디지털 트랜스포메이션을 통한
비즈니스 혁신과 4차 산업혁명 대응을 위한

# GIT 솔루션즈 데이

# 하이브리드 IT 환경의 특권계정 접근 통제 방안 및 사례(CA PAM)

2018-10-17 / 신현덕 상무

# 목차

# 디지털 변혁 시대 - 보안의 중심은 IDENTITY

Customers
Citizens

Partners

Connected Devices

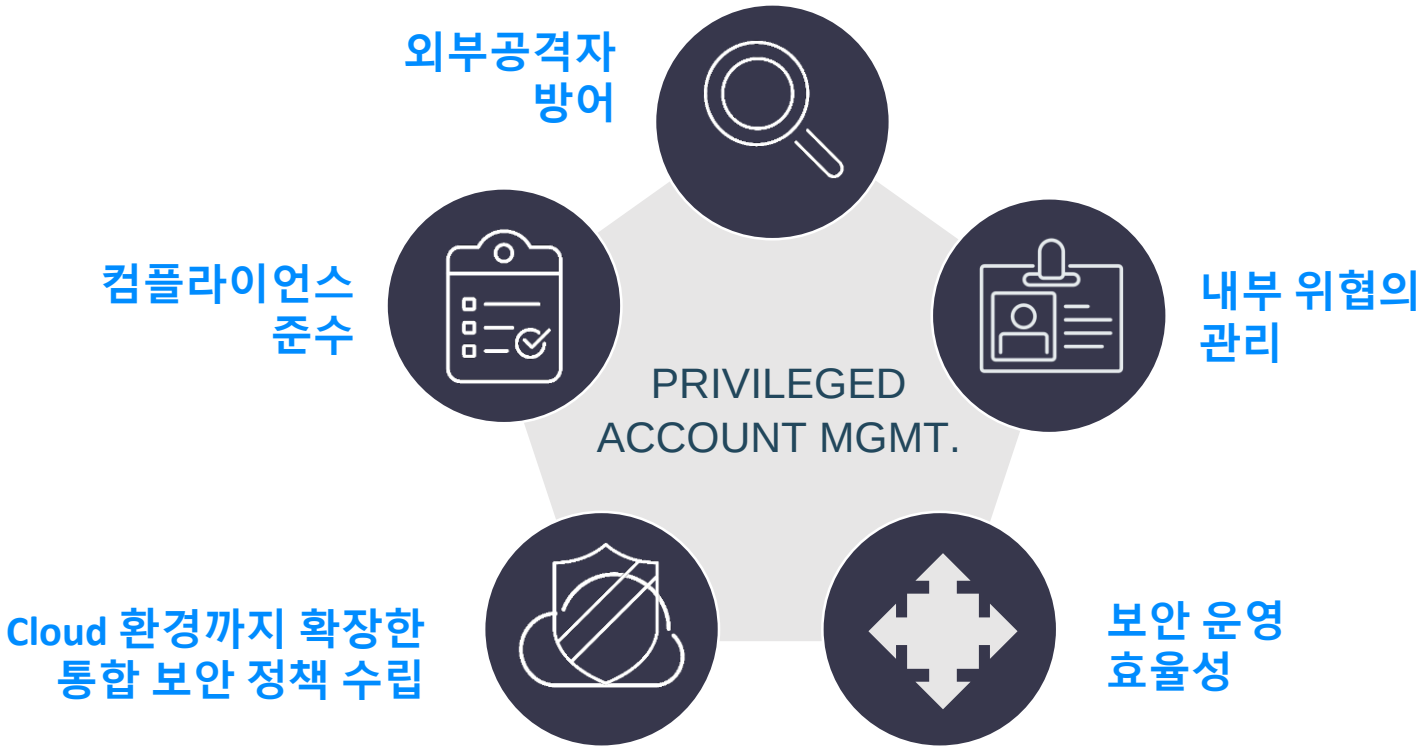
Employees


Office 365
salesforce
amazon web services™

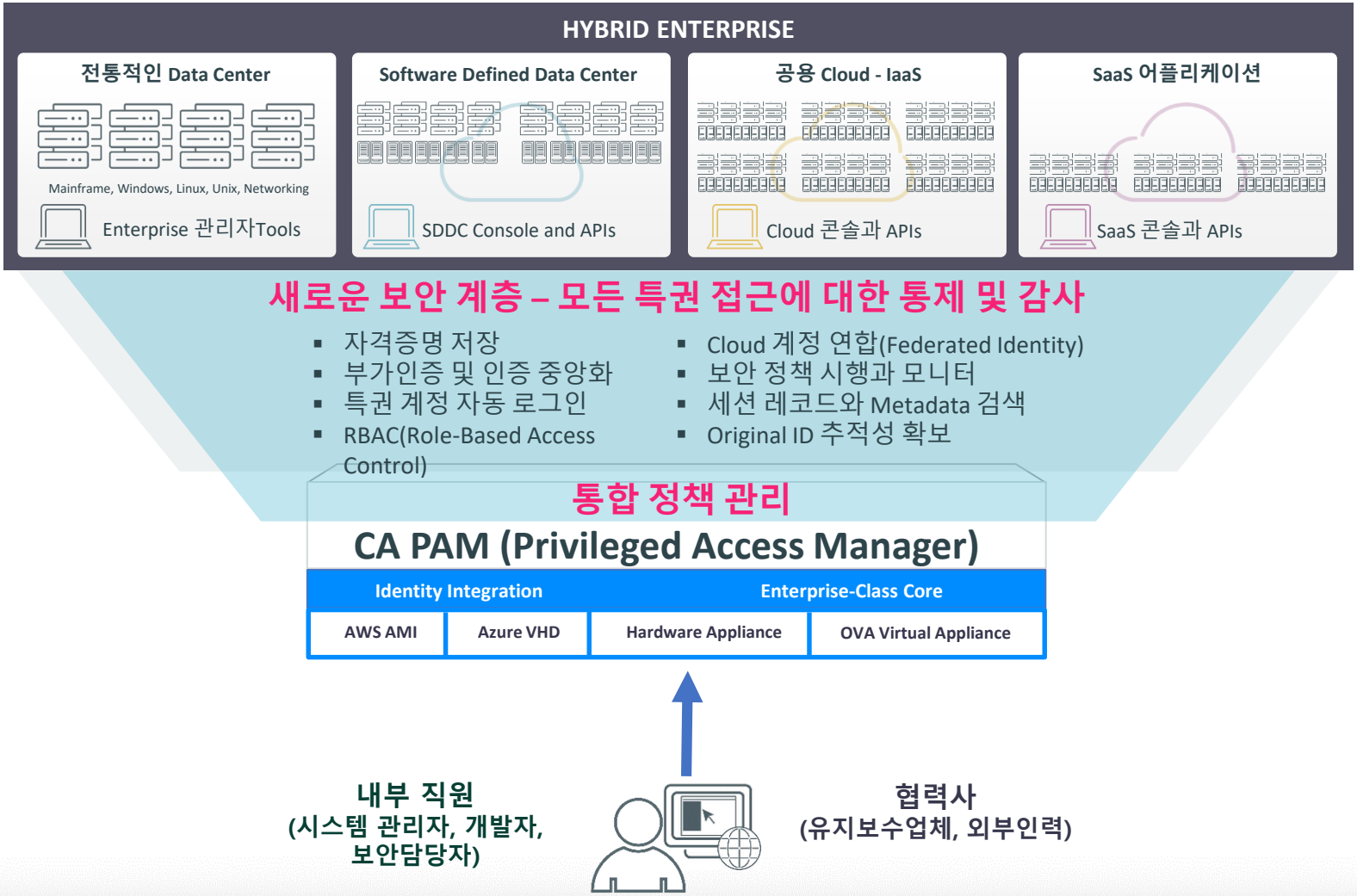
Cloud Services

On Premise Apps

# 특권 계정 관리의 주요과제



# CA PAM - Hybrid IT환경을 위한 특권계정 관리



# CA PAM 범주 별 주요 기능

## 접근제어

- 접근 경로 단일화
- 특권 계정 접근 관리
- RDP Application
- 어플리케이션 자동 로그인
- VMWare 접근통제

## 패스워드 관리

- 패스워드 관리 정책
- 패스워드 자동 변경
- Application 패스워드 관리 (A2A)

## 세션기록

- 특권계정 세션 레코딩
- Meta Data 검색

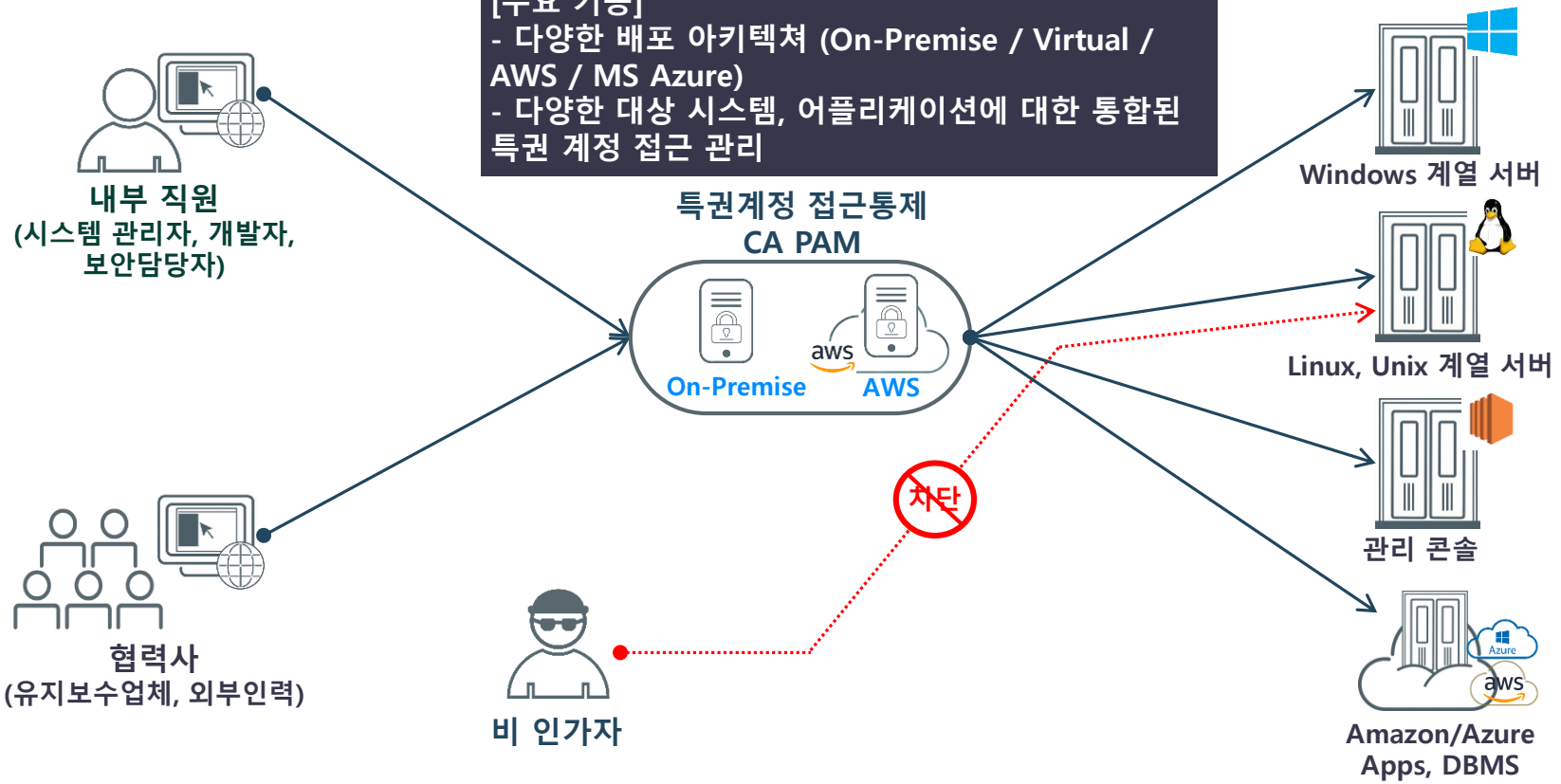
## 권한통제

- 명령어 필터
- 경유 접속 차단

# 접근 경로 단일화

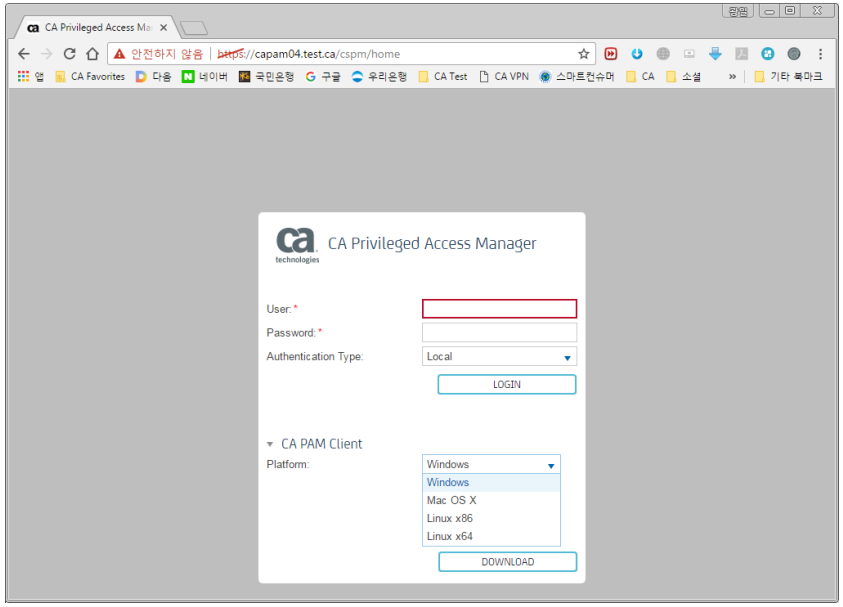
접근제어

[주요 기능]
- 다양한 배포 아키텍쳐 (On-Premise / Virtual / AWS / MS Azure)
- 다양한 대상 시스템, 어플리케이션에 대한 통합된 특권 계정 접근 관리

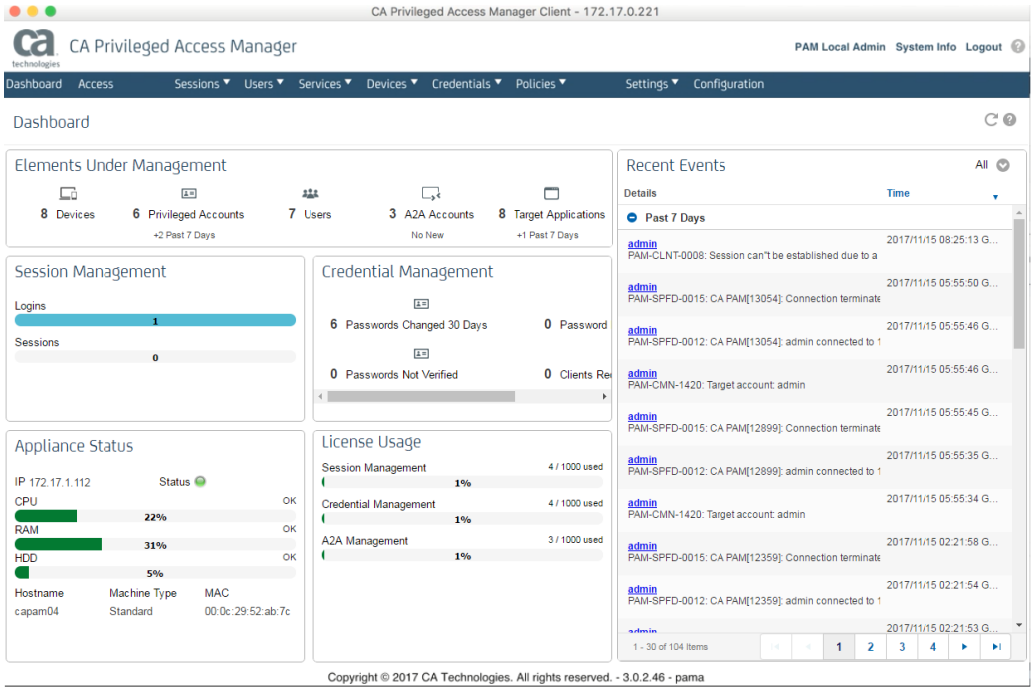


# Windows/Linux/MAC 전용 Client 지원

접근제어



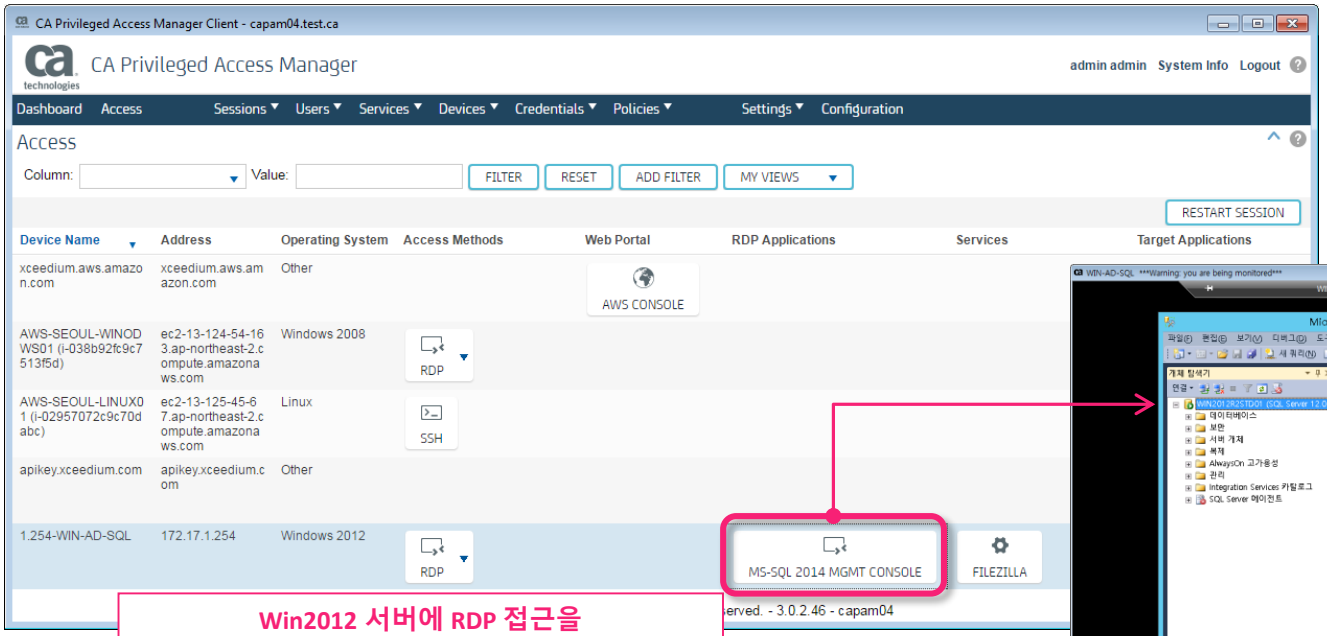

Login Page



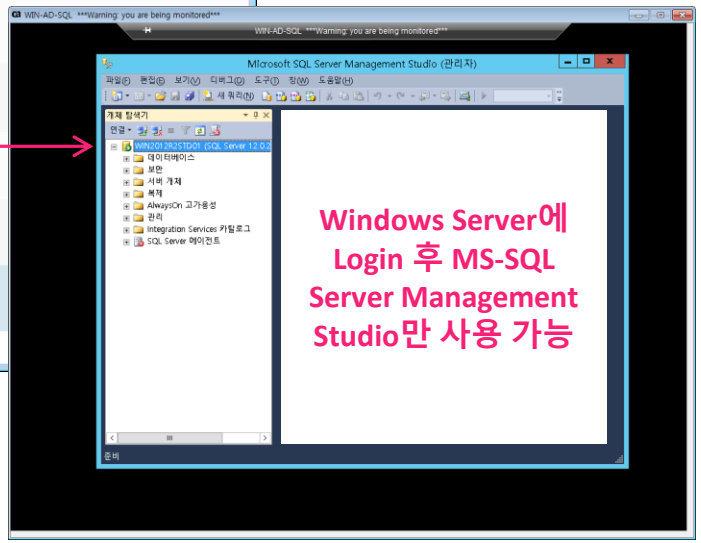

Mac 전용 Client

# RDP Application 접근 제한






Win2012 서버에 RDP 접근을
MSSQL Management Studio 2014로 제한

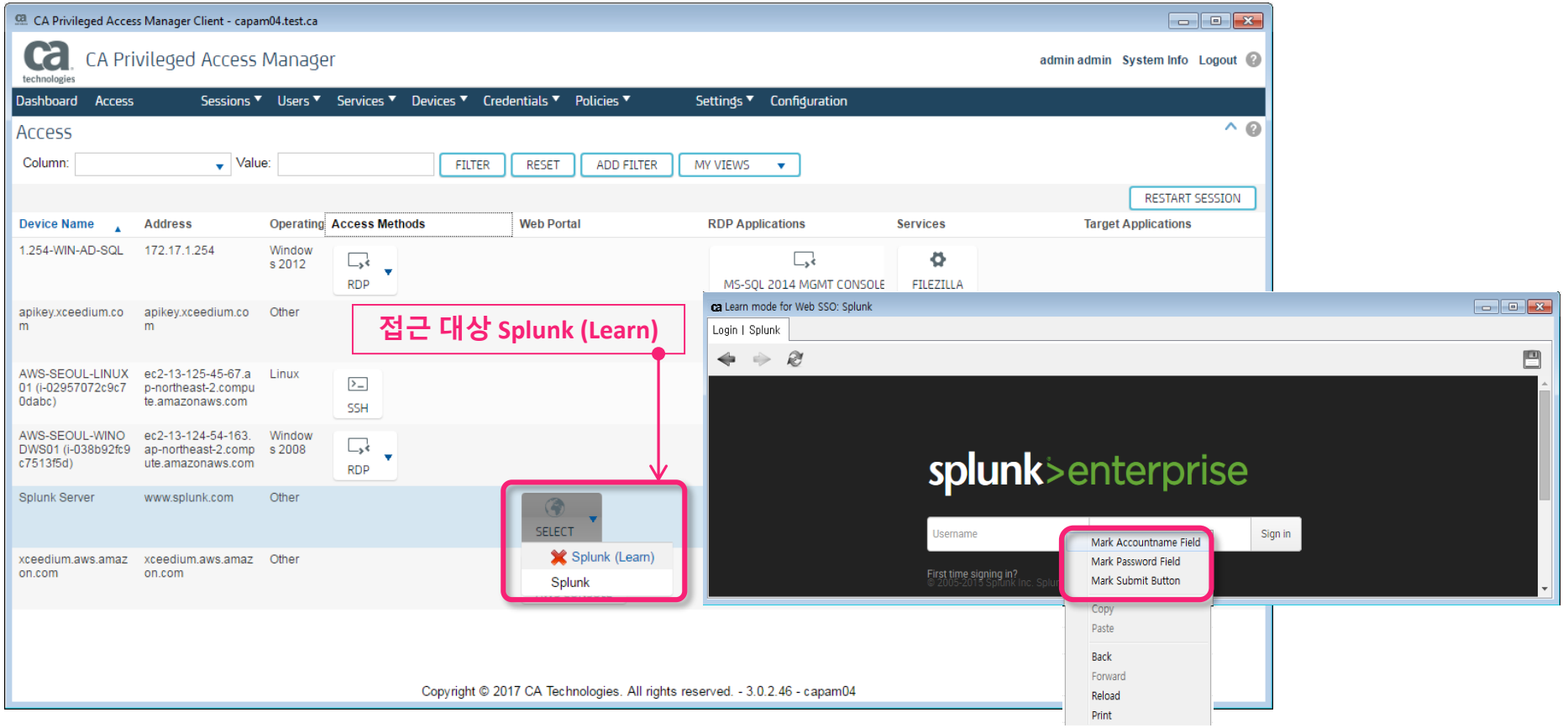



## RDP Application :

1. Windows 환경일 경우 서버의 특정 응용프로그램을 사전에 서비스로 등록하여 해당 응용 프로그램만 나타나게 하게 함.
2. 접속자의 권한을 해당 응용프로그램으로 제한하여 보안성 강화

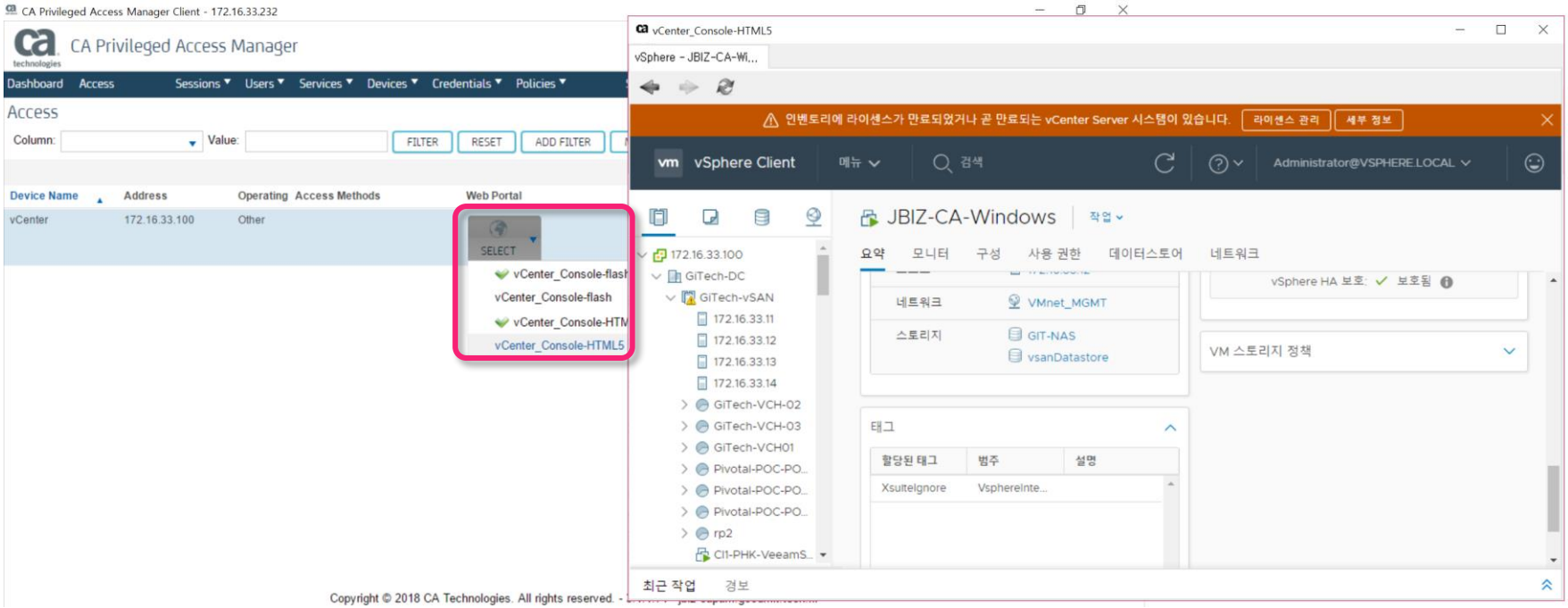
# Application 자동 로그인





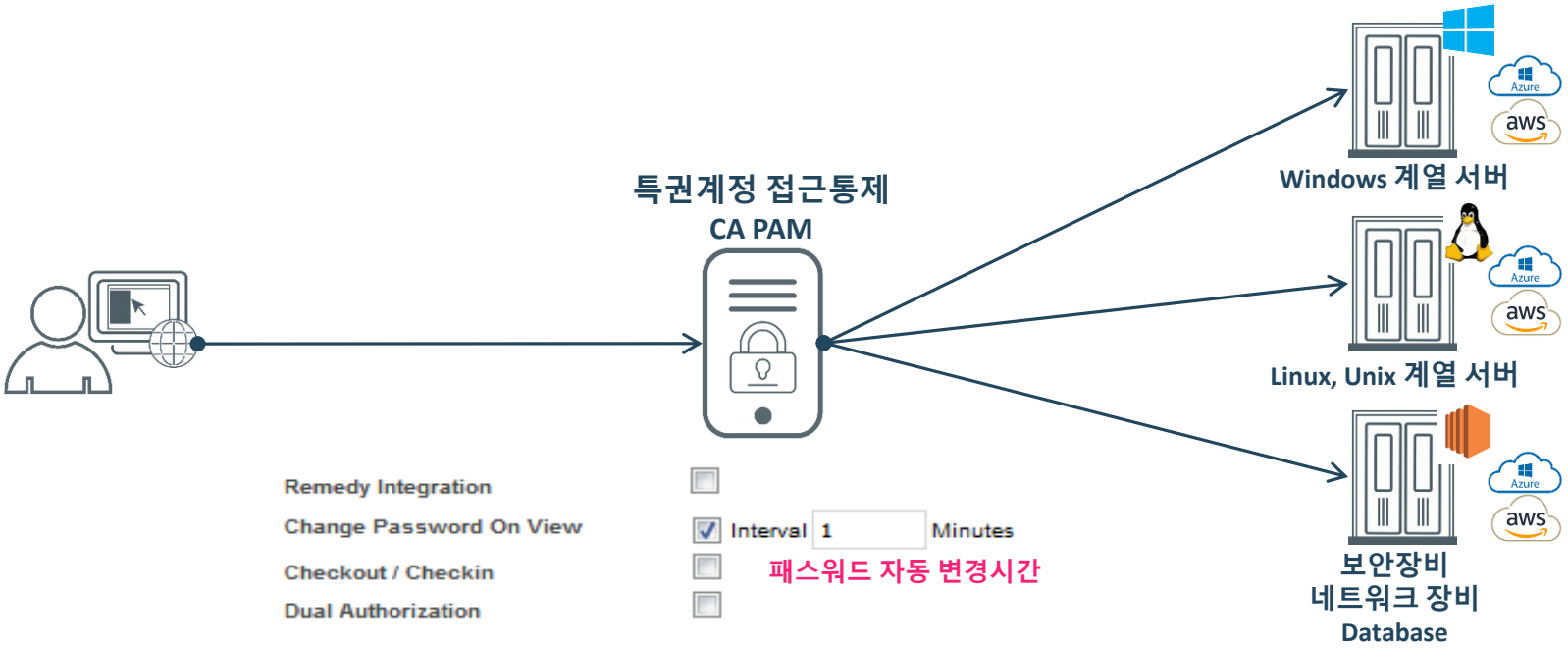
# VMware vCenter 콘솔 (HTML5) 접근 연동

접근제어



# 패스워드 관리 정책






**Password 관리(Password Management)**

✓ 지정된 규칙(복잡도) 및 주기에 따라 자동으로 시스템 패스워드를 변경
✓ 시스템 패스워드 변경 규칙은 시스템의 종류에 따라 여러 가지를 생성
✓ 생성된 규칙을 관리자는 각각의 시스템에 서로 다르게 적용

Amazon/Azure API's
& Apps, DBMS

# Application Password 관리 (A2A)

패스워드 관리

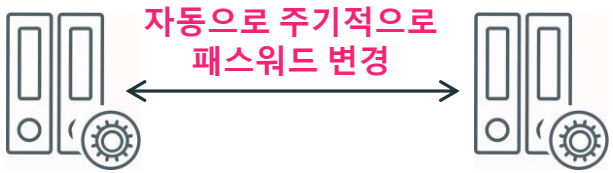
## AS-IS (개념도)

Application (CS, WEB 등) Application (DB 등)

### 하드코딩 된 Static Password를 기반으로 통신

- ✓ 시스템 구성 단계에서 설정된 하드코딩 된 Static Password를 통하여 상호 통신
- ✓ 하드코딩 된 패스워드의 경우 변경이 불가
- ✓ 하드코딩 된 패스워드의 외부 유출 시 DB 등 주요 서버들이 공격을 당할 수 있는 위험 존재

## TO-BE (개념도)



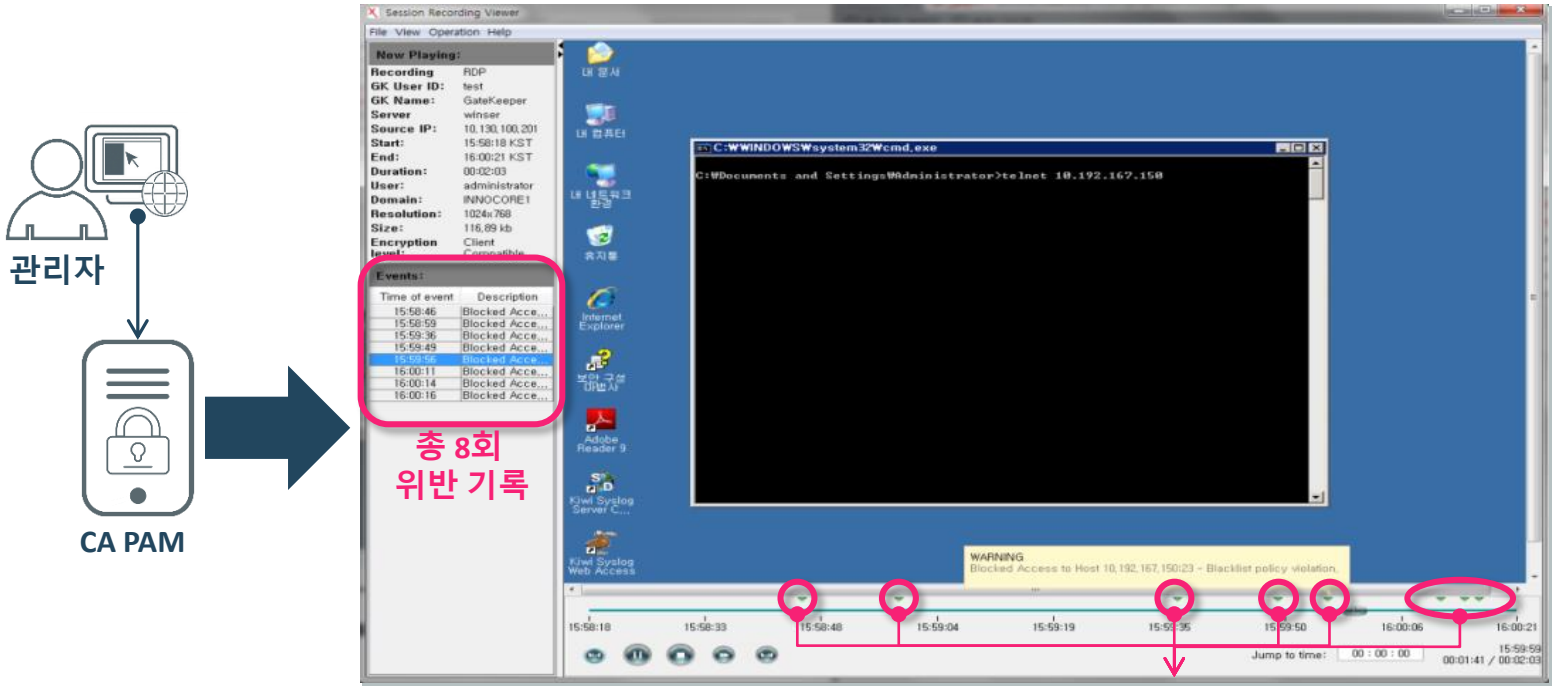

Application (CS, WEB 등) Application (DB 등)

### A2A 패스워드 관리를 통하여 주기적으로 상호 패스워드 변경

- ✓ 자동으로 Application간에 접속 패스워드를 변경 (관리자가 설정한 주기에 따름)
- ✓ DB 등 주요 자원에 접근하는 모든 패스워드가 정해진 정책에 따라 변경 됨
- ✓ 모든 접속 형태의 패스워드가 변경되어 주요 서버들이 좀더 공격으로부터 안정성을 확보

# 특권 계정 세션 레코딩

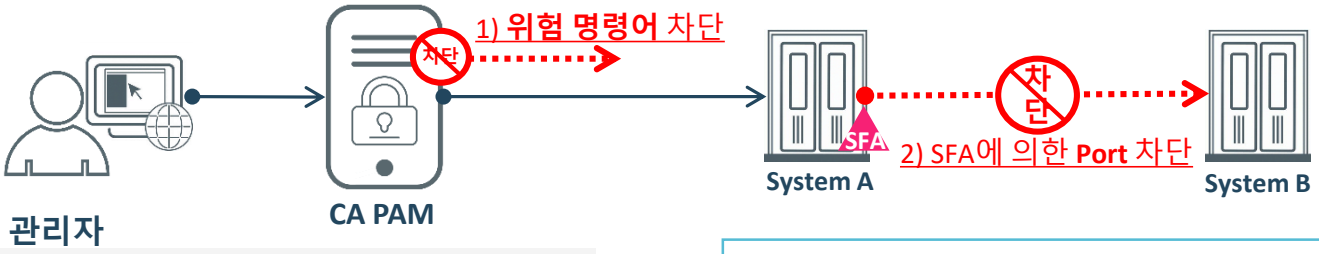
세션기록

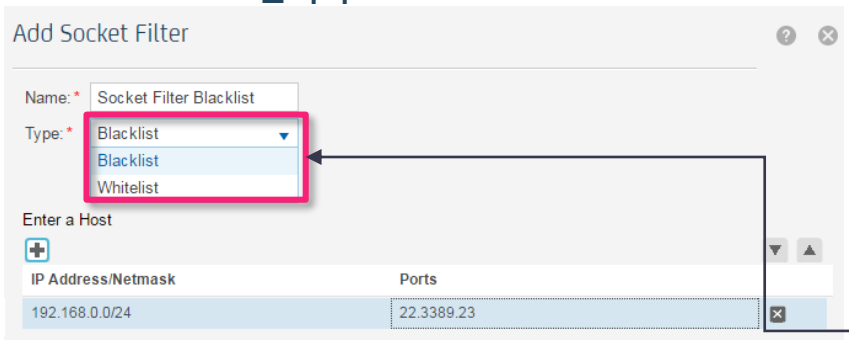



- ✓ 시스템에서 수행한 모든 내역을 동영상으로 Recording 하며, 위반이 발생 시 문제 발생 시점 표시하고 해당 시점으로 바로 이동할 수 있어 전체 내용을 다시 볼 필요가 없는 효율적인 검색
- ✓ Idle 타입 관리와 프로토콜 레이어 기반 녹화로 효율적인 녹화 파일 크기 제공

# 명령어 통제 / 경유 접속 차단

권한통제




- **Command Filter** : 모든 CLI 세션에 대한 위험명령어 정책을 디바이스별/그룹별로 설정하여 허용되지 않는 명령어는 실시간을 차단
- **Socket Filter** : 정책에 의해 허용된 리소스 이외에 임의 접속 시도의 원천 차단

**접속 허용/불가 IP 대역/Port/Web URL White List, Black List 2가지로 설정**

**Socket Filter Agent (SFA) 상태 모니터링**

Socket Filter Agents Status

| Device Name | Address | Agent Version | OS | Status | Action |
|---|---|---|---|---|---|
| Windows 2003 | 192.168.0.90 | 1.37 | WINDOWS | active | |
| windows 2008 | 192.168.0.100 | 1.38 | WINDOWS | unknown | remove |
| IP관리도구 | 121.0.137.35 | 1.35 | LINUX | unknown | remove |
| CS 서버 | 121.0.137.38 | 1.35 | LINUX | active | |

# AWS/Azure + CA PAM 솔루션

**Amazon Web Service**
- 세계 최고의 IaaS 클라우드 제공업체
- 2006년부터 AWS 비즈니스 시작
- AWS EC2, S3 등 다양한 IaaS 용 클라우드 서비스 제공
- 2016년 1월 서울 리전 (Seoul Region)출시

**Microsoft Azure**
- 2010년 시작된 마이크로소프트의 클라우드 컴퓨팅 플랫폼
- 2011년 PaaS에 이어 2013년 IaaS 서비스 시작
- 2018년 현재 50개 Region 지원



**CA PAM for Amazon Web Service**
- 2012년 6월에 Amazon WS 지원 CA PAM 출시
- 어플라이언스 및 AMI 타입 지원
- 2018년 현재 다수의 AWS 상의 PAM운영고객 확보

**CA PAM for Microsoft Azure**
- 2018년 4월에 Microsoft Azure 지원
- Microsoft Azure 배포를 위한 VHD 배포 유형 지원

# CA PAM에서의 AWS 특화 기능(Cloud Infra Access Control)

**1** Cloud 패스워드/SSH Public Key 관리

**2** AWS 콘솔 활동 내역 기록

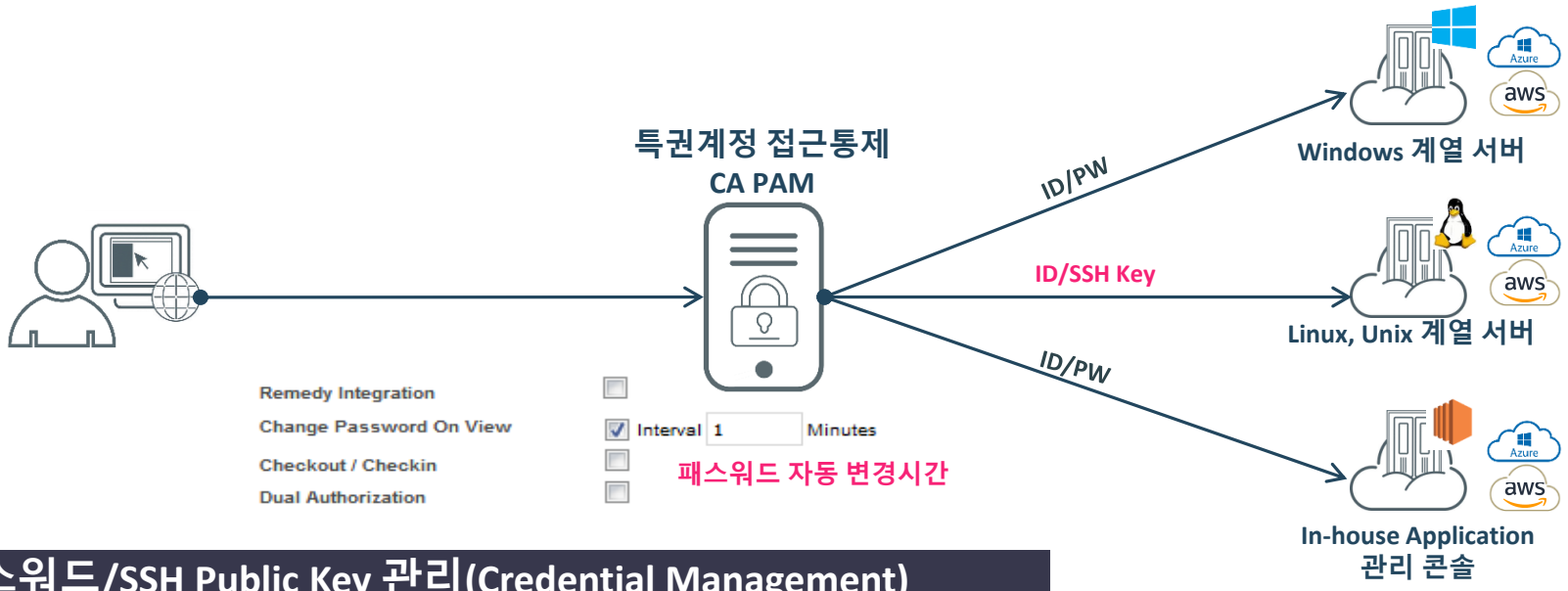
**3** Dynamic AWS EC2, Azure VM 통제 및 보호

**4** AWS Access Key 관리 및 ID Federation

**5** AWS, Azure 환경의 배포 유연성
(물리, 가상화, Cloud 지원)

**6** Cloud 환경의 통합 접근 통제

# 패스워드/SSH Public Key 관리

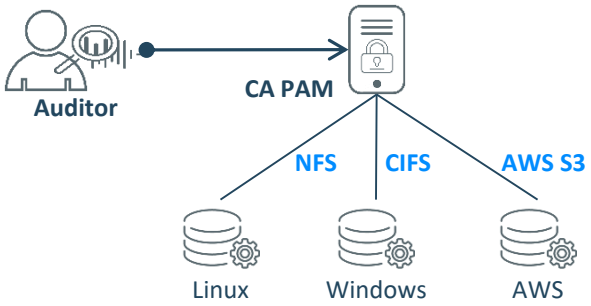


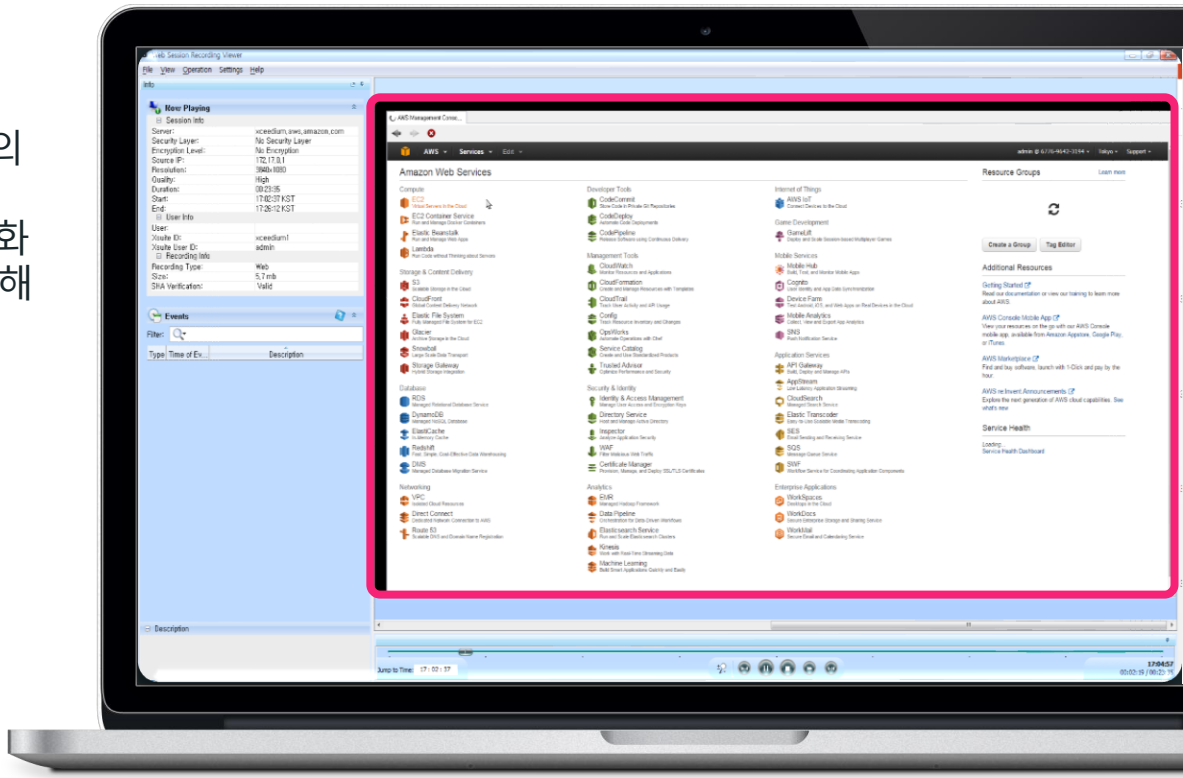

## 패스워드/SSH Public Key 관리(Credential Management)

- ✓ 패스워드 / SSH Public Key 자동 인증
- ✓ 지정된 규칙(복잡도) 및 주기에 따라 자동으로 시스템 패스워드를 변경
- ✓ 자신의 계정 또는 서비스 계정으로 지정된 주기에 따라 SSH Key 자동 변경
- ✓ 시스템 패스워드 변경 규칙은 시스템의 종류에 따라 다르게 생성
- ✓ 생성된 규칙을 관리자는 각각의 시스템에 서로 다르게 적용

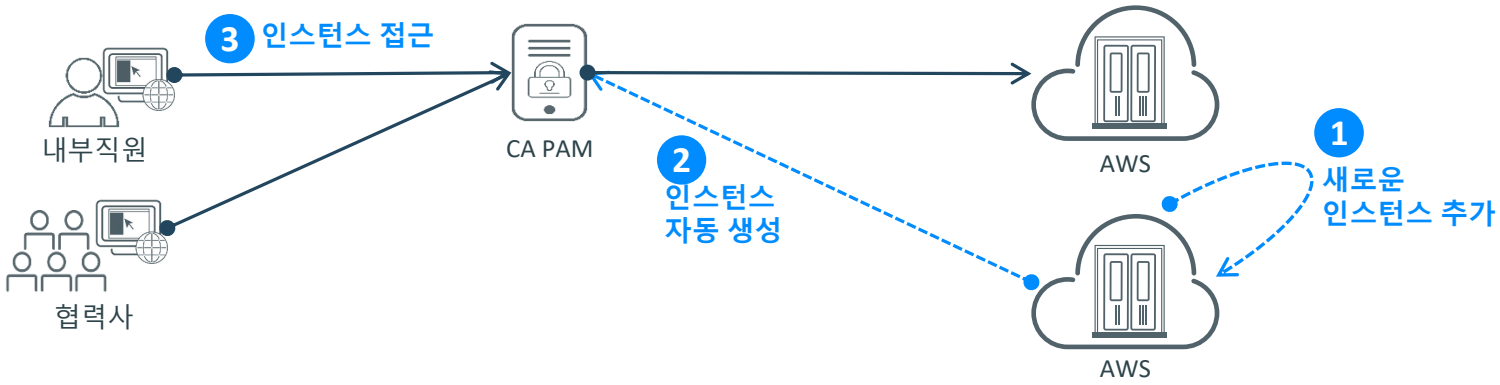
# 웹 관리 콘솔 활동 내역 기록

- **Value**
  - ✓ 관리자 행위에 대한 감사 및 추적성 확보
  - ✓ AWS Management Interface 상의 모든 활동 내역 녹화
  - ✓ AWS 인스턴스에 작업 세션 녹화
  - ✓ 녹화된 정보의 변조 확인을 통해 무결성 확보
  - ✓ 세션 레코딩 사이즈 최소화



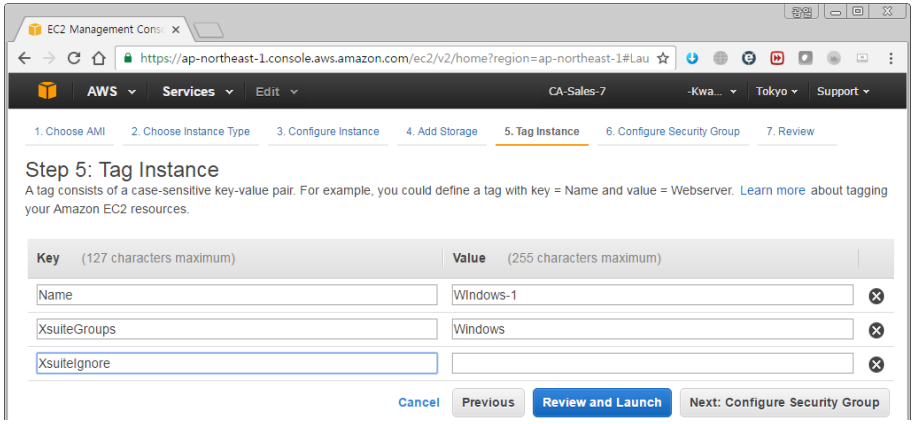
# Dynamic 인스턴스 통제 및 보호



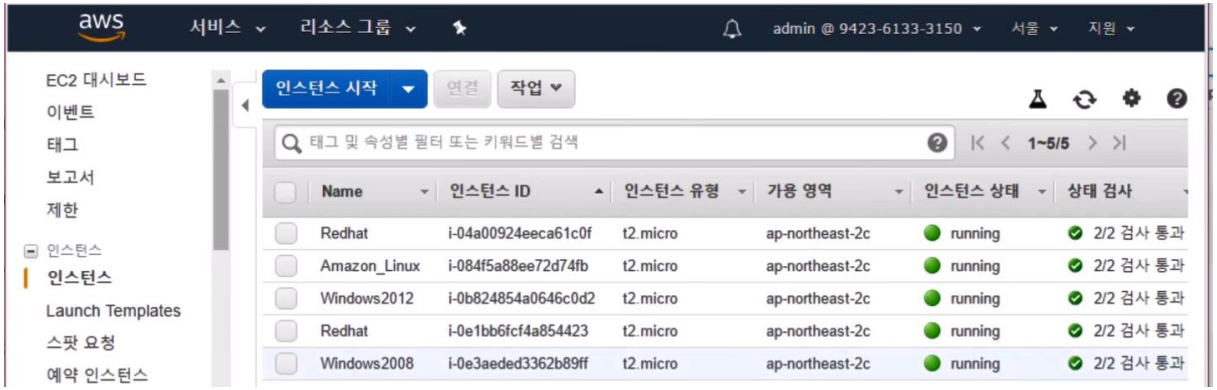

## Dynamic 인스턴스 통제 및 보호

- ✓ AWS의 AMI Tagging을 이용해 CA PAM에 Device 자동 등록
- ✓ AWS 환경에 인스턴스가 생성되는 즉시 CA PAM에 정책 보호 및 액세스 권한을 실시간으로 추가
- ✓ 동적 EC2 리소스 전체에 대한 자동으로 정책을 설정 및 시행
- ✓ 자동 등록 및 정책 시행을 원치 않을 경우, 예외 Tagging 설정

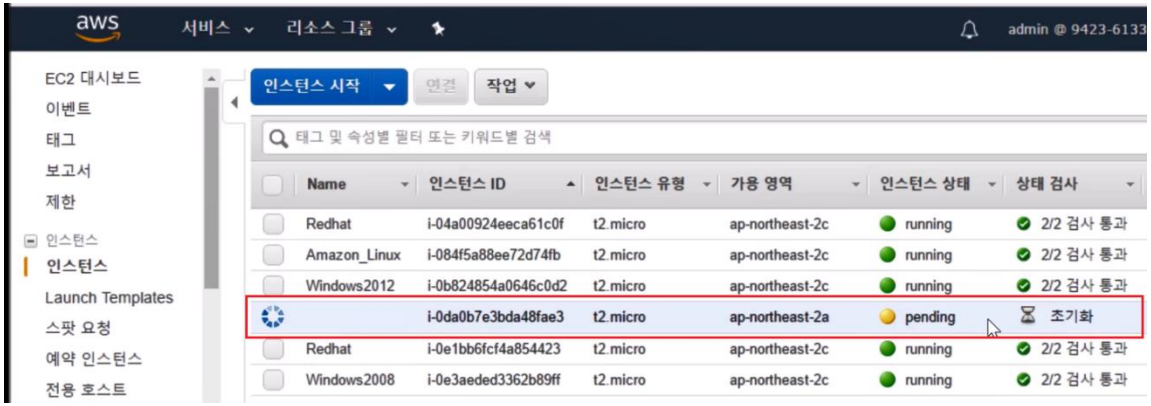
AWS EC2 Tagging 설정



# Dynamic 인스턴스 통제 및 보호(계속 1)

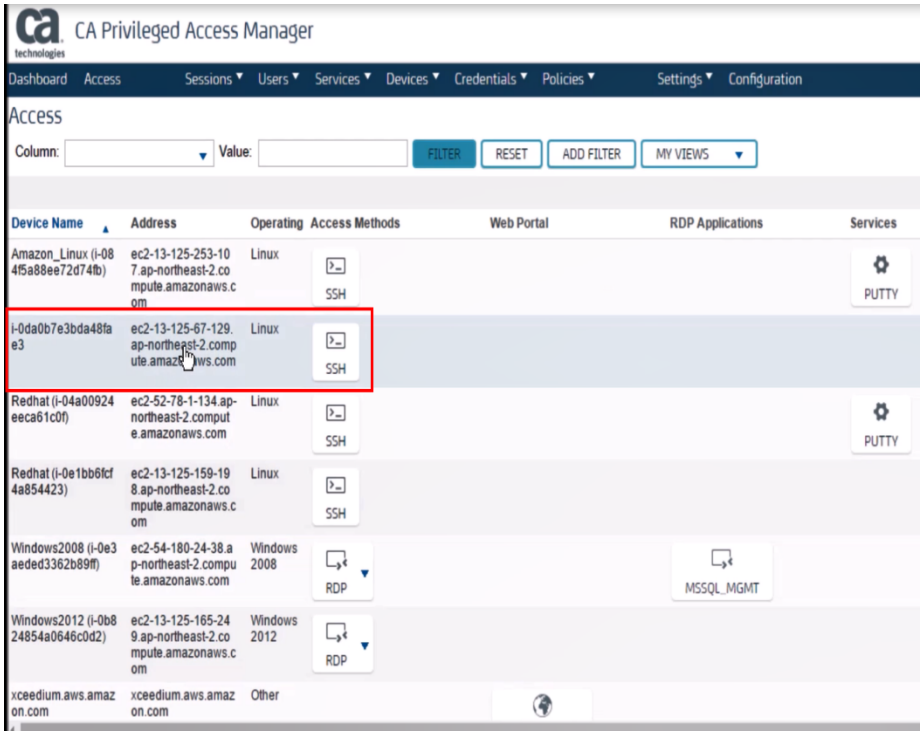



1 AWS 새로운 인스턴스 추가(Auto Scaling)

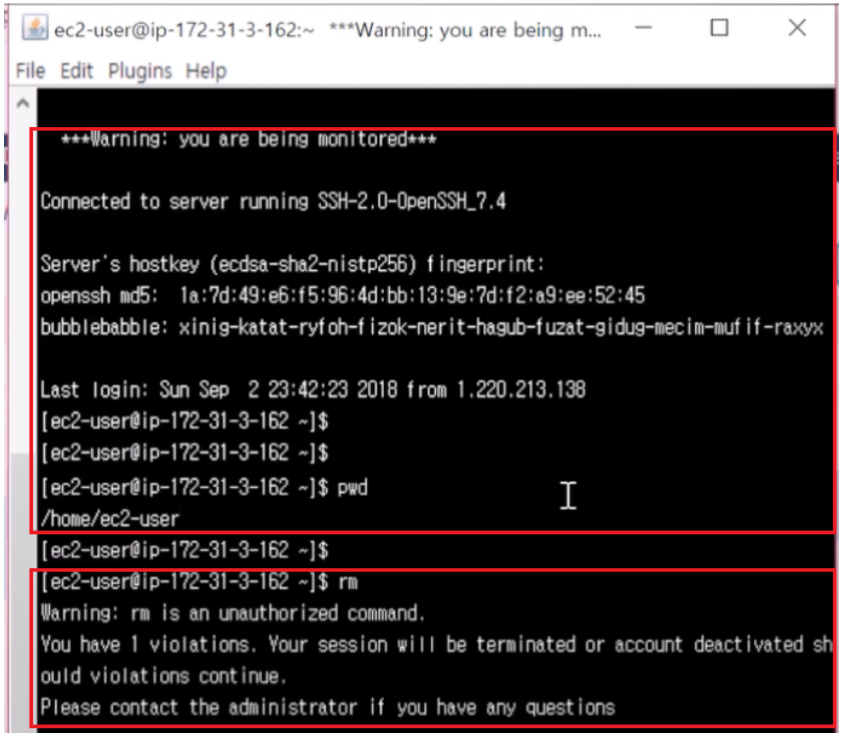


# Dynamic 인스턴스 통제 및 보호(계속 2)

**2** PAM에서 인스턴스 자동 생성

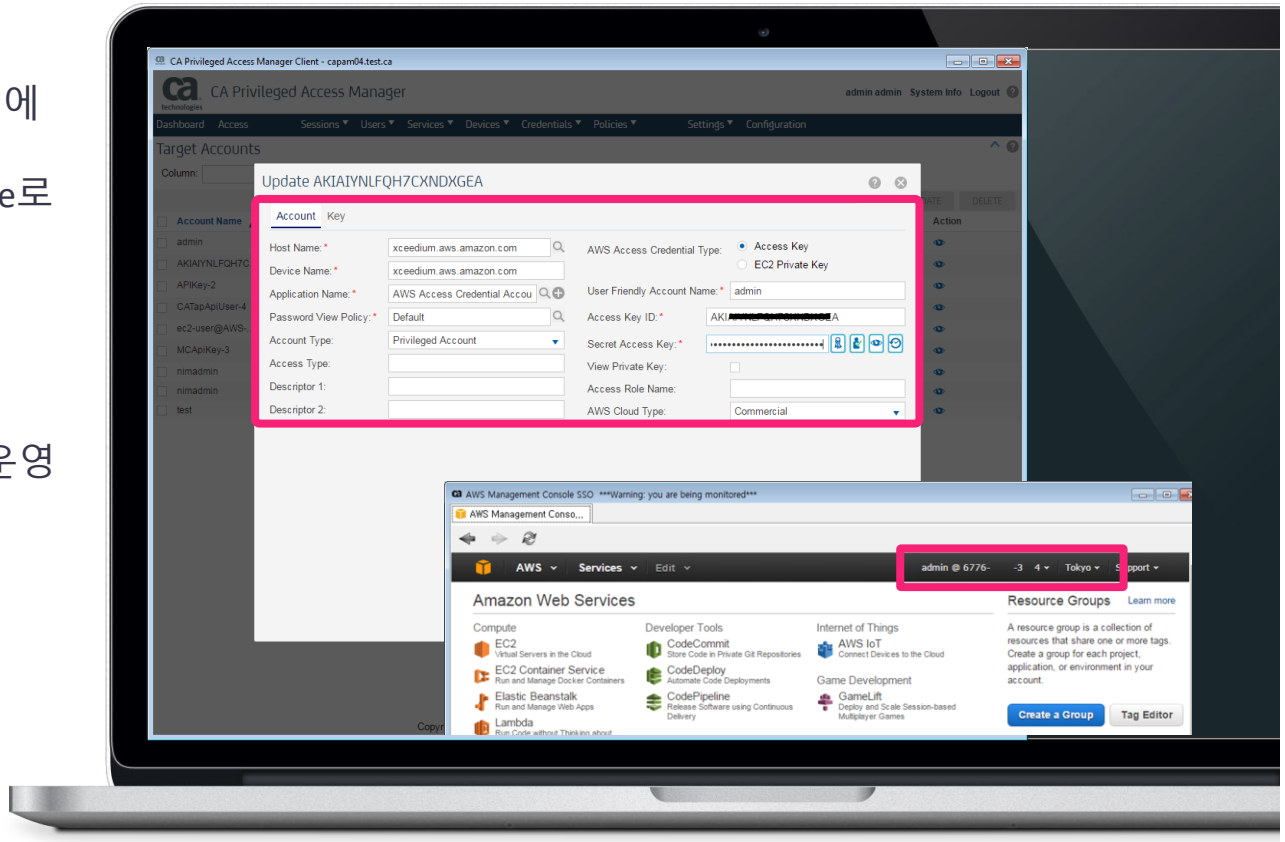



**3** 인스턴스 접근 및 통제

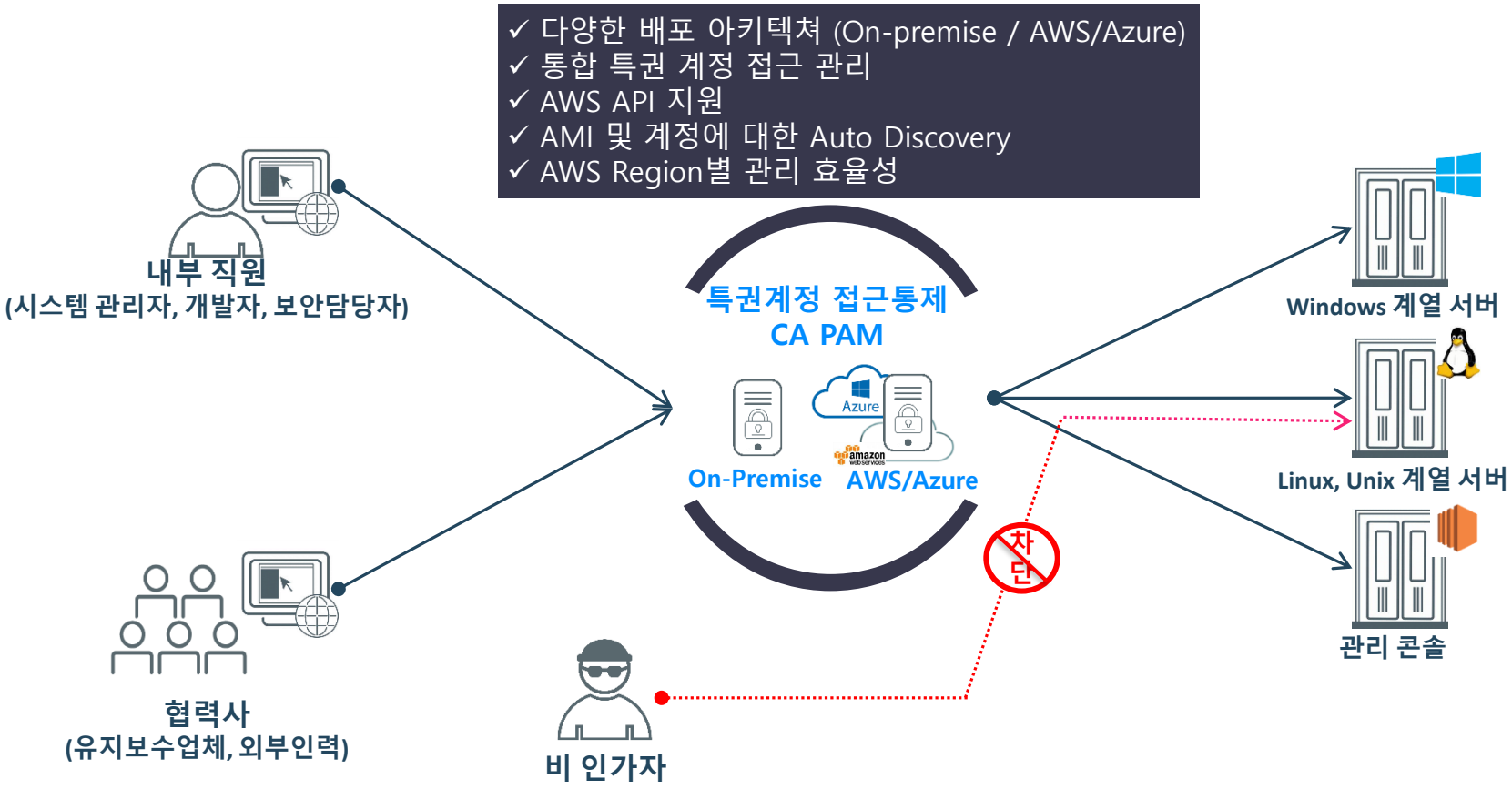


# AWS Access Key 관리 및 ID Federation

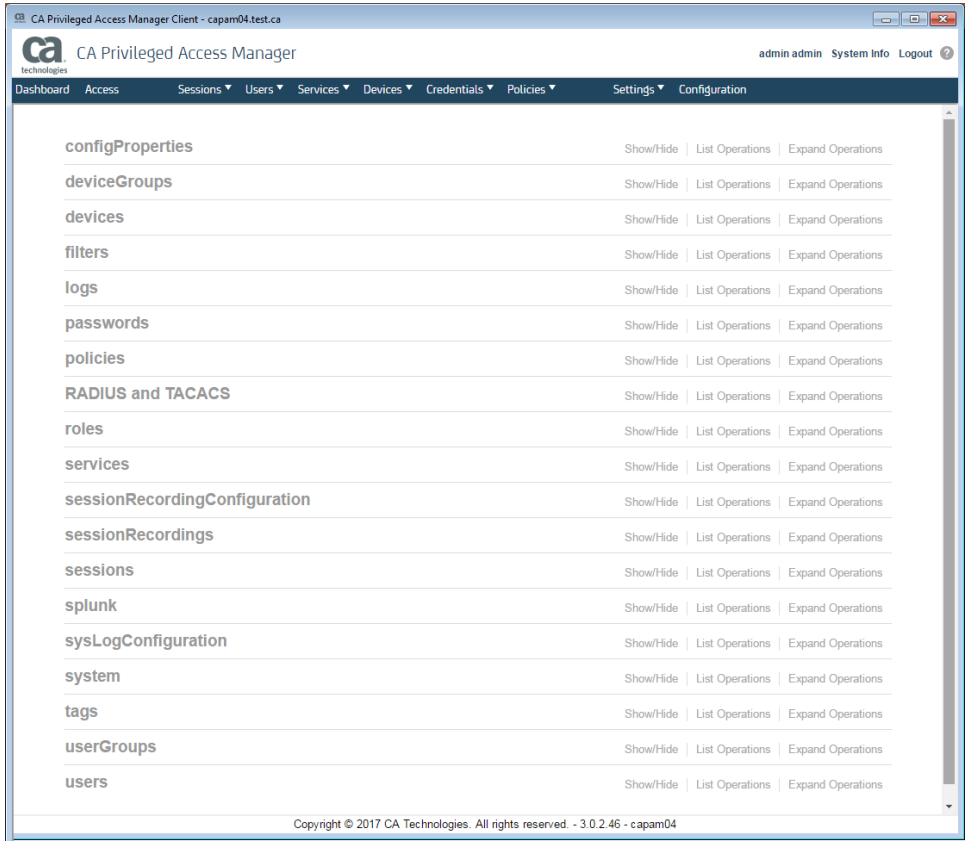
- **Value**
  - ✓ 도메인/로컬 CA PAM 계정에 대한 AWS ID Federation
  - ✓ AWS Management Interface로 운영자의 빠른 접근 (ID Federation을 이용한 자동로그인 제공)
  - ✓ AD/LDAP 계정과 AWS IAM Interface 연계 지원
  - ✓ AWS의 IAM 계정 최소화 운영 및 오남용 방지
  - ✓ AWS 계정의 추적성 향상



# AWS 환경의 배포 유연성



# Policy Automation을 위한 External API



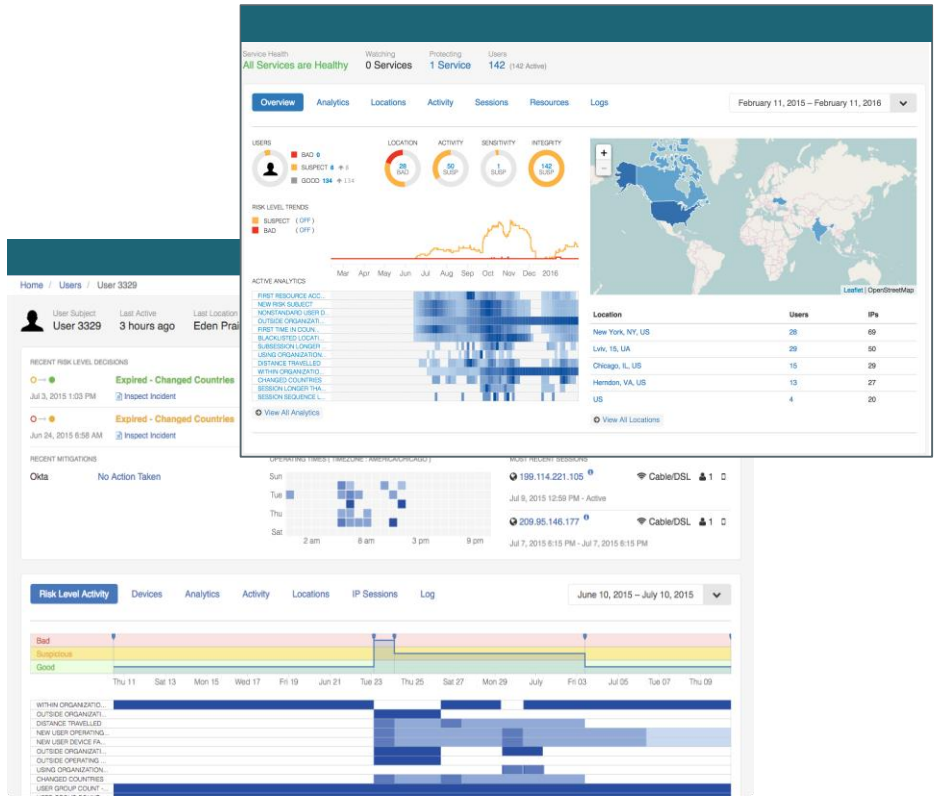

## CA PAM에서의 External API

- ✓ Policy Automation과 Programmatic Integration을 위한 External API (JSON/Restful API)
- ✓ 손쉬운 External API 검증과 Sample Request/Response Test를 위한 API Doc 제공
- ✓ API Key를 통한 Web Service 인증

# Proactive Detection을 위한 Threat Analytics

Threat Analytics for PAM(TAP)은 머신러닝 기반의 분석 엔진 기능을 활성화

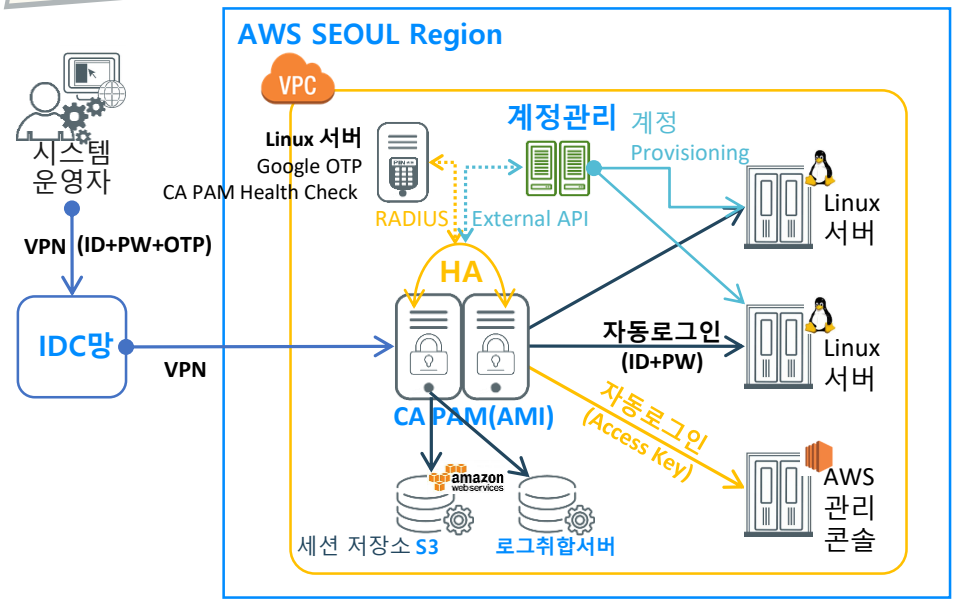
- **위협 탐지(Detection)**
- **자동화된 완화 조치(Automated Mitigation)**
- **운영 가시성(Operational Insights)**



# A 제조사 구축 사례 (CA PAM)

## A 제조사 운영 환경

사업 기간 : 2018.04 ~ 현재(약 4개월)
대상 서버 수: 총 OOO대
대상 서버 종류 : Linux(OO0)
운영자 : 약 O00명 (O0명 AWS 관리)
배포 유형 : CA PAM AMI * 3[운영(2), 개발(1)]




| CA PAM 주요 운영 기능 | |
|---|---|
| 전용 WIN /.MAC OS Client | ✓ |
| 역할 기반의 서버 접근 통제 | ✓ |
| 세션 레코딩 (S3) | ✓ |
| 시스템 접근 자동 로그인 | ✓ |
| EC2 AMI Password 변경 | ✓ |
| AMI Auto Scaling 관리(Scale in/out) | ✓ |
| 2FA 부가인증(Google OTP) | ✓ |
| CA PAM Health Monitor | ✓ |
| 계정 관리 솔루션 연동 | ✓ |
| AWS 관리콘솔 접근통제 및 세션 레코딩 | ✓ |

## 상세 설명

### Challenge (해결 과제)

- Compliance 대응 미흡
- AWS 기반의 Linux Only 대상으로만 접근 통제
- AMI Auto Scale 대응 부재
- 계정관리, 접근통제 자동화
- 사용자 행위 이력 감사 로그

### Solution (솔루션)

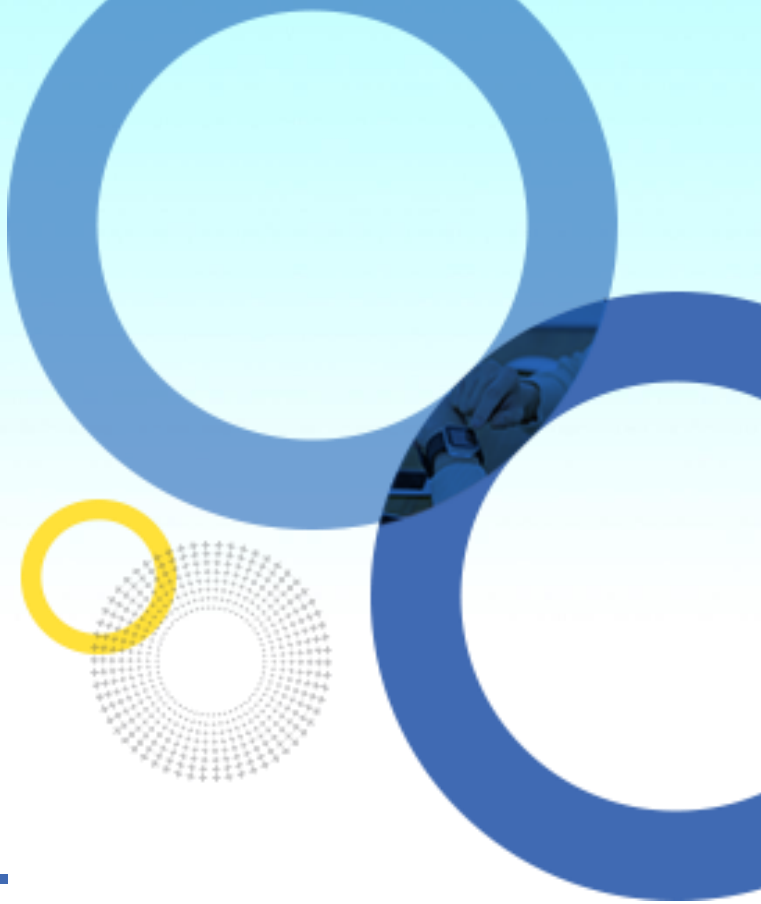
- Cloud 환경의 서버 접근 통제를 위한 CA PAM 솔루션 도입

### Result (결과)

- Compliance 준수 기틀 마련
- EC2 AMI 세션 레코딩
- EC2 AMI Password 변경
- Syslog 연동(로그취합 서버)
- Google OTP 연동
- 자동 로그인
- 계정관리 솔루션 연동
- AMI Auto Scale 관리
- Scale-Out/Scale-In AMI 자동로그인

디지털 트랜스포메이션을 통한
비즈니스 혁신과 4차 산업혁명 대응을 위한

# GIT 솔루션즈 데이



감사합니다.