01 용어 정리

용어 정리

CloudGuard Controller는 클라우드·데이터센터의 객체를 자동으로 배워 보안 정책에 반영 하는 기능입니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

핵심 개념

CloudGuard Controller 는 Security Management Server의 한 구성요소 로, 공용·온프레미스 클라우드 환경의 객체를 동적으로 배워 정책에 반영합니다(소개).

핵심 동작이 **Data Center 연동** 입니다 — 벤더의 API로 클라우드(Data Center)와 신뢰 관계를 맺고, 정기적으로 폴링(polling)해 객체 변화를 감지 합니다. 배우는 객체는 서브넷, 보안 그룹(Security Group), 가상 머신(VM), IP 주소, 태그(tag) 등입니다.

이렇게 배운 객체는 **Data Center Object(데이터센터 객체)** 가 되어 정책 규칙에 쓰입니다. 핵심은 클라우드에서 객체가 바뀌면(IP 변경·VM 추가 등) 그 변화가 자동으로 게이트웨이에 반영 된다는 점입니다 — 관리자가 일일이 정책을 고치지 않아도 됩니다.

객체와 쿼리

Data Center Query Object 는 태그·이름 같은 속성으로 클라우드 객체를 동적으로 묶는 객체입니다(데이터센터 서버 연동). 예를 들어 ="tag=web인 모든 VM"== 을 한 객체로 묶으면, 그 조건에 맞는 VM이 늘고 줄 때 객체도 자동으로 갱신됩니다 — Identity Awareness·SmartProvisioning의 Dynamic Object와 비슷한 발상입니다.

지원 환경과 운영

CloudGuard Controller는 다양한 클라우드·가상화 플랫폼 을 지원합니다 — AWS, Microsoft Azure, GCP, Cisco ACI·ISE, Kubernetes, OCI, Nutanix, Nuage, OpenStack, VMware 등입니다(지원 데이터센터).

운영에는 Data Center Updates(객체 갱신), 로그·이벤트, Status, SNMP Trap, SmartTask(이벤트 기반 자동화) 가 쓰이고(모니터링), Identity Awareness 연동으로 신원 정보까지 결합할 수 있습니다.

02 CloudGuard Controller 소개

CloudGuard Controller 소개

클라우드에서는 IP·VM이 수시로 바뀝 니다. 그때마다 방화벽 정책을 손으로 고치는 건 불가능하죠. **CloudGuard Controller** 는 클라우드 객체의 변화를 자동으로 배워 정책에 반영 해 이를 해결합니다.

CloudGuard Controller가 하는 일

CloudGuard Controller는 Security Management Server의 한 구성요소 로, 공용·온프레미스 환경을 하나의 통합 관리로 다룹니다. 핵심은 데이터센터의 객체와 속성(서브넷·보안 그룹·VM·IP·태그)의 변화를 동적으로 배운다 는 것입니다.

동작 흐름은 이렇습니다.

!CloudGuard Controller 동작 *① CloudGuard Controller가 클라우드 환경과 신뢰 관계를 맺음 ② 벤더 API로 클라우드에 연결해 정기적으로 변화를 폴링 ③ 클라우드의 변화가 Controller로 전달됨 ④ Controller가 정책 규칙의 객체·속성 업데이트를 게이트웨이에 push*

즉 벤더 API로 데이터센터와 신뢰를 맺고 → 정기 폴링으로 변화를 감지 → 그 변화를 자동으로 게이트웨이 정책에 반영 합니다. 관리자는 ="tag=web인 VM 허용" 같은 규칙을 한 번 만들 면, 그 조건에 맞는 VM이 늘고 줄어도 정책이 알아서 따라== 갑니다.

활용 사례

대표 사례는 클라우드의 동적 자원을 정책에 자동 반영 하는 것입니다 — 예를 들어 오토스케일링으로 VM이 추가될 때마다, 그 VM이 태그·보안 그룹 기준으로 정책에 자동 포함 되게 합니다. 그래서 빠르게 변하는 클라우드 환경에서도 정책이 항상 최신 으로 유지됩니다.

What's New

R82 CloudGuard Controller에는 AWS·VMware용 새 기능 등이 추가되었습니다. 클라우드 플랫폼별 최신 지원은 지원 데이터센터에서 다룹니다.

정리하면, CloudGuard Controller는 클라우드 객체의 변화를 API로 배워 정책에 자동 반영 해, 수동 관리 없이 동적 클라우드 환경을 보호합니다. 실제 시작은 시작하기에서 이어집니다.

03 시작하기와 지원 게이트웨이

시작하기와 지원 게이트웨이

CloudGuard Controller를 쓰기 시작하는 전제와 큰 흐름 을 정리합니다.

큰 흐름

CloudGuard Controller는 Security Management Server에 내장 되어 있어 별도 설치가 필요 없습니다. 쓰기 시작하는 큰 줄기는 ① 데이터센터(클라우드)와 연동 설정 → ② 데이터센터 객체·Query Object 정의 → ③ 정책 규칙에서 그 객체 사용 → ④ 정책 설치 입니다(데이터센터 서버 연동).

지원 게이트웨이

CloudGuard Controller가 배운 객체를 push할 대상 게이트웨이 에는 지원 버전·조건이 있습니다. Data Center 객체를 정책에 쓰려면 그 정책을 받는 게이트웨이가 이를 지원 해야 하므로, 소개에서 본 "자동 push"가 동작하려면 지원 게이트웨이인지 먼저 확인합니다.

어떤 클라우드·가상화 플랫폼을 연동할 수 있는지는 지원 데이터센터에서, 신원 정보까지 결합하려면 Identity Awareness 연동을 봅니다. 지원 게이트웨이 목록·버전 조건의 세부는 원문 해당 절을 참고하세요.

04 Identity Awareness 연동

Identity Awareness 연동

CloudGuard Controller가 배운 클라우드 객체에 신원 정보까지 결합 하려면 Identity Awareness와 연동합니다. 이 장은 그 연동을 정리합니다.

Identity Awareness 블레이드 활성화

CloudGuard Controller의 일부 기능은 Identity Awareness 블레이드를 켜야 동작합니다. 게이트웨이에서 Identity Awareness를 활성화 하면, 클라우드에서 배운 객체와 신원(사용자·컴퓨터) 정보를 함께 정책에 쓸 수 있습니다.

이렇게 하면 클라우드 자원(VM·서브넷)과 그 자원을 쓰는 사용자 신원을 결합한 정책 이 가능해집니다 — 예를 들어 "특정 클라우드 환경의 특정 그룹 사용자만 허용" 같은 규칙입니다.

Identity Sharing 지원

Identity Awareness의 Identity Sharing도 지원합니다. 한 게이트웨이(PDP)가 취득한 신원을 다른 게이트웨이(PEP)와 공유 하는 구조를, CloudGuard Controller 환경에서도 활용할 수 있습니다. 그래서 클라우드 객체 정보와 공유된 신원 정보가 함께 여러 게이트웨이에 걸쳐 일관되게 적용됩니다.

정리하면, CloudGuard Controller에 Identity Awareness를 연동하면 클라우드 객체 + 신원을 결합한 정책 을 만들 수 있고, Identity Sharing으로 그 신원을 여러 게이트웨이가 공유합니다. 세부 활성화 절차는 원문 해당 절과 Identity Awareness 가이드를 참고하세요.

05 지원 데이터센터 (클라우드 플랫폼)

지원 데이터센터(클라우드 플랫폼)

CloudGuard Controller는 다양한 퍼블릭 클라우드·가상화·SDN 플랫폼 과 연동합니다. 이 장은 어떤 플랫폼을 지원하고 연동의 공통 원리가 무엇인지를 정리합니다(플랫폼별 세부 설정은 원문 해당 절 참고).

연동의 공통 원리

플랫폼은 제각각이지만 연동 원리는 같습니다(소개). 각 플랫폼의 API로 신뢰 관계(인증)를 맺고 → 정기 폴링으로 객체·속성을 가져와 → Data Center 객체로 정책에 반영 합니다.
그래서 각 플랫폼 절은 그 플랫폼에서 필요한 인증 정보(API 키·서비스 계정·자격 증명)와 연결 방법 을 다룹니다.

지원 플랫폼

지원 범위가 넓습니다. **퍼블릭 클라우드** 로는 **AWS**(Amazon Web Services), **Microsoft Azure**, **GCP**(Google Cloud Platform), **OCI**(Oracle Cloud Infrastructure) 를 지원합니다. **컨테이너·가상화** 로는 **Kubernetes**, **VMware Servers**(vCenter 등), **Nutanix** 를 지원합니다.

네트워크·SDN·신원 쪽으로는 **Cisco ACI**(Application Centric Infrastructure), **Cisco ISE**(Identity Services Engine), **Nuage VSP**(Virtualized Services Platform), **OpenStack** 을 지원합니다. 특히 Cisco ISE 연동은 신원 기반 정보를 가져오는 데 쓰입니다(Identity Awareness 연동과 맞물림).

플랫폼별 연동의 요점

각 플랫폼 연동의 핵심은 그 플랫폼이 제공하는 API와 인증 방식 입니다 — 예를 들어 AWS는 IAM 자격 증명·역할, Azure는 앱 등록·서비스 주체, GCP는 서비스 계정 키, VMware는 vCenter 자격 증명 을 씁니다. 연동을 맺으면 그 플랫폼의 VM·서브넷·보안 그룹·태그 등이 Data Center 객체로 들어와, 클라우드가 바뀔 때 정책이 자동으로 따라갑니다.

정리하면, CloudGuard Controller는 주요 퍼블릭 클라우드(AWS·Azure·GCP·OCI), 가상화·컨테이너(VMware·K8s·Nutanix), SDN·신원(Cisco ACI/ISE·Nuage·OpenStack) 을 같은 원리(API 신뢰 → 폴링 → 객체 반영)로 연동합니다. 플랫폼별 인증·연결 절차의 세부는 원문 해당 절을 참고하세요.

06 데이터센터 서버 연동

데이터센터 서버 연동

지원 플랫폼과 실제로 연동해 객체를 정책에 가져오는 방법을 정리합니다.

데이터센터 서버에 연결하기

연동의 시작은 **Connecting to a Data Center Server** 입니다 — SmartConsole에서 Data Center Server 객체를 만들고, 그 플랫폼의 인증 정보(API 키·서비스 계정·자격 증명)를 입력해 신뢰를 맺 습니다(소개). 연결되면 CloudGuard Controller가 정기적으로 그 환경을 폴링해 객체를 가져 옵니다.

Data Center Query Object

가져온 객체를 정책에 쓰는 핵심이 **Data Center Query Object** 입니다. 태그·이름·보안 그룹 같은 속성으로 클라우드 객체를 동적으로 묶는 객체입니다 — 예를 들어 ="tag=web인 모든 VM", "특정 보안 그룹의 인스턴스"== 를 한 객체로 정의합니다.

핵심은 쿼리 조건에 맞는 객체가 클라우드에서 늘고 줄면 Query Object도 자동으로 갱신 된다는 점입니다(Identity Awareness·SmartProvisioning의 Dynamic Object와 같은 발상). 이 Query Object를 방화벽 규칙의 출발지·목적지로 쓰 면, 정책이 클라우드 변화를 자동으로 따라갑니다.

자동화·모니터링

Automation and Monitoring 으로 연동을 자동화하고 상태를 감시 합니다 — API·SmartTask로 연동 작업을 자동화하고, 객체 갱신이 제대로 이뤄지는지 모니터링합니다.

정리하면, 데이터센터 서버에 인증으로 연결 → Query Object로 클라우드 객체를 동적으로 묶음 → 정책 규칙에 사용 하는 흐름이 핵심입니다. 그러면 클라우드가 바뀔 때 정책이 자동으로 갱신됩니다. 세부 절차는 원문 해당 절을 참고하세요.

07 모니터링과 SmartTask

모니터링과 SmartTask

CloudGuard Controller가 클라우드 객체를 제대로 배워 정책에 반영하는지 를 들여다보고, 이벤트에 자동 대응하는 방법을 정리합니다.

무엇을 모니터링하나

핵심 모니터링 항목은 다음과 같습니다. **Data Center Updates** — 클라우드 객체가 언제 어떻게 갱신됐는지, **Logs and Events** — CloudGuard Controller 관련 로그·이벤트(Logs & Events), **Status** — Controller와 연동된 데이터센터의 연결 상태 입니다. 연동이 끊기거나 객체 갱신이 멈추면 여기서 확인합니다.

외부 시스템 연동으로 **SNMP Trap** 으로 상태 변화를 NMS에 알리 고, **User Defined Event** 를 만들어 특정 조건에서 알림(Alert)을 보내 도록 구성할 수 있습니다.

SmartTask — 이벤트 기반 자동화

SmartTask 는 특정 이벤트가 발생하면 정해진 작업(스크립트·웹 요청 등)을 자동 실행 하는 기능입니다. CloudGuard Controller에서는 데이터센터 객체 변화 같은 이벤트에 맞춰 자동 대응 하는 데 활용합니다 — 예를 들어 새 VM이 특정 조건으로 추가되면 알림을 보내거나 외부 시스템에 연동하는 식입니다.

정리하면, Data Center Updates·로그·Status로 연동 상태를 감시하고, SNMP Trap·User Defined Event로 알림을 보내며, SmartTask로 이벤트에 자동 대응 하는 것이 모니터링의 축입니다. 세부 구성은 원문 해당 절을 참고하세요.

08 명령줄·구성 파라미터·한계

명령줄·구성 파라미터·한계

CloudGuard Controller를 명령줄로 다루고, 동작을 파라미터로 조정 하는 참조와 알려진 한계를 정리합니다.

명령줄 인터페이스

CloudGuard Controller는 전용 CLI를 제공합니다. 연동 상태 확인, 데이터센터 객체 조회, 연동 제어 등을 명령줄에서 할 수 있어, GUI 없이 진단·자동화할 때 유용합니다. 전체 명령 구문은 원문 Command Line Interface 절과 R82 CLI Reference 계열 문서를 참고하세요.

Configuration Parameters

Configuration Parameters 로 CloudGuard Controller의 동작을 세밀하게 조정 합니다 — 예를 들어 폴링 주기(클라우드를 얼마나 자주 확인할지), 타임아웃, 객체 처리 동작 같은 파라미터입니다. 환경 규모·변화 빈도에 맞춰 폴링 주기를 조정해 부하와 반영 속도를 균형 잡습니다.

한계(Limitations)

CloudGuard Controller에는 알려진 한계 가 있습니다 — 플랫폼별로 지원되는 객체·속성의 범위가 다르거나, 특정 기능이 일부 환경에서 제한될 수 있습니다. 연동을 설계하기 전에 쓰려는 플랫폼·객체가 지원 범위 안인지 를 한계 목록에서 확인하는 것이 좋습니다.

정리하면, 일상 운영은 SmartConsole로 하되 진단·자동화는 CLI, 동작 미세조정은 Configuration Parameters(특히 폴링 주기) 로 다루며, 설계 전 Limitations로 지원 범위 를 확인합니다. 세부 명령·파라미터·한계 목록은 원문 해당 절을 참고하세요.