다. 각 멤버가 자기에게 라우팅된 트래픽을 검사하고, 기록한 연결을 동료에게 동기화 합니다.

여기서 꼭 짚을 점이 있습니다. Active-Active는 트래픽을 멤버 간에 분산하지 않 습니다(Load Sharing이 아님). 트래픽은 라우팅에 따라 각 멤버로 들어오는 대로 처리되며, 관리자가 각 멤버의 부하를 직접 모니터링 해야 합니다(모니터링·문제 해결).

구성 전제도 있습니다 — 관리 서버·ClusterXL 모두 R80.40 이상, CCP 암호화가 켜져 있어야 함(기본값), 필요하면 각 멤버에서 Dynamic Routing을 켜 라우터로 동작 시킬 수 있습니다(이때 동적 라우팅 인터페이스마다 BFD 활성화 필요).

한계도 분명합니다. 지원 블레이드는 Firewall·IPS·NAT(Hide/Static)·Application Control·URL Filtering·Content Awareness·Anti-Spam·Anti-Bot·Anti-Virus 로 한정, 최대 4대, VSX 미지원, 모든 Multi-Portal(Mobile Access·Identity Awareness Captive Portal·DLP Portal) 미지원 이며, 같은 "쪽"의 인터페이스 이름은 모든 멤버에서 같아야 합니다(예: 한 멤버에서 eth1을 Switch A에 연결했으면 다른 멤버도 eth1을 Switch A에).

Geo Cluster

Geo Cluster(R81.20 도입)는 클라우드 환경의 ClusterXL High Availability 모드입니다. 멤버들이 서로 다른 클라우드 가용 영역(availability zone)에 위치 한 클러스터를 위해 설계되었습니다.

동작은 HA와 같은 원리입니다 — 각 멤버가 자기에게 라우팅된 트래픽을 검사하고 연결을 동료에게 동기화 하며, 자기 상태와 동료 상태를 감시하다 장애가 나면 페일오버 합니다. 클라우드에서의 실제 배포는 CloudGuard Network for AWS Cross Availability Zone Cluster Deployment Guide 를 참고하세요.

정리하면, 같은 네트워크 안의 묶음이 HA·Load Sharing이라면, 지역·클라우드 영역을 가로지르는 묶음이 Active-Active와 Geo Cluster 입니다.

06 연결 동기화(State Synchronization)

연결 동기화(State Synchronization)

방화벽이 죽으면 오가던 활성 연결이 즉시 끊깁 니다. 금융 거래처럼 중요한 연결이라면 큰일이죠. ClusterXL은 각 멤버가 다른 멤버를 지나는 연결을 알게 해 장애 시에도 데이터를 잃지 않 게 합니다 — 이것이 **State Synchronization(상태 동기화)** 입니다.

게이트웨이가 인식하는 모든 IP 기반 서비스(TCP·UDP 포함)가 동기화 됩니다. Load Sharing 멤버는 반드시 동기화 되어야 하고, HA 멤버는 동기화가 필수는 아니지만, 안 하면 페일오버 때 연결이 끊깁 니다.

동기화 네트워크

Synchronization Network 는 연결·상태 정보를 멤버 사이에 주고받는 통로 입니다. 조직에서 가장 민감한 정보가 흐르므로 보호가 중요 합니다. 권장 방법은 세 가지입니다 — CCP 암호화 켜기(기본값), 전용 동기화 네트워크 쓰기, 멤버의 물리 인터페이스를 크로스 케이블로 직결(3대 이상이면 전용 허브·스위치).

> 참 고
>
> WAN을 가로질러 동기화할 수도 있고, VLAN 인터페이스에서는 가장 낮은 VLAN 태그 만 동기화에 쓸 수 있습니다(예: eth1에 태그 10·20·30이 있으면 eth1.10만 가능).

동기화의 두 가지 모드

State Synchronization은 두 모드 로 동작합니다.

Full Sync 는 한 멤버에서 다른 멤버로 모든 커널 테이블 정보를 옮깁 니다. 멤버가 클러스터에 새로 합류하거나 down 후 다시 올라올 때 처음 한 번 수행합니다. `cxld` 데몬이 동료의 TCP 263 포트 에 연결하며(실패하면 옛 방식인 `fwd` 데몬의 TCP 256으로 폴백), Full Sync가 끝나면 더 빠른 Delta Sync로 넘어갑니다.

Delta Sync 는 커널 테이블의 변경분만 옮깁 니다. 모든 멤버가 Full Sync를 마친 뒤 연결 상태 변화를 주고받 는 데 쓰이며, 게이트웨이 커널이 UDP 8116 포트 로 처리합니다. State Synchronization 트래픽은 전체 CCP 트래픽의 약 90% 를 차지하며, 멤버들은 UDP 헤더의 opcode로 동기화 패킷을 나머지 CCP와 구분합니다.

짧은 연결은 지연 동기화

모든 연결을 동기화할 필요는 없습니다. HTTP처럼 아주 짧게 끝나는 연결 은 동기화해 봐야 멤버 자원만 쓰고 페일오버 전에 이미 끝날 가능성이 높습니다. 그래서 **Delayed Notifications** 기능으로, 연결이 시작된 지 X초 뒤에도 살아 있을 때만 동기화 하도록 알림을 미룹니다(SecureXL이 모든 멤버에 켜져 있어야 함 — 기본값). 설정은 SmartConsole의 Object Explorer에서 해당 서비스 객체에 지정합니다.

정리하면, State Synchronization이 ClusterXL의 "끊김 없음"을 떠받치는 토대 이며, 처음엔 Full Sync로 전체를, 이후엔 Delta Sync로 변경분만, 짧은 연결은 지연 동기화로 효율을 챙깁니다.

07 ClusterXL 구성

ClusterXL 구성

이 장은 Load Sharing Multicast·Unicast·High Availability 모드를 처음부터 구성 하는 흐름을 다룹니다. 세 모드의 구성은 SmartConsole에서 모드를 고르는 것만 다르 고 나머지는 같습니다.

멤버 설치와 클라이언트 라우팅

먼저 요구사항·호환성을 충족하는지 확인하고 R82 Installation and Upgrade Guide에 따라 멤버를 설치합니다.

그다음 클라이언트 컴퓨터의 라우팅 을 잡습니다. 핵심은 각 네트워크의 컴퓨터가 그쪽 클러스터 VIP를 Default Gateway로 쓰는 것입니다. 예를 들어 내부망(10.10.2.0/24) 컴퓨터는 Default Gateway를 VIP `10.10.2.100` 으로, 외부망(192.168.2.0/24) 컴퓨터는 VIP `192.168.2.100` 으로 설정합니다(Proxy ARP는 sk30197 참고).

CCP 설정

멤버들을 잇는 **CCP(Cluster Control Protocol)** 는 멤버들이 자동으로 모드를 구성 합니다 (R82에서 CCP는 항상 unicast 모드).

> 중 요
>
> 클러스터에서는 모든 멤버를 똑같이 설정 해야 합니다.

보안을 위해 CCP 암호화 를 켤 수 있습니다. Gaia Clish의 `set cluster member ccpenc {off|on}` 또는 Expert 모드의 `cphaconf ccp_encrypt {off|on}` 으로 설정합니다.

```
set cluster member ccpenc on          # Gaia Clish
cphaconf ccp_encrypt on               # Expert mode
```

클러스터 객체와 멤버 정의

실제 클러스터는 SmartConsole에서 클러스터 객체와 그 멤버를 정의 해 만듭니다. **Wizard Mode**(마법사)와 **Classic Mode**(상세 구성) 중에 고를 수 있으며, 이 단계에서 모드(HA / Load Sharing Multicast / Load Sharing Unicast)를 선택 합니다.

구성의 큰 줄기는 HA·Load Sharing 모드에서 본 주소 체계 그대로입니다 — 각 멤버에 외부·내부·동기화 인터페이스를 주고, 클러스터에 외부·내부 VIP를 정의 한 뒤, 멤버 우선순위를 정하고 정책을 클러스터 객체에 설치하면 모든 멤버에 자동으로 설치됩니다.
VMAC·VPN·NAT·VLAN·Bond 같은 세부 구성은 고급 기능·절차에서 다룹니다.

08 고급 기능·절차

고급 기능·절차

기본 클러스터를 세운 뒤 더 정교하게 다듬는 기능들을 모은 장입니다. 원문 분량이 가장 크니, 여기서는 각 기능이 무엇을 위한 것인지 를 잡고 세부 절차는 원문 해당 절을 참고하세요.

주소·인터페이스 다루기

VMAC(Virtual MAC) 구성 은 페일오버를 매끄럽게 합니다(요구사항·호환성) — 모든 멤버가 같은 Virtual MAC을 VIP에 연결해, 페일오버 때 스위치·장비가 ARP를 갱신할 필요가 없게 합니다.

Bond 인터페이스 로 여러 물리 인터페이스를 묶어 대역폭·이중화 를 얻고, 특히 Sync 중복(Sync Redundancy) 을 Bonding으로 구현합니다. **VLAN** 을 클러스터에서 쓰고, **Cluster IP Addresses on Different Subnets** 로 클러스터 VIP와 멤버 IP를 다른 서브넷에 둘 수 있습니다(공인 IP 절약, 기존 네트워크에 클러스터를 끼워 넣을 때 유용).

Link Monitoring 으로 클러스터 인터페이스의 링크 상태를 감시 하고, **Non-Monitored Interfaces** 로 감시에서 제외할 인터페이스 를 정합니다. Load Sharing Unicast에서는 **Assigned Load** 로 Pivot이 맡을 부하 비중 을 조정합니다.

VPN·NAT·라우팅 연동

Working with VPN in Cluster 는 클러스터에서 VPN을 쓸 때의 고려사항 을, **Working with NAT in Cluster** 는 NAT 동작 을 다룹니다. **ISP Redundancy on a Cluster** 로 여러 ISP 회선 이중화 를(Security Gateway 가이드의 ISP 이중화 참고), **Dynamic Routing Protocols in a Cluster** 로 OSPF·BGP 같은 동적 라우팅 을 클러스터에서 구성합니다.

멤버 추가·제거와 무중단 운영

운영 중에 기존 클러스터에 멤버를 추가(Adding Another Member)하거나 제거(Removing a Member) 할 수 있습니다. 이때 핵심은 요구사항·호환성에서 본 모든 멤버가 동일해야 한다는 원칙입니다.

세밀한 동작을 조정하는 항목도 있습니다 — **Policy Update Timeout**(정책 갱신 시간), **Enhanced 3-Way TCP Handshake Enforcement**(3-way 핸드셰이크 강제), **Minimum Number of Required Subordinate Interfaces**(Bond의 최소 활성 인터페이스 수) 등입니다.

특히 무중단 업그레이드를 위한 **Multi-Version Cluster(MVC)** 메커니즘이 있어, 서로 다른 버전의 멤버가 잠시 한 클러스터에 공존 하며 순차로 올라갈 수 있습니다(Maestro 가이드의 업그레이드에서 본 MVC와 같은 개념). 이 명령들의 구체적 사용법은 ClusterXL 구성 명령에서 다룹니다.

09 ClusterXL 구성 명령

ClusterXL 구성 명령

이 장은 클러스터 동작을 세밀하게 조정하는 명령들 을 정리합니다. 대부분 CLI에서 실행하며, 클러스터에서는 모든 멤버를 똑같이 설정 하는 것이 원칙입니다.

Critical Device 관리

ClusterXL이 멤버 상태를 판정하는 핵심이 **Critical Device(중요 장치)** 입니다 — 하나라도 "problem"을 보고하면 페일오버 가 일어납니다(모니터링·문제 해결). 명령으로 Critical Device를 등록(Register)·해제(Unregister)하고, 상태를 보고(Report) 할 수 있으며, 파일에 나열된 장치를 한꺼번에 등록 하거나 전체를 해제 할 수도 있습니다. 이를 활용해 사용자 정의 모니터링을 클러스터 판정에 끼워 넣습니다.

CCP·페일오버·Bond 조정

ClusterXL 구성에서 본 **CCP 설정**(암호화 등)도 여기에 속합니다. **수동 페일오버(Initiating Manual Cluster Failover)** 로 원하는 시점에 강제로 페일오버 를 일으키고, **Bond Load Sharing의 최소 subordinate 인터페이스 수** 를 정해 몇 개가 살아 있어야 Bond를 유지할지 조정합니다.

무중단 업그레이드의 핵심인 **Multi-Version Cluster(MVC) 메커니즘** 도 명령으로 구성합니다 — 서로 다른 버전의 멤버가 잠시 공존 하며 순차로 올라가게 합니다(고급 기능).

또 로그에서 멤버를 ID로 표시할지 이름으로 표시할지(Cluster Member ID Mode in Local Logs) 도 설정합니다.

> 주 의
>
> 이 명령들 중 일부는 게이트웨이나 Check Point 지원팀이 자동으로만 실행해야 하는 내부 동작 명령입니다. 직접 실행은 권장되지 않으니, 명령의 정확한 구문·옵션은 CLI·스크립트·API 참조가 가리키는 R82 CLI Reference Guide와 함께 신중히 다루세요.

10 모니터링·문제 해결

모니터링·문제 해결

클러스터를 운영하면서 멤버 상태를 들여다보고, 문제가 생기면 원인을 찾는 방법을 다룹니다. 명령줄 도구, SmartConsole, SNMP, 그리고 흔한 문제의 진단이 핵심입니다.

상태 모니터링

ClusterXL은 상태를 보는 명령들 을 제공합니다. 대표가 `cphaprob` 계열로, 멤버의 상태(Active/Standby/Down), Critical Device 목록, 인터페이스 상태, CCP 설정 등을 봅니다. 멤버 상태는 **Active**(트래픽 처리), **Standby**(HA 대기), **Down**(문제), **Active(!)**(모든 멤버 문제 시 하나만 살린 상태) 로 나타납니다.

SmartConsole에서도 클러스터 상태를 한눈에 볼 수 있고, **SNMP Trap** 으로 상태 변화를 외부 모니터링 시스템에 알릴 수 있습니다.

Critical Device — 페일오버의 방아쇠

문제 해결의 중심은 **Critical Device(중요 장치)** 입니다. 멤버가 정상 동작하는 데 필수인 요소들 로, 하나라도 "problem"을 보고하면 페일오버 가 일어납니다(ClusterXL 구성 명령). 예를 들어 `fwd` 프로세스 실패, 정책 미설치, 인터페이스 링크 다운 등이 Critical Device 문제로 잡힙니다.

페일오버 일으키기와 문제 진단

테스트나 유지보수를 위해 수동으로 페일오버를 일으킬 수 있습니다(ClusterXL 스크립트의 `clusterXL_admin` 참고).

흔한 문제로 **Critical Device** `routed` 가 있습니다 — 동적 라우팅 데몬(routed)이 Critical Device로 등록되어 문제를 보고 하면 페일오버가 일어나니, 동적 라우팅 환경에서 예기치 않은 페일오버가 잦다면 여기를 살핍니다. 이 밖에 **ClusterXL Error Messages**(오류 메시지) 를 해석해 원인을 좁혀 갑니다.

특히 요구사항·호환성에서 강조한 멤버 간 불일치(CoreXL 인스턴스 수·버전·블레이드 차이) 가 예기치 않은 상태 변화나 Full Sync 실패의 흔한 원인이므로, 문제가 생기면 멤버들이 정말 동일한지 부터 확인하는 것이 좋습니다. 자세한 명령·오류 코드는 CLI·스크립트·API 참조가 가리키는 R82 CLI Reference Guide를 참고하세요.

11 CLI·스크립트·API 참조

CLI·스크립트·API 참조

ClusterXL을 명령줄·스크립트·API로 다루는 방법을 한데 모았습니다. 방대한 명령 사전은 전용 참조 문서로 넘기고, 여기서는 무엇이 있고 어디서 찾는지 를 짚습니다.

명령줄 참조

ClusterXL 운영 명령 전체는 **R82 CLI Reference Guide** 에 정리되어 있습니다. 앞 장들에서 본 상태 확인용 `cphaprob` (모니터링·문제 해결), 구성용 `cphaconf` · `set cluster member` (ClusterXL 구성) 같은 명령이 거기에서 자세히 다뤄집니다.

> 주 의
>
> ClusterXL 내부 동작을 바꾸는 일부 구성 명령은 게이트웨이나 Check Point 지원팀이 자동으로만 실행해야 합니다. 직접 실행은 권장되지 않습니다.

ClusterXL 스크립트

멤버의 상태를 바꾸는 특수 스크립트 가 있습니다. 대표가 `clusterXL_admin` 으로, 멤버에서 수동 페일오버를 일으킬 때 씁니다(위치: `$FWDIR/bin/clusterXL_admin`). 테스트나 유지보수 때 원하는 멤버를 의도적으로 down/up 시키는 데 유용합니다.

Cluster 관리 API

Cluster API 는 `simple-gateway` API처럼 클러스터를 자동화·오케스트레이션 하기 위한 것입니다. 새 클러스터 객체 생성, 기존 객체 수정(멤버 추가·제거, 인터페이스 조작) 같은 일반적인 작업을 지원합니다.

이 API들이 "simple"이라 불리는 이유는 클러스터 객체의 모든 기능을 다 지원하지는 않 기 때문입니다. 따라서 API가 제공하지 않는 작업은 SmartConsole 에서 하면 됩니다. 자동화로 클러스터를 대량 생성·변경 할 때 이 API가 큰 힘이 되며, 자세한 명령은 Check Point Management API Reference를 참고하세요.

정리하면, 일상 운영은 SmartConsole로 하되 상태 진단은 `cphaprob` , 수동 페일오버는 `clusterXL_admin` , 대량 자동화는 Cluster API 로 내려가며, 그 방대한 명령 사전은 CLI Reference Guide와 Management API Reference 가 담당합니다.