01 용어 정리

용어 정리

Multi-Domain Security Management은 많은 네트워크 구간을 도메인으로 나눠 한곳에서 관리하는 대규모 중앙 관리 솔루션입니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

핵심 서버 — MDS·DMS·MDLS

가장 먼저 세 서버입니다. **MDS(Multi-Domain Server)** 는 Domain Management Server들과 정책·시스템 데이터·MDM 소프트웨어를 담은 물리 서버 로, MDM 기능을 다루려면 여기에 접속합니다. **DMS(Domain Management Server)** 는 단일 도메인 환경의 Security Management Server와 기능적으로 동일 한 것으로, 한 도메인과 그 게이트웨이·정책·객체를 관리합니다. **MDLS(Multi-Domain Log Server)** 는 도메인 게이트웨이가 만든 로그를 담는 서버로, 도메인마다 **Domain Log Server** 를 둘 수 있습니다(소개).

Domain과 Global Domain

Domain(도메인) 은 한 엔티티(회사·사업부·부서·지역)에 관련된 네트워크를 정의하는 가상 객체 입니다. 예를 들어 클라우드 서비스 제공자는 고객마다, 은행은 지역마다 도메인을 둡니다. 각 도메인은 자기만의 보안 정책·네트워크 객체·설정 을 가집니다.

Global Domain(글로벌 도메인) 은 모든(또는 특정) 도메인이 공유하는 규칙·객체·설정 입니다. MDM 설치 시 자동 생성되며 삭제할 수 없습니다. 공통 정책을 **Global Policy** 로 만들어 각 도메인에 **Global Assignment** 로 배정 하면, 도메인별 로컬 정책과 합쳐집니다(글로벌 관리).

관리·운영 용어

도메인을 다루는 도구는 SmartConsole입니다. MDS에 접속하면 **Multi-Domain view**로 도메인·서버를 관리 하고, 특정 DMS에 접속하면 그 도메인의 정책·객체 를 다룹니다. **Gateways & Servers view** 에서는 환경의 모든 게이트웨이·DMS·Log Server를 한눈에 봅니다.

High Availability(고가용성) 는 두 수준으로 동작합니다 — **MDS HA**(여러 MDS가 모두 Active로 동기화) 와 **DMS HA**(한 도메인의 DMS를 여러 MDS에 두어 Active/Standby 이중화·부하분산) 입니다(고가용성).

프로세스·환경 용어

MDS·DMS는 여러 프로세스로 돌아갑니다 — `cpd`(정책 설치·SIC 등 범용 데몬), `cpca`(인증기관 관리), `fwd`(로그 서버), `cpm` · `postgres` · `solr`(관리 핵심) 입니다(아키텍처와 프로세스). 각 컨텍스트(MDS/DMS)는 `$FWDIR` · `$MDSDIR` · `$CPDIR` 같은 환경 변수 로 자기 설치 경로를 가리키며, `mdsenv` 명령으로 컨텍스트를 전환합니다(명령줄 참조).

02 Multi-Domain 소개

Multi-Domain 소개

Security Management 가이드가 하나의 관리 서버로 한 환경을 다루는 방법이라면, **Multi-Domain Security Management(MDM)** 는 여러 네트워크 구간을 "도메인"으로 나눠 한곳에서 대규모로 관리 하는 솔루션입니다. 이 장은 그 구성요소와 큰 그림을 잡습니다.

왜 도메인으로 나누나

MDM은 보안 요구가 제각각인 많은 네트워크 구간을 가진 대규모·분산 환경 을 위한 것입니다. 지역·사업부·보안 기능별로 **Domain** 을 만들 어 보안을 강화하고 관리를 단순화합니다. 각 도메인은 자기만의 보안 정책·네트워크 객체·설정 을 가지고, **Global Domain** 으로 모든(또는 특정) 도메인에 공통으로 적용할 정책·객체 를 둡니다.

세 가지 핵심 서버

MDM 환경은 세 서버로 돌아갑니다.

MDS(Multi-Domain Server) 는 DMS들과 정책·시스템 데이터·MDM 소프트웨어를 담은 물리 서버 입니다. 여기에 접속하면 DMS·Global Policy·관리자·로그·시스템 설정 을 다룹니다. **DMS(Domain Management Server)** 는 단일 도메인 환경의 Security Management Server와 같은 것 으로, 한 도메인의 게이트웨이·정책·객체·블레이드를 관리합니다 — SmartConsole로 직접 접속해 다룹니다. **MDLS(Multi-Domain Log Server)** 는 도메인 게이트웨이의 로그를 담 으며, 도메인마다 Domain Log Server를 둬 로그 트래픽을 분리해 처리량을 높 입니다.

!두 MDS·두 도메인 구성 예 *① London MDS(London용 Active DMS + Tokyo용 Standby DMS) ② MDLS(London·Tokyo Domain Log Server) ③ Tokyo MDS(Tokyo용 Active DMS + London용 Standby DMS) ④ Tokyo 네트워크 ⑤ London 네트워크 ⑥ 인터넷*

위 예처럼 MDS를 여러 사이트에 두고 서로 동기화 해 고가용성·부하분산을 이룹니다(고가용성).

SmartConsole로 관리하기

SmartConsole이 MDM도 다룹니다. MDS에 로그인하면 **Multi-Domain view** 로 MDS·도메인·시스템 객체를 관리하고, 특정 도메인을 고르면 그 DMS의 정책·규칙·객체를 다룹니다. Multi-Domain view에서 도메인을 우클릭해 **Connect to Domain Server** 로 바로 들어갈 수도 있습니다.

> 참 고
>
> HA 환경에서는 Active DMS(검은 아이콘)에서만 변경 할 수 있습니다. Standby DMS(흰 아이콘)에 접속하면 SmartConsole이 읽기 전용으로 열립니다.

이 가이드는 MDM 고유 기능 만 다룹니다. 정책·Rule Base·객체 작업은 Security Management 가이드, 로그·모니터링은 Logging and Monitoring 가이드를 참고하세요.

03 아키텍처와 프로세스

아키텍처와 프로세스

MDM이 어떻게 돌아가는지 — 어떤 프로세스가 떠 있고, 컨텍스트가 어떻게 나뉘는지 — 를 정리합니다. 문제 해결이나 CLI 작업의 바탕이 됩니다.

Check Point Registry

각 서버는 자기 **Registry** 를 가집니다. `$CPDIR/registry/HKLM_registry.data` 에 Check Point 제품의 설치·버전 정보 가 담기며, MDS·MDLS·DMS·Log Server가 각각 자기 레지스트리 를 갖습니다. `$CPDIR` 환경 변수가 각 컨텍스트의 레지스트리 위치를 가리킵니다.

서버 프로세스

프로세스는 두 수준으로 나뉩니다.

MDS 수준 프로세스 는 MDS/MDLS 한 대에 인스턴스 하나 씩 돕니다 — `cpd` (정책 설치·온라인 업데이트·SIC 인증서 등 범용 데몬), `cpca` (인증 기관 관리), `fwd` (Audit Log 서버), `fwm` (레거시 관리 메인) 입니다. MDS가 제대로 동작하려면 `cpm` · `postgres` · `solr` 와 함께 떠 있어야 합니다(단 Domain Log Server처럼 `cpca` 가 못 도는 경우는 예외).

DMS 수준 프로세스 는 DMS마다 별도 인스턴스 가 돕니다 — `cpd` , `cpca` (DMS 전용), `fwd` (로그 서버), `fwm` , 그리고 SmartLSM 게이트웨이 상태 수집용 `status_proxy` 입니다. DMS에서는 `cpca` · `fwd` · `fwm` 이 항상 떠 있어야 합니다.

부팅 시 MDS 프로세스는 `/etc/init.d/firewall1` 스크립트(`/etc/rc3.d` 의 `S95firewall1` 링크) 로 자동 시작됩니다.

환경 변수와 컨텍스트

MDS 프로세스는 설치 경로·관리 IP·초기화 데이터를 담은 표준 환경 변수 를 씁니다. 핵심은 컨텍스트마다 다른 경로입니다 — `$MDSDIR` (MDS 설치, `/opt/CPmds-R82`), `$FWDIR` (MDS에서는 `$MDSDIR` 과 같고, DMS에서는 그 도메인의 `/opt/CPmds-R82/customers/<DMS>/CPsuite-R82/fw1`), `$CPDIR` (SVN Foundation), `$PGDIR` (PostgreSQL) 입니다.

환경 변수는 `.CPprofile.sh` (Bourne)· `.CPprofile.csh` (C-Shell) 스크립트가 정의합니다. 핵심은 어느 컨텍스트(MDS인지 특정 DMS인지)에 있느냐에 따라 `$FWDIR` 등이 다른 곳을 가리킨다 는 점입니다 — 그래서 명령줄 참조에서 보듯 `mdsenv [DMS]` 명령으로 컨텍스트를 전환 한 뒤 명령을 실행합니다. 프로세스·데몬의 상세는 sk97638을 참고하세요.

04 배포 계획

배포 계획

MDM을 어떻게 깔지 — 몇 개의 MDS를 어디에 두고 어떻게 동기화할지 — 를 계획하는 장입니다. 화면 절차보다 배포 형태의 선택지를 잡습니다.

배포 형태

대표적인 두 형태가 있습니다.

Multi-Site High Availability 는 대기업이 여러 사이트(때로 다른 나라)에 MDS를 두고 서로 계속 동기화 하는 형태입니다. 각 MDS·MDLS가 원격 피어와 지속 동기화 해, 한 사이트가 죽어도 다른 사이트에서 관리가 이어집니다(고가용성).

Single Site Deployment 는 한 사이트에 MDS를 두는 단순한 형태입니다. 규모가 작거나 단일 데이터센터 환경에 맞습니다.

계획 시 고려할 점

배포를 효율적으로 하려면 몇 가지를 미리 정합니다 — MDS·MDLS의 수와 위치, 도메인 수와 각 도메인의 DMS 배치, HA로 둘 도메인과 그 Standby DMS의 위치, 로그를 담을 MDLS 입니다. Security Management 가이드의 사이징 원칙(전용 서버·전용 로그 서버)이 여기서도 그대로 적용되며, 규모가 클수록 로그 트래픽을 MDLS로 분리 하는 것이 중요합니다.

설치의 큰 줄기

설치 자체는 설치·업그레이드 가이드가 자세히 다룹니다. MDM 관점의 큰 줄기는 MDS 설치 → (HA면) 추가 MDS 설치·동기화 → 도메인과 DMS 생성(도메인 관리) → Global Domain·정책 구성(글로벌 관리) → 관리자·권한 정의(관리자·권한) 입니다. 정리하면, 배포 계획의 핵심은 사이트·MDS·MDLS의 배치와 도메인별 DMS·HA 구성을 규모에 맞게 설계 하는 것입니다(세부 절차는 원문 해당 절과 설치 가이드 참고).

05 도메인 관리

도메인 관리

Domain 은 MDM의 기본 단위입니다. 이 장은 도메인을 만들고 그 DMS를 다루는 흐름을 정리합니다.

Domain과 DMS

Domain Management Server(DMS) 는 단일 도메인 환경의 Security Management Server와 기능적으로 동일 합니다. SmartConsole로 DMS에 직접 접속해 그 도메인이 관리하는 게이트웨이, 도메인 보안 정책·규칙, 도메인 시스템 객체(서비스·사용자·VPN Community), 도메인 블레이드 설정 을 다룹니다.

즉 한 도메인 안에서의 작업은 일반 Security Management와 똑같 고, MDM은 그 위에 "여러 도메인을 한곳에서" 라는 층을 더한 것입니다.

도메인 만들기

새 도메인은 Multi-Domain view에서 만듭니다. 큰 줄기는 도메인 이름·정의 → 그 도메인의 DMS를 어느 MDS에 둘지 지정 → (HA면) 다른 MDS에 Standby DMS 추가 → DMS 초기화·SIC 입니다. 만든 도메인의 DMS에 접속하면 그 도메인만의 SmartConsole 환경 이 열려, 게이트웨이를 추가하고 정책을 짭니다.

HA 환경에서는 한 도메인의 DMS를 여러 MDS에 두어 이중화·부하분산하며, Active DMS에서만 변경 하고 Standby는 읽기 전용입니다.

도메인 운영

도메인을 운영하며 다루는 일들 — 도메인 추가·삭제, DMS 시작·정지, 도메인 간 이동, 백업 등 — 이 이 장에 모여 있습니다. 각 도메인은 독립된 정책·객체 를 가지므로, 한 도메인의 변경이 다른 도메인에 영향을 주지 않습니다. 모든 도메인에 공통으로 적용할 것은 Global Domain으로 다룹니다. 세부 절차는 원문 해당 절을 참고하세요.

06 글로벌 관리 — Global Domain·Policy

글로벌 관리 — Global Domain·Policy

도메인마다 정책을 따로 짜면 공통 규칙을 매번 중복 해야 합니다. **Global Domain** 은 모든(또는 특정) 도메인이 공유하는 규칙·객체·설정 으로 이를 해결합니다.

Global Domain

Global Domain 은 MDM 설치 시 자동 생성되는, 도메인들이 공유하는 규칙·객체·설정의 모음 입니다. 삭제할 수 없고 추가로 만들 수도 없 습니다(하나뿐). Global Domain에 접속하려면 Multi-Domain view에서 들어갑니다.

전역 규칙·객체·설정은 **global configuration** 으로 묶이며, 한 구성에는 하나의 **Global Access Control Policy**(모든 도메인에 공통으로 적용할 접근 규칙) 등이 들어갑니다. 예를 들어 회사 전체에 공통인 "사내망 차단" 규칙 을 Global Policy에 한 번 만들면 모든 도메인에 퍼집니다.

Global Policy와 Global Assignment

전역 정책은 **Global Policy** 로 만들어 각 도메인에 **Global Assignment** 로 배정 합니다. 배정하면 그 도메인의 로컬 정책과 전역 정책이 합쳐져 게이트웨이에 설치됩니다 — 보통 전역 규칙이 로컬 규칙보다 위·아래의 정해진 자리에 들어가, 공통 규칙은 전역에서·도메인 고유 규칙은 로컬에서 관리하는 분업이 가능합니다.

전역에서 함께 관리하는 것으로 IPS Protections·Application & URL Filtering 데이터베이스 업데이트 도 있어, 한곳에서 갱신해 모든 도메인에 반영합니다.

글로벌 vs 로컬

핵심은 분업입니다 — 회사 전체 공통 정책·객체는 Global Domain에서, 도메인 고유 정책은 각 DMS에서 관리합니다. 전역 정책의 예외 처리는 Exceptions에서, 전역으로 적용한 규칙이 도메인마다 조금씩 달라야 할 때의 처리도 함께 다룹니다. 세부 절차(Global Policy 생성·할당·갱신)는 원문 해당 절을 참고하세요.

07 예외(Exceptions)

예외(Exceptions)

전역 정책을 강하게 두되 특정 대상만 예외로 다뤄야 할 때가 있습니다. 이 장은 예외와 예외 그룹, 그리고 글로벌 예외와 로컬 예외의 차이를 정리합니다.

예외 규칙

예외(Exception) 는 규칙에 직접 더해, Protected Scope의 특정 객체에 대해 그 규칙과 다른 Action을 적용 하는 것입니다. 핵심 원칙은 예외는 보통 특정 보호의 집행 수준을 "낮추는" 용도이지 "높이는" 용도가 아니 라는 점입니다(Threat Prevention의 예외와 같은 개념).

예를 들어 R&D 네트워크 보호가 Prevent 프로파일에 포함 되어 있는데, 특정 보호가 R&D의 정상 트래픽을 오탐으로 막는다면, 그 보호만 R&D 범위에서 예외 처리 해 풀어 줍니다.

글로벌 예외 vs 로컬 예외

MDM에서는 예외도 두 수준입니다. **글로벌 예외** 는 Global Domain에서 정의해 여러 도메인에 공통으로 적용되고, **로컬 예외** 는 개별 도메인에서 적용됩니다. 공통으로 풀어 줄 예외는 전역에서, 도메인 고유 예외는 로컬에서 관리하는 분업이 글로벌 관리의 정책 분업과 같은 결로 동작합니다.

예외를 묶어 관리하려면 **예외 그룹(Exception Group)** 을 만들어 여러 예외를 한 묶음으로 여러 규칙에 재사용 합니다.

정리하면, 예외는 강한 전역 정책의 "구멍"을 필요한 곳에만 정밀하게 내는 장치이며, 글로벌·로컬 두 수준으로 공통 예외와 도메인 고유 예외를 나눠 다룹니다. 세부 절차는 원문 해당 절을 참고하세요.

08 관리자·권한 관리

관리자·권한 관리

여러 도메인을 여러 사람이 나눠 관리하므로, 누가 어느 도메인의 무엇을 다룰 수 있는지 를 세밀하게 정하는 것이 중요합니다. 이 장은 관리자와 권한 프로파일을 정리합니다.

무엇을 관리하나

MDM 환경의 관리자는 다양한 대상을 다룹니다 — MDS·MDLS, 도메인·DMS, HA 구성·동기화, 도메인 게이트웨이·네트워크·객체, 도메인 보안 정책, Global Domain 입니다. 핵심은 이 넓은 범위를 권한으로 쪼개 각자에게 필요한 만큼만 주는 것입니다.

권한의 두 축 — 범위와 역할

MDM의 권한은 "어느 도메인을"× "무엇을 할 수 있는지" 로 나뉩니다.

범위(scope) 로는 모든 도메인을 다루는 관리자(Superuser 등), 특정 도메인만 다루는 관리자 를 나눌 수 있습니다 — 예를 들어 London 도메인 담당자는 London DMS만 관리하게 제한합니다. **역할(permission profile)** 로는 읽기 전용/읽기·쓰기, 정책·객체·설정별 권한 을 정합니다(Security Management 가이드의 권한 프로파일과 같은 개념을 도메인 단위로 확장).

이렇게 도메인별로 담당 관리자를 분리 하면, 한 도메인의 관리자가 다른 도메인을 건드리지 못하게 해 대규모 환경에서 책임과 보안을 함께 지킵니다.

관리자 계정 만들기·바꾸기

관리자 계정은 Multi-Domain view에서 이름·인증 방식(인증서·암호·SAML 등)·범위·권한 프로파일을 지정 해 만듭니다. 계정을 만들고 바꾸는 세부 절차(인증서 발급, 권한 배정 등)는 Security Management 가이드의 방식과 같으며, MDM은 거기에 도메인 범위 제한 을 더한 것입니다. 세부는 원문 해당 절을 참고하세요.

09 VPN과 Multi-Domain

VPN과 Multi-Domain

MDM 환경에서도 VPN을 쓰는데, 여러 도메인에 걸친 VPN 이라는 특수성이 있습니다. 이 장은 그 요점을 정리합니다.

도메인 안의 VPN과 전역 VPN

한 도메인 안에서의 VPN은 단일 환경과 똑같 습니다 — Site-to-Site VPN·Remote Access VPN 가이드의 방식대로 그 도메인의 DMS에서 VPN Community를 만들고 정책을 짭니다.

MDM 고유의 특징은 여러 도메인에 공통으로 적용할 VPN 설정을 Global Domain에서 다룰 수 있다는 점입니다. 전역 VPN Community나 공통 VPN 객체를 Global Policy로 만들어 여러 도메인이 공유 하게 할 수 있습니다.

인증서와 신뢰

VPN의 바탕인 인증서는 각 DMS의 ICA(Internal Certificate Authority) 가 발급합니다 (아키텍처에서 본 `cpca` 프로세스). 도메인 간이나 외부와 VPN을 맺을 때는 인증서·신뢰 관계를 도메인 단위로 관리하며, 외부 게이트웨이와의 연동은 Site-to-Site VPN 가이드의 외부 게이트웨이 방식을 따릅니다.

정리하면, VPN 자체의 구성은 단일 환경과 같되, MDM에서는 도메인별 VPN과 Global Domain의 공통 VPN을 함께 다룬다는 점이 핵심입니다. 자세한 VPN 구성은 Site-to-Site VPN·Remote Access VPN 가이드를, MDM 특유의 세부는 원문 해당 절을 참고하세요.

10 고가용성(High Availability)

고가용성(High Availability)

MDM은 대규모 환경의 중추이므로 관리 서버가 죽어도 관리가 끊기지 않아야 합니다. MDM의 High Availability는 두 수준 으로 동작합니다.

두 수준의 HA

MDS High Availability 는 둘 이상의 완전히 동기화된 MDS를 쓰는 Active/Active 이중화 입니다. 모든 MDS가 Active 라, primary든 secondary든 로그인해 작업할 수 있습니다. 한 MDS가 죽어도 다른 MDS에서 관리가 이어집니다.

DMS High Availability 는 도메인 단위의 이중화이자 부하분산 입니다. 한 도메인의 DMS를 둘 이상의 MDS에 만들 어 완전히 동기화하면, 하나가 Active이고 나머지는 Standby 가 됩니다(소개의 London/Tokyo 예처럼, 한 MDS의 Active DMS가 다른 MDS에서는 Standby).

동기화와 변경 규칙

동기화된 서버들은 같은 정책·규칙·사용자·객체·시스템 설정 을 갖습니다. 핵심 규칙은 Active DMS에서만 변경 할 수 있다는 것입니다(소개) — Active는 검은 아이콘, Standby는 흰 아이콘 으로 표시되고, Standby에 접속하면 SmartConsole이 읽기 전용으로 열립니다. 변경 후 동기화로 Standby에 전파 됩니다.

Security Management 가이드의 HA가 단일 환경의 Primary/Standby였다면, MDM은 MDS 수준(Active/Active)과 DMS 수준(Active/Standby)이 겹쳐 더 정교한 이중화를 이룹니다. 동기화 모니터링·changeover·충돌(collision) 처리 같은 세부 절차는 원문 해당 절을 참고하세요. 정리하면, MDS는 모두 Active로 서로 받쳐 주고, 각 도메인의 DMS는 Active/Standby로 이중화 되어, 어느 한 서버가 빠져도 전체 관리가 살아 있습니다.

11 로깅·모니터링

로깅·모니터링

MDM 환경에서도 로그·모니터링을 다루는데, 여러 도메인의 로그를 어떻게 모으고 보는지 가 핵심입니다. 이 장은 MDM에 직접 관련된 부분만 정리하고, 전체 개념은 Logging and Monitoring 가이드로 넘깁니다.

통합된 로깅·모니터링

R80부터 로깅·이벤트 관리·리포팅·모니터링이 그 어느 때보다 긴밀하게 통합 되었습니다. 로그가 정책 규칙과 밀접하게 연결 되어 특정 규칙을 클릭하면 관련 로그를 바로 볼 수 있고, 자유 텍스트 검색으로 수백만 건의 로그에서 몇 초 만에 결과를 찾습니다. SmartReporter·SmartEvent 기능도 SmartConsole에 통합되었습니다.

뷰는 두 곳에서 봅니다 — SmartConsole의 **Logs & Events** 와 **SmartView Web Application**(`https://<서버 IP>/smartview/`) 입니다.

MDM에서의 로그 구조

MDM 특유의 점은 도메인별 로그 분리 입니다. 소개에서 본 **MDLS(Multi-Domain Log Server)** 가 도메인마다 Domain Log Server를 담 아, 로그 트래픽을 도메인별로 격리해 처리량을 높 입니다. 도메인 게이트웨이는 자기 Domain Log Server로 로그를 보내고, 관리자는 자기 권한 범위(관리자·권한)의 도메인 로그만 봅니다.

고가용성 환경에서는 Active DMS·Domain Log Server가 로그를 다루며, 여러 MDLS를 둬 로그도 이중화할 수 있습니다.

정리하면, MDM의 로깅은 단일 환경과 도구·개념은 같되, 도메인별로 Domain Log Server에 로그를 분리해 모으고 권한 범위대로 본다 는 점이 다릅니다. 로그·뷰·리포트·SmartEvent의 전체 내용은 Logging and Monitoring 가이드를 참고하세요.

12 API로 관리

API로 관리

MDM도 API로 자동화 할 수 있습니다. Security Management 가이드의 API와 같은 토대 위에, 여러 도메인을 다룬다 는 점만 더해집니다.

API Server와 컨텍스트

MDS·DMS에서 **API Server** 가 돌아, API 요청으로 구성·운영을 자동화 합니다. 핵심은 어느 컨텍스트에서 명령을 실행하느냐 입니다 — 아키텍처에서 본 대로, `mdsenv [DMS 이름/IP]` 로 특정 도메인 컨텍스트로 전환한 뒤 그 도메인에 대한 API·명령을 실행합니다.

도구는 단일 환경과 같습니다 — `mgmt_cli` (Gaia·SmartConsole 포함)와 Web Services API(`/web_api/`) 입니다. 예를 들어 여러 도메인에 같은 객체·규칙을 한 번에 배포 하거나, 도메인을 스크립트로 대량 생성 하는 작업에 API가 큰 힘이 됩니다.

권한과 활용

API를 쓰려면 관리자의 권한 프로파일에 Management API 권한 이 있어야 하고(관리자·권한), 그 관리자의 도메인 범위 안에서만 API가 동작합니다. 이렇게 범위 제한 + API 로, 대규모 다중 도메인 환경을 안전하게 자동화합니다.

자세한 API 구성(API Server 활성화·접근 설정·API 키)은 Security Management 가이드의 API와 같으며, 전체 명령은 Check Point Management API Reference를 참고하세요.
정리하면, MDM의 API는 단일 환경 API에 "컨텍스트 전환(mdsenv)과 도메인 범위"를 더한 것입니다.

13 Implied Rule·커널 테이블 구성

Implied Rule·커널 테이블 구성

게이트웨이에 정책을 설치할 때, 관리자가 명시한 규칙 외에 시스템이 자동으로 더하는 규칙(Implied Rule)과 커널 동작 이 있습니다. 이 장은 이를 조정하는 방법을 정리합니다.

정책 설치 시 생기는 파일

관리자가 SmartConsole에서 보안 정책·검사 설정을 구성하면, 정책 설치 때 관리 서버가 해당 파일들을 만들어 대상 게이트웨이로 전송 합니다. 이 파일들은 SmartConsole의 보안 정책과 Global Properties 를 바탕으로 생성됩니다.

Implied Rule과 커널 테이블

Implied Rule(암묵 규칙) 은 관리자가 명시하지 않아도 시스템이 자동으로 더하는 규칙 입니다 — 예를 들어 Identity Sharing·VPN 제어 연결에서 본 것처럼, Check Point 컴포넌트 간 필수 통신을 허용하는 규칙들입니다. **커널 테이블** 은 게이트웨이 커널이 상태·연결을 다루는 내부 자료구조입니다.

MDM 환경에서는 이런 Implied Rule·커널 동작을 구성 파일로 조정 할 수 있습니다. 관리자가 Global Properties나 전용 구성 파일을 편집하면, 정책 설치 시 그 설정이 반영된 파일이 게이트웨이로 내려갑니다. 이는 기본 동작으로 부족하거나 특수한 통신을 허용·차단 해야 할 때 쓰는 고급 조정입니다.

정리하면, 이 장은 정책 설치가 만들어 내는 Implied Rule·커널 설정을 구성 파일로 세밀하게 조정 하는 방법입니다. 대부분 깊은 튜닝이므로, 구체적 파일·파라미터는 Check Point Support의 SK 문서와 함께 신중히 다루고 세부는 원문 해당 절을 참고하세요.

14 명령줄 참조

명령줄 참조

MDM을 명령줄로 다루는 도구를 정리합니다. 원문에서 가장 방대한 부분(440여 페이지)이 이 명령 참조인데, 모두 옮기기보다 어디서 무엇을 찾는지 를 짚습니다.

컨텍스트 전환이 먼저 — mdsenv

MDM CLI의 출발점은 **컨텍스트** 입니다. 아키텍처에서 봤듯 MDS 컨텍스트와 각 DMS 컨텍스트는 `$FWDIR` 등 환경 변수가 다른 곳을 가리 킵니다. 그래서 명령을 실행하기 전에 `mdsenv [DMS 이름/IP]` 로 원하는 컨텍스트로 전환 합니다 — 인자 없이 `mdsenv` 만 하면 MDS 컨텍스트, DMS를 지정하면 그 도메인 컨텍스트가 됩니다.

주요 명령 영역

MDM 운영 명령 전체는 **R82 CLI Reference Guide** 에 정리되어 있습니다. 대표 영역은 이렇습니다.

`mdsstart` · `mdsstop` · `mdsstat` 로 MDS·DMS를 시작·정지·상태 확인 하고, `mdsconfig` 로 MDS를 구성 합니다. `mds_backup` · `mds_restore` 로 MDM 환경을 백업·복원 하며(Security Management 가이드의 HA에서도 언급), 단일 환경에서 본 `cpstart` · `cpstop` · `cpconfig` · `fwm` · `api` 같은 명령도 컨텍스트 안에서 그대로 씁니다.

> 참 고
>
> MDM 명령은 반드시 올바른 컨텍스트(mdsenv)에서 실행 해야 합니다. MDS 명령을 DMS 컨텍스트에서 실행하거나 그 반대면 의도와 다르게 동작할 수 있습니다.

정리하면, 일상 관리는 SmartConsole로 하되 시작·정지·백업·자동화는 `mdsenv` 로 컨텍스트를 잡고 `mds*` 계열· `cp*` · `mgmt_cli` 명령 으로 내려가며, 그 방대한 명령 사전은 R82 CLI Reference Guide 가 담당합니다.