01 용어 정리

용어 정리

Gaia 는 Check Point의 모든 게이트웨이·관리 서버가 그 위에서 돌아가는 보안 운영체제 입니다. 그리스 신화에서 Gaia가 만물의 어머니이듯, 이 OS는 여러 부품을 하나의 효율적인 시스템으로 통합합니다. 원문 글로서리에는 일반 Check Point 용어가 많지만, 여기서는 이 가이드를 읽는 데 바탕이 되는 Gaia 관련 핵심 용어 만 흐름에 따라 추려 둡니다.

Gaia를 다루는 세 가지 창구

Gaia를 운영하는 방법은 셋입니다. **Gaia Portal** 은 웹 브라우저로 접속하는 그래픽 관리 화면이고, **Gaia Clish** 는 기본 명령줄 셸 입니다. Gaia Clish는 역할 기반으로 쓸 수 있는 명령이 제한된 "restricted shell"이라, 사용자마다 다룰 수 있는 명령이 다릅니다. 더 낮은 수준의 시스템·파일 작업이 필요할 때는 **Expert Mode** 로 들어갑니다 — 전체 root 권한을 주는 상위 셸 입니다.

> *Gaia Clish — The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).*
>
> — Gaia AdminGuide, "Glossary" (p.762)

Maestro·ElasticXL·Chassis 같은 **Scalable Platform** 의 Security Group에서는 Gaia Clish 대신 **Gaia gClish**(Global Clish)를 씁니다. 이건 같은 명령을 그룹의 모든 멤버에 한꺼번에 적용 하는 셸입니다.

시스템과 배포 형태

Gaia가 어떤 역할로 설치됐는지에 따라 동작이 달라집니다. **Security Gateway** 는 트래픽을 검사하고 보안 정책을 집행하는 서버 이고, **Security Management Server** 는 객체와 정책을 관리하는 서버 입니다. 둘을 한 서버에 같이 올리면 **Standalone**, 서로 다른 서버에 나누면 **Distributed Deployment** 입니다. **Multi-Domain Server**(MDS)는 여러 가상 관리 서버(Domain Management Server)를 한 서버에 호스팅 합니다. **Open Server** 는 Check Point가 아닌 다른 회사가 만든 일반 하드웨어 를 뜻합니다.

Cluster 는 두 대 이상의 게이트웨이를 High Availability나 Load Sharing으로 묶은 것 이고, 그 구성원이 **Cluster Member** 입니다. **VSX**(Virtual System Extension)는 한 장비 위에 여러 가상 게이트웨이를 올리는 가상화 솔루션 입니다(자세히는 VSX 가이드 참고).

운영·관리에 쓰는 도구

SmartConsole 은 정책 구성·장치 관리·모니터링을 하는 Check Point GUI 애플리케이션 으로, Gaia 장비를 중앙에서 관리할 때도 씁니다(SmartConsole 중앙 관리). **CPUSE**(Check Point Upgrade Service Engine)는 Gaia OS와 그 위 제품을 자동으로 업데이트해 주는 엔진 입니다(소프트웨어 업데이트).

신뢰의 바탕이 되는 두 약어도 알아 둡니다. **ICA**(Internal Certificate Authority)는 관리 서버에 내장돼 인증서를 발급하는 인증 기관 이고, **SIC**(Secure Internal Communication)는 Check Point 장비끼리 SSL로 서로를 인증하는 메커니즘 입니다.

인터페이스와 네트워크

Management Interface 는 관리 서버가 게이트웨이에 접속하는 통로이자, 사용자가 Gaia Portal·CLI에 접속하는 인터페이스 입니다(네트워크 관리). **DAIP Gateway** 는 외부 인터페이스 IP를 ISP가 동적으로 할당하는 게이트웨이 를 뜻합니다.

마지막으로 운영하다 만나는 패키지 용어입니다 — **Hotfix** 는 기존 버전 위에 얹어 잘못된 동작을 고치거나 기능을 더하는 소프트웨어 패키지 이고, **Jumbo Hotfix Accumulator**(JHF)는 여러 핫픽스를 하나로 모은 패키지 입니다.

02 Gaia 개요와 시작하기

Gaia 개요와 시작하기

Gaia 는 Check Point 보안 제품을 위한 차세대 운영체제 로, 게이트웨이부터 관리 서버까지 모든 Software Blade와 제품군을 그 위에서 돌립니다. 이 장은 Gaia가 무엇이고 무엇을 지원하는지, 그리고 새 장비를 처음 받았을 때 어떤 순서로 구성해 나가는지를 큰 그림으로 잡습니다.

Gaia가 통합한 것

Gaia라는 이름은 그리스 신화에서 만물을 낳은 어머니 신에서 왔습니다. 긴밀하게 맞물린 부품들이 하나의 효율적인 시스템을 이룬다 는 뜻을 담은 작명입니다. 실제로 Gaia는 Check Point의 옛 운영체제(SecurePlatform)와 어플라이언스용 IPSO의 장점을 한데 합친 통합 OS 로, Check Point 어플라이언스와 Open Server를 가리지 않고 모두에서 동작합니다.

현대의 고성능 배포를 처음부터 염두에 두고 설계되어, 다음을 지원합니다. IPv4·IPv6를 OS에 완전히 통합 했고, 64비트 Linux 커널로 높은 연결 용량과 많은 Virtual System 을 감당합니다. 부하 분산은 ClusterXL과 Interface bonding으로, 고가용성은 ClusterXL·**VRRP**·bonding으로 제공합니다(고가용성 — VRRP). 동적·멀티캐스트 라우팅으로 BGP·OSPF·RIP·PIM·IGMP를 다룹니다.

운영 편의 면에서는 같은 문법 규칙으로 구조화된 명령줄(Gaia Clish) 과 자동 완성·도움말을 제공하고(명령줄 인터페이스), **Role-Based Administration** 으로 관리자마다 기능별 읽기/쓰기 권한을 역할로 나눠 줍니다(사용자 관리). 또 **CPUSE** 로 라이선스된 제품을 OS에서 바로 내려받아 빠르게 설치하고 손쉽게 롤백 할 수 있으며(소프트웨어 업데이트·API), **Gaia API** 로 설정을 자동화할 수 있습니다(sk143612 참고).

새 장비를 받으면 — 구성 순서

처음 장비를 설치할 때는 정해진 순서를 따르면 길을 잃지 않습니다. 먼저 Gaia OS를 설치하고, First Time Configuration Wizard를 돌려 기본 골격을 잡 습니다(자세히는 최초 구성 마법사). 그다음 필요한 인터페이스를 살리고 IP를 배정한 뒤, Bond·VLAN·Bridge 같은 특수 인터페이스를 구성합니다(네트워크 관리).

이어서 DNS 설정과 IPv4·IPv6 static route, 필요하면 Proxy 서버 를 잡아 네트워크 경로를 완성합니다. 운영 주체를 정하는 단계로 넘어가 Role과 User를 만들고 Password Policy를 적용 하며(사용자 관리), 마지막으로 라이선스를 설치하고(유지보수) 적용 가능한 소프트웨어 업데이트 를 올리면 기본 구성이 끝납니다. 각 단계의 화면 클릭 단위 절차는 해당 장에서 이어집니다.

03 Gaia Portal과 시스템 정보

Gaia Portal과 시스템 정보

Gaia Portal 은 웹 브라우저로 접속하는 Gaia의 그래픽 관리 화면 으로, 거의 모든 시스템 구성 작업을 여기서 할 수 있습니다. 이 장은 Portal의 화면 구성과 로그인·잠금, 그리고 시스템 현황을 보는 방법을 정리합니다.

Gaia Portal에 접속하기

접속은 간단합니다 — 브라우저로 `https://<Gaia 관리 인터페이스 IP>` 에 들어가 사용자 이름과 암호를 입력하면 됩니다. Edge·Firefox·Chrome·Safari 등 주요 브라우저를 지원하고, 강력한 검색창으로 기능 이름이나 설정 파라미터를 키워드로 쳐서 해당 구성 페이지를 바로 찾을 수 있습니다. 화면은 기본 옵션만 보이는 **Simplified** 와 모든 옵션을 보이는 **Advanced** 두 모드를 오갈 수 있고, 브라우저 안에서 클라이언트 설치 없이 Gaia Clish 콘솔 까지 띄울 수 있습니다.

Maestro·Chassis 같은 Scalable Platform에서는 해당 Security Group의 Gaia Portal에 접속 해야 합니다. 한 가지 주의할 점은 브라우저의 뒤로 가기 버튼은 지원되지 않 으니 쓰지 말아야 한다는 것입니다.

!① 탐색 트리 ② 도구 모음 ③ 상태 표시줄 ④ 시스템 정보 위젯이 있는 Overview 페이지 ⑤ 검색 도구 — Gaia Portal 인터페이스 *① 탐색 트리 ② 도구 모음 ③ 상태 표시줄 ④ 시스템 정보 위젯이 있는 Overview 페이지 ⑤ 검색 도구*

화면은 왼쪽의 **탐색 트리**(기능별로 묶인 페이지 목록), 위쪽 **도구 모음**, 아래쪽 **상태 표시줄**(마지막 구성 작업 결과를 보여 줌), 가운데 **Overview 페이지** 로 이뤄집니다. 탐색 트리는 기본 페이지만 보이는 Basic과 전부 보이는 Advanced 모드가 있습니다. 또 구성을 보고 바꾸는 **Configuration** 탭과, 동적 라우팅·VRRP의 상태·통계를 실시간으로 보여 주는 **Monitoring 탭** 이 나뉘어 있습니다.

구성 잠금 — 한 번에 한 사람만 쓰기 가능

Gaia 구성에서 중요한 원칙은 한 시점에 단 한 사용자만 Read/Write 권한을 갖는다 는 것입니다. 다른 사용자는 자기 역할에 따라 Read-Only로 설정을 볼 수만 있습니다. 로그인할 때 아무도 잠금을 쥐고 있지 않으면 자동으로 배타적 구성 잠금(Read/Write)을 얻 고, 이미 다른 사용자가 쥐고 있으면 그 잠금을 **override**(빼앗기)할지 선택합니다. 빼앗으면 상대는 Read-Only로 남고, 빼앗지 않으면 설정을 바꿀 수 없습니다.

이 잠금은 브라우저를 닫아도 풀리지 않 는다는 점이 함정입니다. 다른 사용자가 풀거나 비활동 타임아웃(기본 10분)이 지나야 풀리므로, 쓰기를 마치면 반드시 오른쪽 위에서 로그아웃 해야 합니다. 같은 잠금 개념을 CLI에서 다루는 `lock database` · `set config-lock` 명령은 명령줄 인터페이스에서 이어집니다.

> 참 고
>
> XSS 공격을 막으려고 Gaia Portal은 입력 필드에서 일부 문자(<, >, &, ;)와 일부 단어 (after·apply·catch·eval·subset)를 받지 않습니다.

시스템 현황 보기

Overview 페이지에는 한눈에 상태를 보여 주는 **위젯** 들이 놓입니다. **System Overview**(설치 제품·버전·커널 에디션·빌드·가동 시간·하드웨어·시리얼 번호), **Blades**(켜진 Software Blade는 컬러, 꺼진 것은 회색), **Network Configuration**(인터페이스·IP·링크 상태), 그리고 CPU·메모리·패킷 속도·처리량 그래프 가 그것입니다. 위젯은 드래그로 옮기거나 추가·제거·접기를 할 수 있습니다.

같은 정보를 명령줄에서도 봅니다. `show uptime` 은 가동 시간, `show version all` 은 OS 구성요소의 전체 버전 정보 를 보여 주며, `show version os build` · `edition` · `kernel` , `show version product` 로 항목을 골라 볼 수 있습니다. Scalable Platform에서는 Gaia gClish로 실행하면 그룹 전체에, 멤버의 Gaia Clish로 실행하면 그 멤버에만 적용됩니다.

04 명령줄 인터페이스 (Gaia Clish)

명령줄 인터페이스 (Gaia Clish)

Gaia의 기본 셸은 **clish** 입니다. 이 장은 Gaia Clish에 로그인하고, 명령을 짓고, 자동 완성·이력으로 빠르게 입력하며, 변경을 저장하고, 필요하면 Expert mode로 내려가는 명령줄 작업의 기본기를 정리합니다.

Gaia Clish에 들어가기와 변경 저장

Gaia에는 SmartConsole, 또는 SSH·콘솔 명령줄로 접속해 사용자 이름·암호로 로그인합니다 (설치 직후 기본값은 모두 `admin`). 명령을 짓는 규칙은 일관됩니다 — `<Operation> <Feature> <Parameter>` 꼴 로, 주 동작은 `add` (생성)· `set` (값 설정)· `show` (조회)· `delete` (삭제) 입니다. 그 외에 `reboot` · `halt` · `expert` · `ver` 같은 동작과, 변경을 한꺼번에 적용/취소하는 트랜잭션(`start` → `commit` / `rollback`)도 있습니다.

여기서 반드시 기억할 것 하나 가 있습니다. Gaia Clish로 OS 구성을 바꾸면 그 변경은 실행 중인 시스템에 즉시 적용되지만, 재부팅하면 사라진 다는 점입니다.

> 주 의
>
> 변경을 재부팅 후에도 유지하려면 반드시 `save config` 를 실행해야 합니다.

Maestro·Chassis 등 Security Group에서는 Gaia Clish에서 `gclish` 를 쳐서 **Gaia gClish**(Global Clish)로 들어갑니다. gClish 명령은 기본적으로 그룹의 모든 멤버에 적용되며(DOWN 상태 멤버는 제외), 멤버끼리 설정이 같아야 하므로 일부에만 적용할 때도 `set blade-range` 를 쓰도록 권장합니다. gClish 트래픽은 Sync 인터페이스의 TCP 1129 포트로 흐릅니다.

자동 완성과 명령 이력 — 빠르게 입력하기

Gaia Clish는 외우지 않아도 다음 입력을 알려 주는 자동 완성이 강력합니다. `<TAB>` 은 키워드를 완성하거나 가능한 후보 를 보여 주고, `<SPACE><TAB>` 은 그 기능이 받는 인자를, `<ESC><ESC>` 는 가능한 전체 명령 형태를 펼쳐 줍니다. `<SHIFT>?` 는 현재 키워드의 도움말 을 띄웁니다. 화살표 키로 이력을 오가고 줄 안에서 커서를 옮겨 편집할 수 있습니다.

이미 쓴 명령은 이전 세션 것까지 불러올 수 있습니다. `history` 는 최근 100개 명령 을 보여 주고, `!!` 는 마지막 명령을, `!14` 는 14번 명령을, `!show` 는 `show` 로 시작하는 가장 최근 명령을 다시 실행합니다. 줄 안에서 움직이는 단축키도 Emacs식으로 갖춰져 있어, `CTRL A` / `CTRL E` 로 줄 처음·끝, `CTRL U` 로 전체 삭제, `CTRL R` 로 이력 검색 을 합니다.

가능한 명령 목록을 직접 둘러볼 수도 있습니다. `show commands` 는 권한 있는 명령을, `show commands feature <이름>` 은 특정 기능의 명령을 보여 주며, 빈 동작어 (`set` · `show` · `add` · `delete`) 뒤에 `<SPACE><TAB>` 을 눌러도 됩니다.

구성 잠금과 클라이언트 환경

Gaia Portal에서 본 구성 잠금은 CLI에도 그대로 적용됩니다. 한 번에 한 사용자만 Read/Write 권한 을 갖고 나머지는 Read-Only입니다. `lock database override` 는 다른 관리자의 쓰기 권한을 빼앗아 배타적 권한 을 얻고(이때 상대는 알림을 못 받으니 신중히), `unlock database` 로 풉니다. 이 두 명령은 각각 `set config-lock on override` · `set config-lock off` 와 같으며, `show config-lock` 으로 상태를 봅니다. Gaia Clish가 잠금을 쥐면 그 잠금이 풀릴 때까지 Gaia Portal에서는 구성을 바꿀 수 없 습니다.

셸 동작은 클라이언트 환경으로 다듬습니다. `set clienv` 로 출력 형식 (`pretty` · `structured` · `xml`), 프롬프트 문자열, 디버그 수준, 실패 시 동작 (`continue` / `stop`), 문법 검사 모드 등을 바꾸고, `save clienv` 로 영구 저장합니다. 출력 형식은 보기 좋은 `pretty` 가 기본이고, 세미콜론으로 구분된 `structured` 나 태그가 붙은 `xml` 은 스크립트 파싱에 유용합니다.

Expert Mode — 낮은 수준 접근

Gaia Clish는 보안을 위해 명령이 제한된 "restricted shell"이라 저수준 시스템 기능에는 닿지 않습니다. 파일 시스템 등 낮은 수준의 구성이 필요하면 더 허용적인 **Expert mode** 셸로 내려갑니다 — Gaia Clish에서 `expert`로 들어가고 `exit`로 돌아옵니다(암호 설정은 시스템 관리).

여기엔 중요한 원칙이 있습니다. Expert mode는 "더 많은 권한"이 아니라 "더 많은 구성 능력"을 줄 뿐이며, 보안 기능이 아니라 실수를 막는 보호 장치 입니다. 그래서 Gaia Clish에 명령이 있는 작업은 Expert mode에서 대응 명령을 쓰면 안 됩니다 — 예컨대 인터페이스는 Gaia Clish의 `set interface`로 다뤄야지 Expert mode의 `ifconfig`로 건드리면 안 됩니다. Expert mode 로그인은 `/var/log/messages`에 기록되며, `set audit login-notifier on` (기본값)으로 이 감사 로깅을 제어합니다.

끝으로 **User Defined (Extended) Commands** 가 있습니다. 일반 Linux 명령을 Gaia Clish 명령으로 등록 한 뒤(역할)에서 역할에 할당해, 특정 사용자만 그 명령을 쓰게 만드는 RBA 기법입니다. 예를 들어 `add command free path /usr/bin/free ...`로 `free`를 등록하고, 그 확장 명령(`ext_free`)을 역할에 넣어 사용자에게 부여합니다.

05 최초 구성 마법사

최초 구성 마법사

Gaia를 처음 설치한 뒤에는 **First Time Configuration Wizard** 로 시스템과 그 위 Check Point 제품의 기본 골격을 잡습니다. 이 장은 마법사가 차례로 묻는 항목들을 흐름에 따라 설명합니다 — 배포 방식 → 암호 → 관리 연결 → 인터넷 연결 → 장치 정보 → 날짜·시간 → 설치 유형 의 순서입니다.

마법사를 시작하기

마법사는 Gaia Portal에서, 또는 CLI Expert mode에서 돌릴 수 있습니다. Portal 방식이 일반적입니다 — 설치 때 정한 관리 인터페이스(예: eth0)에 컴퓨터를 연결하고, 같은 서브넷의 고정 IP를 잡은 뒤, 브라우저로 `https://<관리 인터페이스 IP>` 에 접속 해 기본 계정 `admin` / `admin` 으로 로그인하면 마법사가 열립니다. 이후 화면 안내를 따라가며, 제품·하드웨어에 따라 보이는 창과 필드가 조금씩 달라집니다.

마법사가 묻는 것들

첫 화면인 **Deployment Options** 에서 설치된 Gaia로 그대로 구성을 이어 갈지(Continue with R82 configuration), Check Point Cloud나 USB에서 새로 설치할지, 기존 스냅샷을 가져올지 를 고릅니다. Cloud 설치를 고르면 Zero Touch Cloud Service로 준비한 초기 배포 구성을 끌어오는 방식도 쓸 수 있으나, Scalable Platform은 이 기능을 지원하지 않 습니다.

Authentication Details 에서는 두 가지 핵심 암호를 정합니다 — Expert mode 암호와, Maintenance Mode(GRUB) 암호 입니다. GRUB 암호는 Maintenance Mode로 부팅하거나 Gaia 스냅샷을 되돌릴 때 묻는 암호입니다. 보안을 위해 두 암호는 서로 다르게 정하길 권장하며, 마법사를 마친 뒤에도 시스템 관리에서 바꿀 수 있습니다.

이어 **Management Connection** 에서 Gaia Portal·CLI에 접속할 주 관리 인터페이스와 그 IP 를 정하고(설치 때 쓴 인터페이스가 기본값, R82는 관리 인터페이스에 IPv6 주소를 아직 지원하지 않음), 선택 사항인 **Internet Connection** 에서 인터넷에 닿는 인터페이스를 잡습니다. **Device Information** 에서는 호스트 이름·도메인·DNS 서버(주/보조/3차)·Proxy 를, **Date and Time Settings** 에서는 수동 날짜·시간 또는 NTP 서버와 시간대 를 설정합니다.

마지막 **Installation Type** 에서 이 장비에 올릴 제품을 고릅니다. Security Gateway·Cluster Member·Security Management Server(관리 HA 포함)·Endpoint 서버·전용 Log Server 등을 선택할 수 있으며, Scalable Platform은 Security Gateway 옵션만 지원 합니다.

마법사가 끝나면 시스템이 재부팅되고, 이후 인터페이스·라우팅·사용자 등 세부 구성은 네트워크 관리·사용자 관리 같은 해당 장에서 이어 갑니다. 각 창의 필드 단위 세부는 원문 "Configuring Gaia for the First Time" 절을 참고하세요.

06 SmartConsole 중앙 관리

SmartConsole 중앙 관리

Gaia 장비는 한 대씩 Portal로 들여다보는 대신, **SmartConsole** 에서 중앙으로 관리 할 수 있습니다. 이 장은 SmartConsole로 Gaia 게이트웨이의 토폴로지·장치 설정을 통합 관리하고, 스크립트를 돌리고, 백업·복원하고, 원격으로 셸·Portal을 여는 방법을 정리합니다. 단, Scalable Platform의 Security Group은 Gaia 장치 설정의 중앙 관리를 지원하지 않 습니다(Known Limitation MBS-4754).

SmartConsole이 중앙에서 할 수 있는 일

Central Management를 켜면 SmartConsole에서 네트워크 토폴로지(IPv4·IPv6 주소와 static route)와 장치 설정(DNS·NTP·Proxy)을 중앙에서 구성 할 수 있습니다. 또 Gaia OS 구성과 게이트웨이 DB를 한꺼번에 .tgz로 백업·복원 하고, SmartConsole에서 바로 Gaia Portal이나 셸을 열어 유지보수를 합니다.

여기서 편리한 점은 정책을 전부 다시 설치(full policy install)하지 않고도, **Push Settings to Device** 동작으로 장치 설정 변경만 반영 할 수 있다는 것입니다. 반대로 장치에서 설정을 가져오는(fetch) 것도 됩니다. 게이트웨이에서 로컬 구성이 바뀌면 Gateways 뷰의 Status 열에 표시되고, 최근 작업은 하단 **Recent Tasks** 탭에서 확인합니다. **Cloning Group** 의 구성·동기화 자동화도 여기서 이뤄집니다(시스템 관리의 Cloning Group).

게이트웨이에서 스크립트 돌리기

SmartConsole에서 Gaia 게이트웨이에 직접 명령줄 스크립트를 실행할 수 있습니다. 일회성으로 즉석에서 치는 **One Time Script** 와, 미리 저장해 두고 재사용하는 **Repository Script** 두 갈래입니다. 게이트웨이를 우클릭해 Scripts 메뉴에서 고르며, 스크립트 본문을 직접 입력하거나 텍스트 파일로 불러옵니다(기본 최대 크기 8KB, Global properties에서 조정 가능). 실행 결과는 Tasks 탭의 Results 열에 뜨고, 더블클릭하면 전체 출력을 봅니다.

한 가지 한계가 있습니다 — 이 스크립트 창은 대화형(interactive)·연속(continuous) 스크립트를 지원하지 않 으므로, 그런 작업은 셸을 직접 열어야 합니다. Cloning Group에 속하지 않은 여러 게이트웨이에는 동시에 스크립트를 돌릴 수 있고, 클러스터 객체에 돌리면 모든 멤버에서 자동 실행 됩니다.

백업·복원과 원격 접속

SmartConsole에서 게이트웨이를 우클릭해 Actions > System Backup 으로 Gaia OS 구성과 방화벽 DB를 압축 파일로 백업 하고, System Restore로 되돌립니다. 백업 파일은 `backup_<게이트웨이 이름>_<날짜>.tgz` 규칙으로 이름이 붙으며, 복원하려면 이 파일 이름이 필요합니다 — 이름을 잊었다면 셸에서 `show backup logs` 로 찾습니다. 복원 시에는 게이트웨이 연결이 끊기고 자동 재부팅되며, 이후 정책을 다시 설치 해야 합니다. 규칙적 보호를 위해서는 유지보수의 System Backup으로 정기 백업을 거는 것을 권장합니다.

마지막으로, SmartConsole에서 게이트웨이를 우클릭하거나 상단 Actions 버튼으로 그 장비의 명령줄 창(Open Shell, 공개 키 인증)이나 Gaia Portal을 바로 열 수 있습니다. 클러스터라면 어느 멤버에 접속할지 고릅니다.

07 네트워크 관리 — 인터페이스와 라우팅

네트워크 관리 — 인터페이스와 라우팅

네트워크 관리는 Gaia 운영의 가장 큰 영역으로, 인터페이스를 종류별로 만들고, ARP·DHCP·DNS를 설정하고, static route로 경로를 정하고, NetFlow로 트래픽을 내보내는 일을 모두 아우릅니다. 이 장은 화면 클릭 단위 절차 대신 각 기능이 무엇이고 언제 쓰는지 를 개념·흐름 위주로 정리합니다. 세부 절차는 원문 "Network Management" 절을 참고하세요.

Gaia가 지원하는 인터페이스 종류

Gaia는 다양한 인터페이스를 다룹니다. 바탕은 **물리 인터페이스**(Ethernet)로, Gaia가 NIC을 자동으로 식별 하므로 Portal·CLI에서 물리 인터페이스를 추가·삭제할 수는 없고, 카드 교체는 시스템을 끈 상태에서만 합니다. 그 위에 여러 가상 인터페이스를 얹습니다 — **Alias**(한 인터페이스에 보조 IP 추가), **VLAN**, **VXLAN**, **Bond**(링크 묶음), **Bridge**(L2 브리지), **Loopback**, **VPN Tunnel**(VTI), **6in4·PPPoE·GRE** 터널 입니다.
Maestro·Chassis용으로는 **MAGG** 도 있습니다. 다만 VXLAN·VTI·6in4·PPPoE·GRE 등 상당수는 Scalable Platform에서 지원되지 않 으니 주의해야 합니다.

> 참 고
>
> 인터페이스 IP를 추가·삭제·변경한 뒤 SmartConsole의 Get Topology가 잘못된 토폴로지를 보이면, 게이트웨이에서 `cpstop` 후 `cpstart`를 실행하세요.

VLAN과 Bridge — 기존 토폴로지에 녹여 넣기

VLAN 인터페이스는 Ethernet 인터페이스 위에 가상 LAN을 올려, 기존 토폴로지를 그대로 둔 채 안전한 사설 링크로 서브넷을 나누 게 합니다. 스위치 포트가 Access 모드인지 Trunk 모드인지에 따라 구성이 달라지며, 서로 다른 VLAN 번호를 Bridge로 묶으면 VLAN 변환(translation)도 됩니다.

!① Security Gateway ② 스위치 ③ VLAN 변환 Access mode bridge 1 ④ VLAN 변환 Access mode bridge 2 ⑤ VLAN 3(eth1.3) — VLAN 변환 토폴로지 예 *① Security Gateway ② 스위치 ③ Access mode bridge 1(VLAN 변환) ④ Access mode bridge 2(VLAN 변환) ⑤ VLAN 3(eth1.3)*

Bridge 인터페이스는 IP 라우팅 구조를 다시 짜지 않고도 보안 장비를 끼워 넣는 강력한 방법입니다. 두 인터페이스(bridge port)를 연결해, 한 포트에 들어온 모든 Ethernet 프레임을 다른 포트로 전달 하면서 그 프레임을 보안 정책으로 검사 합니다 — 즉 두 포트가 같은 브로드캐스트 도메인에 속하는 가상 2포트 스위치가 됩니다. 한 Bridge에는 두 인터페이스만 연결 할 수 있고, 이름은 `br<번호>` (예: br5)이며 IP 없이 동작합니다. Gaia는 native L2 브리징을 지원하되 STP(Spanning Tree Protocol)는 지원하지 않습니다.

Bond — 링크 묶어 이중화·증속

Bond(Link Aggregation)는 여러 물리 인터페이스를 하나의 가상 인터페이스로 묶어, 부하를 나누고 장애에 견디며 처리량을 높이 는 기술입니다. 동적 묶음에는 IEEE 802.3ad **LACP** 를 씁니다. Bond에는 IP가 붙고, 묶인 물리 인터페이스(subordinate)에는 IP가 없 으며, 한 Bond에 최대 8개까지 넣을 수 있습니다.

!① Security Gateway(1A 인터페이스 1 · 1B 인터페이스 2) ② Bond 인터페이스 ③ 라우터 — 두 인터페이스를 하나의 Bond로 묶음 *① Security Gateway(1A 인터페이스 1 · 1B 인터페이스 2) ② Bond 인터페이스 ③ 라우터*

동작 전략은 두 갈래입니다. **High Availability(Active/Backup)** 는 한 인터페이스만 Active로 쓰다가 다운되면 다른 것으로 자동 페일오버 해 이중화를 주고(스위치 이중화도 지원), **Load Sharing(Active/Active)** 는 UP 상태의 모든 인터페이스를 동시에 써 처리량을 극대화 합니다(SecureXL 필요, 스위치 이중화는 미지원). Load Sharing의 분배 방식으로는 순차로 도는 **Round Robin**, LACP로 링크를 완전히 감시하는 **802.3ad**, 해시로 나누는 **XOR**, 묶음(bundle) 단위로 하나만 Active인 **ABXOR** 가 있습니다.

ARP·DHCP·DNS — 기본 네트워크 서비스

ARP(Address Resolution Protocol)는 IP 주소만으로 같은 물리 네트워크 안 대상의 물리(MAC) 주소를 찾는 저수준 프로토콜로, Gaia에서 동적·정적 ARP 항목을 보고 관리합니다. **DHCP Server** 로는 Gaia 장비가 직접 네트워크 호스트에 IP와 네트워크 파라미터를 나눠 주게 해(IPv6는 DHCPv6), 호스트마다 수동 설정하는 수고와 오류를 덜 수 있습니다(Scalable Platform 미지원). **Hosts and DNS** 페이지에서는 호스트 이름·도메인, 정적 host 항목, DNS 서버 를 한자리에서 설정합니다.

정적 라우팅과 동적 라우팅

Static Route 는 목적지와 그곳에 닿는 하나 이상의 경로(next hop)를 수동으로 정의 하는 것으로, `set static-route` 명령(Security Group에서는 gClish)이나 Portal로 만듭니다. 동적 라우팅이 모르는 목적지에 경로를 더하거나, 여러 경로에 우선순위를 주거나, 기본 경로(default route)를 정할 때 씁니다. IPv4·IPv6를 각각 다루며, IPv6 Neighbor 항목도 여기서 설정합니다.

더 큰 규모의 라우팅은 **Advanced Routing** 으로 넘어갑니다. 동적 라우팅은 Gaia Portal·Gaia Clish에 완전히 통합 되어 **BGP·OSPF·RIP** 와 동적 멀티캐스트 라우팅(**PIM** SM/DM/SSM, **IGMP**)을 지원합니다. 동적 라우팅의 상세 구성은 별도 문서인 R82 Gaia Advanced Routing Administration Guide에서 다룹니다.

NetFlow Export — 트래픽 흐름 내보내기

NetFlow 는 트래픽 모니터링의 업계 표준 으로(Cisco가 개발), 한 호스트(NetFlow Exporter)가 자신의 네트워크 흐름 정보를 다른 호스트(NetFlow Collector)로 보내 분석하게 합니다. 여기서 흐름(flow)이란 같은 특성을 가진 단방향 패킷 스트림을 뜻합니다. Gaia에서는 게이트웨이·Cluster Member를 통과하는 모든 트래픽에 대해 NetFlow 레코드를 내보내는 Exporter로 설정 할 수 있으며, SecureXL의 상태와는 무관하게 동작합니다.

08 시스템 관리

시스템 관리

시스템 관리는 네트워크가 아닌, 장비 자체의 살림살이 를 다루는 영역입니다. 암호·시간·Proxy 같은 기본 설정부터 SNMP 모니터링, 작업 스케줄, 로그, 접속 제어, 여러 게이트웨이를 한 묶음으로 동기화하는 Cloning Group까지를 아우릅니다. 이 장은 각 기능의 쓰임을 개념 위주로 정리하며, 화면 단위 절차는 원문 "System Management" 절을 참고하세요.

암호와 시간, 그리고 Proxy

System Passwords 에서는 두 가지 핵심 암호를 관리합니다 — Expert mode 암호와 GRUB(Maintenance Mode) 암호 입니다. 최초 구성 마법사에서 정한 이 암호들을 여기서 다시 바꿀 수 있으며, 보안상 둘은 서로 다르게 두길 권장합니다.

Time 은 날짜·시간·시간대를 수동으로, 또는 NTP 서버로 자동 맞춥니다. 시간 동기화는 인증서 검증·로그 정합성·클러스터 동작에 중요합니다.

Proxy 는 헷갈리기 쉬워 구분이 필요합니다. Gaia 운영체제용 Proxy 설정은 OS에만 적용되고 Software Blade에는 적용되지 않 습니다. 반대로 게이트웨이·관리 서버가 업데이트·ThreatCloud에 접속할 때 쓰는 Proxy는 SmartConsole의 Global properties나 객체 속성에서 설정 하며, 이건 Gaia 위 Software Blade에만 적용됩니다. 또 게이트웨이 자체를 HTTP/HTTPS Proxy로 만드는 것은 또 다른 기능으로, 별도 게이트웨이 가이드에서 다룹니다.

Cloning Group — 여러 게이트웨이를 한 몸처럼

Cloning Group 은 여러 Gaia 게이트웨이가 OS 구성과 공유 기능 설정(예: DNS, ARP)을 서로 동기화하는 묶음 입니다. 한 곳에서 바꾸면 그룹 전체에 퍼지므로, 비슷하게 운영해야 할 게이트웨이들을 일관되게 유지하기 좋습니다(Scalable Platform 미지원). 동기화 자동화는 SmartConsole 중앙 관리와도 맞물립니다.

SNMP — 표준 모니터링

SNMP(Simple Network Management Protocol)는 네트워크 장비끼리 관리 정보를 주고받는 인터넷 표준 입니다. SNMP를 따르는 장비(agent)는 자기 정보를 **MIB**(Management Information Base)에 담아 두고, 요청이 오면 돌려줍니다.

> *Simple Network Management Protocol (SNMP) is an Internet standard protocol... SNMP-compliant devices, called agents, keep data about themselves in Management Information Bases (MIBs) and resend this data to the SNMP requesters.*
>
> — Gaia AdminGuide, "SNMP" (p.342)

Check Point 구현에서는 SNMP 매니저가 시스템을 모니터링하고 일부 객체만 수정 할 수 있습니다. 읽기 전용 community string 하나와 읽기/쓰기 community string 하나를 정하고, trap 수신자를 추가·삭제하며 각종 trap을 켜고 끌 수 있습니다. 보안이 강화된 **SNMP v3**(User-Based Security Model, USM)도 지원합니다.

작업 자동화와 알림 — Job Scheduler·Mail·Messages

Job Scheduler 로는 정해진 날짜·시간이나 부팅 시점에 정기 작업을 돌릴 수 있습니다. **Mail Notification** 은 시스템 이벤트를 메일로 알리는 설정이고, **Messages** 는 로그인 배너나 알림 메시지(MOTD 등)를 띄우는 기능입니다. 이들을 묶어 쓰면 손이 덜 가는 운영을 만들 수 있습니다.

로그와 접속 제어

System Logging 은 시스템 로그 설정과, 원격 서버로 로그를 보내는 Remote System Logging 을 다룹니다(원격 서버 쪽에서 로그 수신 설정 필요). **System Configuration** 에서는 IPv6 지원 켜기 같은 OS 수준 설정을, **Crash Data**·**Display Format**·**Session** 등에서는 진단 데이터와 표시 형식, 세션 타임아웃을 다듬습니다.

접속을 거르는 두 기능도 중요합니다. **Network Access** 와 **Host Access** 로 Gaia Portal·Gaia Clish에 접속할 수 있는 호스트·네트워크를 제한 해 관리 인터페이스를 보호합니다.

끝으로 **LLDP**(Link Layer Discovery Protocol)는 인접 장비끼리 자기 정보를 광고해 물리 토폴로지를 파악 하게 합니다. 관리 서버·게이트웨이용 LLDP와 Maestro Orchestrator용 LLDP가 따로 있으며, 일반 Scalable Platform에서는 지원되지 않습니다.

09 사용자 관리 — 인증·역할·서버

사용자 관리 — 인증·역할·서버

사용자 관리는 누가 Gaia에 들어올 수 있고, 들어와서 무엇을 할 수 있는지 를 정하는 영역입니다. 로그인 인증과 2단계 인증, 사용자 계정, 권한을 묶는 역할(Role), 암호 정책, 그리고 외부 인증 서버 연동까지를 다룹니다. 이 장은 각 기능의 개념을 정리하며, 세부 절차는 원문 "User Management" 절을 참고하세요.

로그인 인증과 2단계 인증

기본은 사용자 이름·암호 로그인이지만, Gaia는 보안을 한 단계 높이는 **2FA**(Two-Factor Authentication)를 지원합니다. 시간 기반 인증 앱(TOTP)을 이용해 Gaia 로그인 흐름에 인증 요소를 하나 더 추가 하는 방식입니다. 2FA를 켜면 Gaia Portal은 물론, SSH·Telnet 원격 로그인과 콘솔·LOM 카드를 통한 로컬 로그인까지 모든 CLI 셸 접속 이 보호됩니다. 특정 사용자에게만 켜거나 전체에 적용할 수 있고, 키 재발급·해제도 사용자 단위로 관리합니다.

사용자 계정과 역할(RBA)

Users 에서는 사용자를 추가하고 홈 디렉터리·기본 셸을 지정 합니다. 여기서 핵심은 권한을 부여하는 방식인 **Role-Based Administration**(RBA)입니다.

> *Role-based administration (RBA) lets you create administrative roles for users... Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features.*
>
> — Gaia AdminGuide, "Roles" (p.480)

즉 각 역할(Role)에 기능별로 읽기/쓰기·읽기 전용·접근 불가를 조합해 담고, 그 역할을 사용자에게 할당 합니다. 역할에는 접근 수단(Gaia Portal인지 Gaia Clish인지)도 지정할 수 있고, 확장 명령을 역할에 넣어 특정 사용자만 그 명령을 쓰게 만들 수도 있습니다. 사용자가 Portal에 로그인하면 자기가 접근 권한을 가진 기능만 보이며, 읽기 전용이면 설정 페이지는 보되 바꾸지는 못 합니다. 기본 제공 역할로는 모든 기능에 읽기/쓰기를 주는 **adminRole**, 읽기 전용을 주는 **monitorRole** 이 있으며 이 둘은 삭제·변경할 수 없습니다. 한 가지 주의할 점은, 외부 인증 서버에 정의된 사용자(external user)는 로컬에 새 사용자로 정의하지 말라는 것입니다.

암호 정책

Password Policy 는 강한 암호 생성을 강제하고, 이미 쓴 암호의 재사용을 막고, 정기적으로 암호를 바꾸게 하는 보안의 핵심 장치입니다. 암호 강도(Password Strength), 이력(History), 의무적 변경 주기, 미사용 계정 잠금, 로그인 실패 시 접근 거부, 해싱 알고리즘 까지 세밀하게 조정합니다. 다만 이 정책은 RADIUS 같은 외부 서버가 관리하는 비로컬 사용자나, SSH 공개 키 같은 비암호 인증에는 적용되지 않 습니다.

외부 인증 서버 — RADIUS·TACACS+

여러 게이트웨이의 계정을 일일이 로컬에 두는 대신, Gaia를 인증 서버의 클라이언트로 만들어, 로컬에 없는 사용자도 중앙에서 인증 할 수 있습니다. 이것이 자격 증명을 중앙 관리하는 좋은 방법입니다. Gaia는 두 종류를 지원합니다.

RADIUS 는 사용자 프로필을 중앙 DB에 두는 클라이언트/서버 인증 시스템 으로, 여러 서버를 우선순위로 등록해 첫 서버가 죽으면 다음 서버로 넘어가게 할 수 있습니다. **TACACS+** 는 모든 정보를 암호화해 원격 서버로 보내는 인증 프로토콜 로, 서비스별(예: Gaia Portal = HTTP 서비스)로 따로 설정합니다. TACACS+가 켜지면 암호를 확인할 때마다 서버에 접속하고, 서버가 실패하거나 닿지 않으면 로컬 암호로 인증을 대신 합니다.

여러 방법을 함께 쓰면 인증 순서는 RADIUS → TACACS+ → Local 입니다. 즉 외부 서버부터 시도하고, 안 되면 로컬로 떨어집니다.

그룹과 GUI 클라이언트

System Groups 로는 사용자를 시스템 그룹으로 묶어 관리하고, **GUI Clients** 로는 (관리 서버인 경우) 어떤 컴퓨터가 SmartConsole로 이 관리 서버에 접속할 수 있는지(신뢰 호스트)를 제한합니다. 특정 IP만 허용하거나 모든 IP를 허용하는 식으로 정하며, 이는 관리 접근을 좁히는 또 하나의 안전장치입니다.

10 고가용성 — VRRP

고가용성 — VRRP

VRRP(Virtual Router Redundancy Protocol)는 두 Gaia 게이트웨이가 서로를 백업해, 한쪽이 죽으면 IP를 다른 쪽으로 자동으로 넘기는 고가용성 솔루션입니다. 이 장은 VRRP의 용어와 동작 원리, 페일오버 방식, 그리고 대표적인 사용 사례를 정리합니다. Scalable Platform은 Gaia OS의 VRRP를 지원하지 않 으니 주의하세요.

VRRP란 — 라우터 이중화 표준

VRRP는 장애 시 IP 주소를 한 라우터에서 다른 라우터로 동적으로 넘겨, 라우팅 경로의 가용성과 신뢰성을 높이는 표준 프로토콜(RFC 3768)입니다. 각 VRRP 라우터는 고유 식별자인 **VRID**(Virtual Router Identifier)를 가지며, 여기에 하나 이상의 **VIP**(Virtual IP Address)가 묶 입니다. 이웃 노드는 이 VIP를 next hop이나 최종 목적지로 삼아 접속합니다.

Gaia는 두 가지 구성 방식을 제공합니다. **Monitored Circuit/Simplified VRRP** 는 모든 VRRP 인터페이스가 서로를 자동으로 감시 하는 간편 방식이고, **Advanced VRRP** 는 각 인터페이스마다 다른 VRID를 두고, 감시 대상을 일일이 명시 하는 방식입니다. 한 멤버에 두 방식을 섞어 쓸 수는 없고, Standalone 배포(게이트웨이와 관리 서버가 한 장비)는 VRRP 클러스터에 넣을 수 없 습니다.

ClusterXL 용어와의 대응

VRRP는 ClusterXL과 같은 고가용성을 다른 용어로 부릅니다. 짝을 지어 두면 이해가 빠릅니다.

VRRP 용어	ClusterXL 용어	뜻
VRRP Cluster	Cluster	이중화를 제공하는 게이트웨이 그룹
VRRP Router	Member	VRRP를 쓰는 멤버 게이트웨이
Master	Active	트래픽을 처리하는, 우선순위가 가장 높은 게이트웨이
Backup	Standby	Master가 죽으면 넘겨받는 예비 게이트웨이
VRID	Cluster name	가상 라우터의 고유 식별자(MAC 마지막 바이트이기도 함)
VIP	Cluster Virtual IP	가상 라우터에 배정된 IP(Portal에선 Backup Address)
VRRP Transition	Failover	Master 장애 시 Backup으로 자동 전환

Gaia에서 VRRP는 ClusterXL을 켜고도, 끄고도 쓸 수 있습니다. ClusterXL을 켜면 Active/Backup 환경만 배포 할 수 있고 인터페이스마다 하나의 VRID·VIP를 둡니다(가장 흔한 경우). ClusterXL을 끄면 Active/Active 환경이 가능 해, 한 인터페이스에 두 VRID를 둘 수 있지만 static route만 지원되고 방화벽 감시를 꺼야 합니다.

인터페이스 감시와 비대칭 경로

모든 VRRP 인터페이스를 모든 VRID가 감시하게 하는 것이 중요 합니다. 그러지 않으면 비대칭 경로 문제가 생기기 때문입니다 — 예컨대 외부 인터페이스만 페일오버하고 내부는 그대로면, 내부 가상 라우터가 트래픽을 받았는데 새 외부 Master에 닿지 못하는 상황이 벌어집니다. 그래서 한 인터페이스가 죽으면 같은 노드의 다른 VRID들도 함께 Backup으로 넘어가도록 priority delta를 설정 합니다.

또 다른 도구가 **interface delay** 입니다. Preempt 모드를 껐을 때 쓰며, 우선순위 높은 노드가 재부팅된 뒤 곧장 Master를 빼앗지 않고, Hello 패킷을 받을 시간을 벌어 줍니다.

페일오버는 어떻게 일어나나

각 가상 라우터는 한 Master와 하나 이상의 Backup 으로 이뤄지고, Master는 주기적으로 **VRRP advertisement**(VRRP Hello 메시지)를 보내 자기 동작 상태를 Backup에 알 립니다. Master는 처음엔 우선순위 값이 가장 높은 게이트웨이 가 됩니다(같으면 먼저 advertisement를 뿌린 쪽).

Master나 그 인터페이스가 죽으면 우선순위 알고리즘이 페일오버를 판단합니다. 장애 시 가상 라우터의 우선순위에서 미리 정한 **Priority Delta** 만큼 빼 **Effective Priority** 를 계산 하고, Effective Priority가 가장 높은 가상 라우터가 새 Master 가 됩니다(같으면 IP가 높은 쪽). 시스템을 올바로 구성하면 이 effective priority가 다른 가상 라우터에 있는 Backup의 우선순위보다 낮아져, 문제 있는 Master가 다른 가상 라우터에 대해서도 함께 페일오버 하게 됩니다.

대표적인 사용 사례

세 가지 전형을 그림으로 봅니다. 첫째는 내부망만 이중화 하는 가장 단순한 구성입니다.

!① VRRP Master 게이트웨이 ② VRRP Backup 게이트웨이 ③ 가상 라우터 VRID 5(VIP 192.168.2.5) ④ 내부망과 호스트 — 내부망 고가용성 *① VRRP Master 게이트웨이 ② VRRP Backup 게이트웨이 ③ 가상 라우터 VRID 5(VIP 192.168.2.5) ④ 내부망과 호스트*

둘째는 내부·외부 연결을 모두 이중화 하는 구성으로, 내부용·외부용 가상 라우터를 따로 두며 두 인터페이스는 서로 다른 서브넷에 있어야 합니다.

!① 외부 가상 라우터 VRID 5(외부 VIP 192.168.2.5) ② VRRP Master 게이트웨이 ③ VRRP Backup 게이트웨이 ④ 내부 가상 라우터 VRID 5(내부 VIP 192.168.3.5) ⑤ 내부망과 호스트 — 내부·외부 고가용성 *① 외부 가상 라우터 VRID 5(외부 VIP 192.168.2.5) ② VRRP Master 게이트웨이 ③ VRRP Backup 게이트웨이 ④ 내부 가상 라우터 VRID 5(내부 VIP 192.168.3.5) ⑤ 내부망과 호스트*

셋째는 내부망 Load Sharing(Active/Active) 구성입니다. ClusterXL을 끄고 static route만 쓰며 방화벽 감시를 꺼야 하고, 게이트웨이 1은 VRID 5의 Master·VRID 7의 Backup, 게이트웨이 2는 그 반대 로 두어 서로를 백업하면서 부하도 나눕니다.

!① VRID 5의 Master·VRID 7의 Backup 게이트웨이 ② VRID 5의 Backup·VRID 7의 Master 게이트웨이 ③ 가상 라우터 VRID 5(VIP 192.168.2.5) — 내부망 Load Sharing *① VRID 5의 Master·VRID 7의 Backup 게이트웨이 ② VRID 5의 Backup·VRID 7의 Master 게이트웨이 ③ 가상 라우터 VRID 5(VIP 192.168.2.5)*

클러스터 준비, Monitored Circuit·Advanced VRRP의 상세 구성과 문제 해결 절차는 원문의 해당 절을 참고하세요.

11 유지보수 — 라이선스·스냅샷·백업

유지보수 — 라이선스·스냅샷·백업

유지보수는 장비를 건강하게 유지하고, 문제가 생겼을 때 되돌릴 안전망을 마련하는 작업입니다. 라이선스 관리, 시스템 전체를 통째로 보존하는 스냅샷, 가벼운 구성 백업, 하드웨어·RAID 상태 점검, 그리고 재부팅·종료를 다룹니다. 이 장은 각 기능의 개념과 스냅샷과 백업의 결정적 차이 를 중심으로 정리합니다.

라이선스 상태

License Status 에서는 장비에 설치된 라이선스를 확인하고 활성화 합니다. Check Point 어플라이언스·Maestro·Open Server·가상 머신에 따라 보이는 정보가 다르며, Gaia Portal에서 라이선스를 활성화할 수 있습니다. 스냅샷을 가져온 뒤에는 라이선스를 다시 활성화해야 한다는 점도 기억해 둘 만합니다.

스냅샷 vs 백업 — 무엇을 언제 쓰나

이 둘을 혼동하면 복구 전략이 어긋나므로 분명히 구분해야 합니다.

Snapshot 은 시스템 설정과 제품 전체의 백업 입니다 — 파일 시스템(커스텀 파일 포함), 시스템 구성(인터페이스·라우팅·호스트 이름), Software Blade 구성, 관리 DB 까지, 사실상 root 파티션 전체와 `/var/log` 일부를 담습니다. 그래서 스냅샷은 용량이 매우 커, 백업처럼 정기적으로 스케줄링할 수 없 습니다. 스냅샷 생성 중에도 모든 프로세스는 계속 돌아 정책 집행이 끊기지 않습니다. 스냅샷은 같은 하드웨어 모델에서만 가져올 수(import) 있고, 가져온 뒤 라이선스를 다시 활성화 해야 합니다.

> 주 의
>
> 내보낸(export) 스냅샷 이미지의 이름을 절대 바꾸지 마세요. 이름을 바꾸면 그 스냅샷으로 되돌릴 수 없습니다.

스냅샷을 만들기 좋은 시점은 Gaia 설치·최초 구성 직후, 그리고 핫픽스 설치나 라우팅 변경 같은 큰 변경 직전 입니다. 스냅샷 동작은 Revert(되돌리기)·Delete·Export(압축 내보내기로 디스크 절약)·Import·View로 이뤄집니다.

반면 **System Backup** 은 더 가벼운 Gaia OS 구성과 관리 서버 DB의 백업 으로, `.tgz` 파일을 `/var/log/CPbackup/backups/` 에 저장하거나 TFTP·SCP·FTP 서버로 원격 보관합니다. 백업은 수동으로도, 스케줄로도 돌릴 수 있어 정기 보호에 알맞 습니다 — Check Point는 스냅샷 대신 System Backup을 권장 복구 수단 으로 삼고, 매일이나 매주 정기 백업을 거는 것을 권장합니다. 시스템 구성을 바로 실행 가능한 CLI 셸 스크립트로 저장 해, 장애·이전(migration) 후 빠르게 복원하는 방법도 있습니다(이전은 양쪽 Gaia 버전이 같아야 함).

복원에는 제약이 있습니다 — 백업 파일은 그것을 만든 원본과 같은 소프트웨어 버전·Jumbo Hotfix·핫픽스를 갖춘 Gaia에만 복원 할 수 있고, 게이트웨이에 복원했다면 정책을 다시 설치해야 합니다. 관리 서버에서 백업할 때는 모든 SmartConsole 클라이언트를 닫아야 백업이 시작됩니다.

하드웨어와 저장소 점검

Hardware Health Monitoring 으로 온도·전압·팬 같은 하드웨어 상태 를 Portal·CLI에서 보고, **Hardware Diagnostics** 로 진단 도구를 LCD·콘솔·Expert mode에서 돌립니다. RAID를 쓰는 장비라면 **Monitoring RAID Synchronization** 으로 RAID 동기화 상태 를 확인합니다. 디스크 구성은 **LVM**(Logical Volume Manager)으로 관리되며, `show system lvm overview` 로 논리 볼륨의 크기·사용량·조정 가능 여부 를 봅니다.

종료와 재부팅, 그리고 SmartConsole 내려받기

Shut Down 에서는 Portal의 Maintenance 메뉴나 Gaia Clish의 `halt` · `reboot` 로 시스템을 끄거나 다시 시작합니다(네트워크 관리에서 NIC 교체 전 `halt` 를 쓰던 것이 이것입니다). 또 **Download SmartConsole** 페이지에서 관리 서버에 맞는 SmartConsole 설치 파일을 내려받 을 수 있습니다.

끝으로 한 가지 OS 동작을 기억해 둘 만합니다 — Gaia에서 Linux 커널 파라미터 `accept_dad` 의 기본값은 0이지만, IPv6 중복 주소 검출(DAD) 기능 자체는 `set neighbor duplicate-detection state on` 으로 기본 활성화 되어 있습니다.

12 고급 구성과 트랜시버 모니터링

고급 구성과 트랜시버 모니터링

이 장은 일상 운영에서는 자주 만지지 않지만 알아 두면 요긴한 Gaia의 고급 구성 을 모았습니다. SSH 보안 강화, 게이트웨이의 동작을 바꾸는 Global Parameters, Gaia Portal 웹 서버 조정, 그리고 광 트랜시버(SFP/QSFP) 모니터링이 그것입니다. 세부 절차는 원문 "Advanced Gaia Configuration"·"Monitoring Transceivers" 절을 참고하세요.

Expert mode 암호 재설정과 SSH 강화

Expert mode 암호를 잊었다면 일반적인 변경 절차로는 풀 수 없고, Security Gateway·Cluster Member·Security Group에서 Expert mode 암호를 재설정하는 별도 절차(sk106490) 를 따릅니다.

보안 강화 차원에서 Gaia의 SSH 데몬이 허용하는 Cipher·MAC·KexAlgorithm을 직접 지정 할 수 있습니다. 오래되고 약한 알고리즘을 빼고 강한 것만 남기면, 관리 접속 경로인 SSH를 더 안전하게 만들 수 있습니다.

Global Parameters — 기능 기본 동작 바꾸기

게이트웨이·Cluster Member·Security Group에서는 Check Point **global parameter** 값을 바꿔 특정 기능의 기본 동작을 제어 할 수 있습니다. 여기에는 R82에서 개선된 점이 있습니다 — R81.20 이하에서는 방화벽 커널 파라미터 등을 여러 구성 파일에 흩어 적어야 했지만, 이제는 일관된 방식으로 다룰 수 있 게 됐습니다. Gaia Clish·gClish에서 파라미터를 조회·설정하거나, Expert mode에서 보고 바꾸며 'Config Point'를 제어합니다. 잘못 건드리면 동작이 달라질 수 있으니 의미를 알고 바꿔야 합니다.

그 밖에 Gaia Portal 웹 서버의 동작을 조정 하거나, Multi-Domain Server에 IPv6 주소를 구성하는 등의 특수 작업도 이 장에서 다룹니다.

트랜시버 모니터링 — 광 링크 상태 보기

Check Point 어플라이언스에 광케이블을 꽂을 때는 **SFP**(Small Form-Factor Pluggable)와 **QSFP**(Quad SFP) 트랜시버 를 씁니다. Gaia Clish 명령으로 설치된 트랜시버의 실시간 데이터 를 볼 수 있어, 광 링크 문제를 진단할 때 유용합니다.

한 인터페이스의 트랜시버는 `show interface <인터페이스> xcvr` 로 보고, 모든 인터페이스의 트랜시버를 한꺼번에 보거나 더 상세한 정보를 뽑는 명령도 있습니다. 광 신호 세기·온도 같은 값으로 케이블·트랜시버 자체의 이상 을 미리 잡아낼 수 있습니다.

13 소프트웨어 업데이트·API·스크립트

소프트웨어 업데이트·API·스크립트

마지막 장은 Gaia를 최신으로 유지하고, 자동화로 운영을 가볍게 만드는 세 가지를 묶습니다 — 소프트웨어 업데이트 엔진 **CPUSE**, 프로그램으로 Gaia를 다루는 **Gaia API**, 그리고 셸 스크립트 안에서 Check Point 명령을 돌리는 방법입니다.

CPUSE — Gaia 소프트웨어 업데이트

CPUSE(Check Point Upgrade Service Engine)는 Gaia OS와 그 위 Check Point 제품을 자동으로 업데이트해 주는 엔진 입니다. 메이저·마이너 릴리스와 핫픽스의 업데이트 패키지·전체 이미지를 다루며, 모든 과정은 **Deployment Agent**(DA) 데몬이 처리합니다.

Gaia는 설치된 버전, 장비 역할(게이트웨이·관리 서버·Standalone), 그 밖의 속성에 맞는 업데이트 패키지·이미지를 자동으로 찾아 보여 주 고, Check Point Support Center에서 내려받아 설치합니다. 제한된 대상에게만 공개되는 핫픽스는 **private package** 로 직접 목록에 추가할 수 있습니다.

업데이트를 할 때는 흐름이 있습니다. 먼저 다운로드·설치 정책(CPUSE policy)을 정 합니다 — 다운로드는 수동·자동·스케줄(매일/매주/매월/1회)로, 설치는 핫픽스는 기본적으로 자동 다운로드·설치되지만, 전체 설치·업그레이드 패키지는 반드시 수동으로 설치 해야 합니다. 완료·신규 패키지에 대한 메일 알림을 걸어 두면 좋습니다.

> 참 고
>
> 다운로드·업그레이드를 실행하기 전에 반드시 CPUSE policy가 정의돼 있어야 합니다. (자세히는 sk92449)

Gaia API — 프로그램으로 Gaia 다루기

Gaia RESTful API 는 Gaia 운영체제의 정보를 읽고 명령을 보내는 프로그래밍 통로 입니다. Gaia Portal·Gaia Clish로 하던 일을 API 명령으로도 할 수 있어 자동화에 유용합니다(다만 아직 모든 Gaia OS 설정을 API로 구성할 수 있는 것은 아님).

API는 세 가지로 호출합니다 — 서드파티 API 클라이언트로 HTTPS 연결을 통해, Gaia의 Expert mode에서 `mgmt_cli` 명령으로, 또는 SmartConsole 설치 폴더의 `mgmt_cli.exe` 로 보냅니다. 레퍼런스는 온라인 Check Point Gaia API Reference에 있고, 장비에서 직접 `https://<관리 인터페이스 IP>/gaia_docs/` 로 로컬 Gaia API 레퍼런스 를, 관리 서버에서는 `/api_docs/` 로 로컬 Management API 레퍼런스(sk174606 선행)를 볼 수 있습니다.

한 걸음 더 나아가 **Gaia API Proxy** 가 있습니다. 관리 서버에서 이 기능을 쓰면, 관리하는 게이트웨이·Cluster Member에 대고 Gaia API 명령을 대신 실행 할 수 있어, 여러 장비를 한 곳에서 프로그램으로 다루기 좋습니다.

셸 스크립트에서 Check Point 명령 돌리기

직접 셸 스크립트를 짜서 Check Point 명령을 돌리려면, 스크립트 맨 위 `#!/bin/bash` 아래에 필요한 Check Point 환경 스크립트를 `source` 로 불러와야 합니다. 그래야 명령들이 올바른 환경에서 동작합니다.

장비 종류마다 불러올 스크립트가 다릅니다. 관리 서버·Log Server·SmartEvent 서버와 일반(non-VSX) 게이트웨이·Cluster Member에서는 `/etc/profile.d/CP.sh` 하나 면 됩니다. Multi-Domain Server 에서는 `CP.sh` 에 더해 `MDSprofile.sh` · `mds_environment_utils.sh` · `sh_utilities.sh` 를 순서대로, VSX 게이트웨이·Cluster Member 에서는 `CP.sh` 와 `vsenv.sh` 를 함께 불러옵니다. 그리고 스크립트 끝에는 반드시 빈 줄(new line)을 하나 둬야 한다는 점도 잊지 마세요.

```
source /etc/profile.d/CP.sh
<필요한 Check Point 명령>
[마지막에 빈 줄 필수]
```