

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

특권 계정 관리의 주요 과제	4p
특권 계정 관리 방안	6p
CA PAM 범주 별 주요 기능	7p
CA PAM for AWS 특화 기능	18p
Threat Analytics for PAM	27p
구축사례 for PAM	28p

디지털 변혁 시대 - 보안의 중심은 IDENTITY



Customers
Citizens



Partners



Connected Devices



Employees



Cloud Services

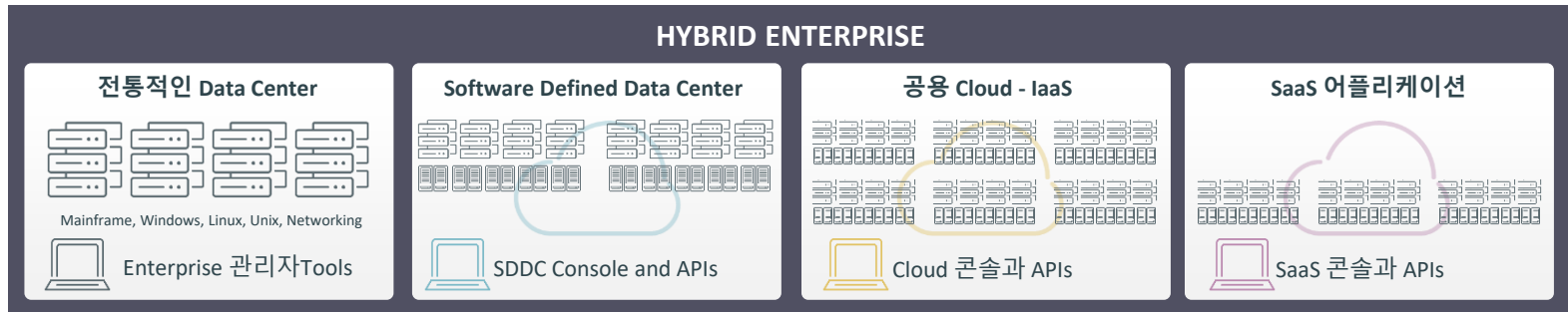


On Premise Apps

특권 계정 관리의 주요과제



CA PAM - Hybrid IT환경을 위한 특권계정 관리

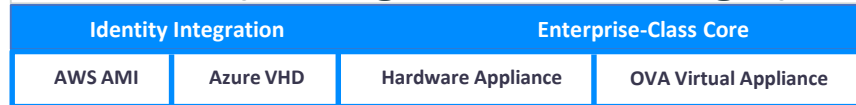


새로운 보안 계층 - 모든 특권 접근에 대한 통제 및 감사

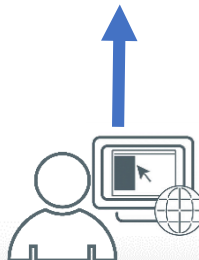
- | | |
|---|---|
| <ul style="list-style-type: none"> ▪ 자격증명 저장 ▪ 부가인증 및 인증 중앙화 ▪ 특권 계정 자동 로그인 ▪ RBAC(Role-Based Access Control) | <ul style="list-style-type: none"> ▪ Cloud 계정 연합(Federated Identity) ▪ 보안 정책 시행과 모니터 ▪ 세션 레코드와 Metadata 검색 ▪ Original ID 추적성 확보 |
|---|---|

통합 정책 관리

CA PAM (Privileged Access Manager)



내부 직원
(시스템 관리자, 개발자, 보안담당자)



협력사
(유지보수업체, 외부인력)

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

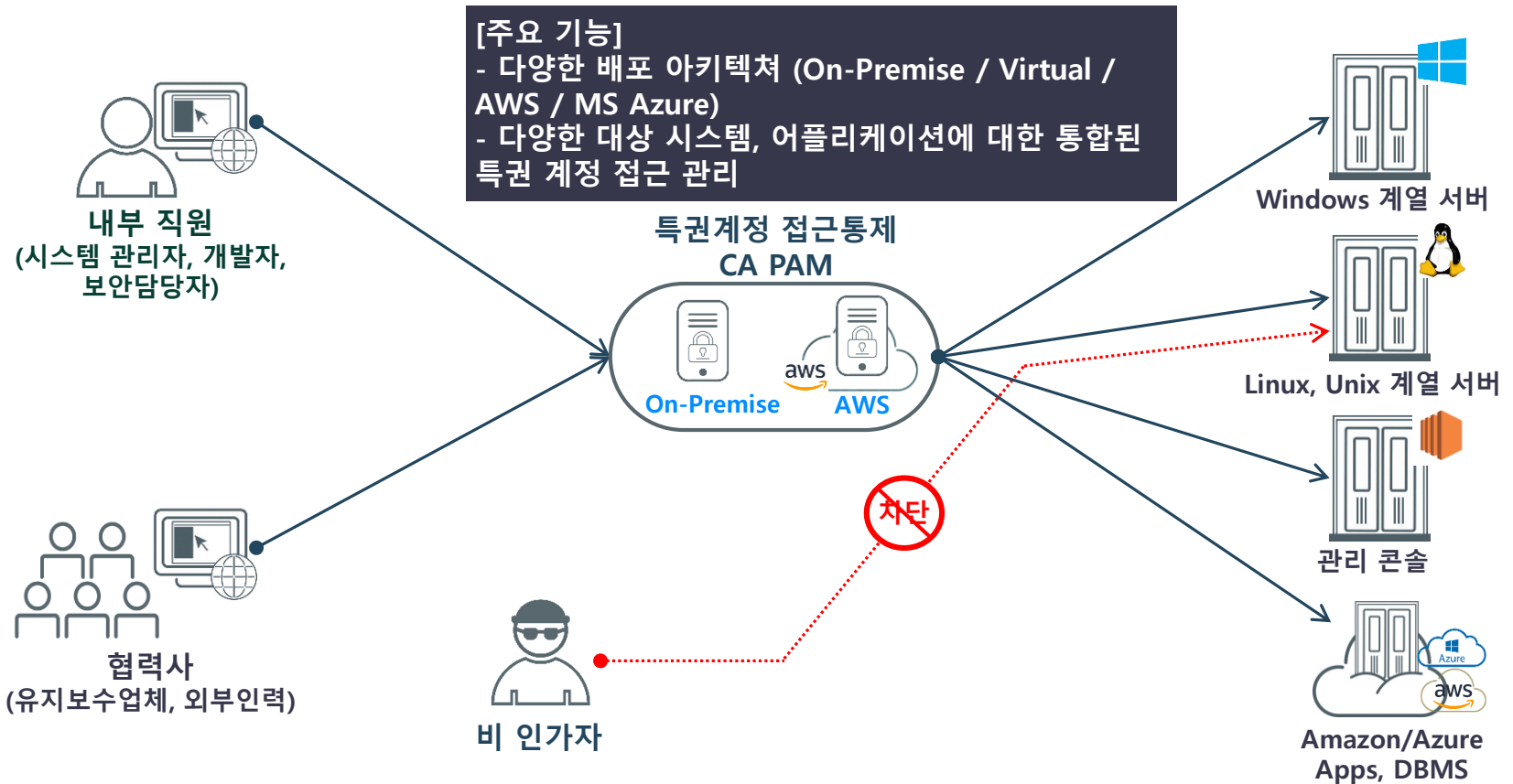
- 특권계정 세션 레코딩
- Meta Data 검색

권한통제

- 명령어 필터
- 경유 접속 차단

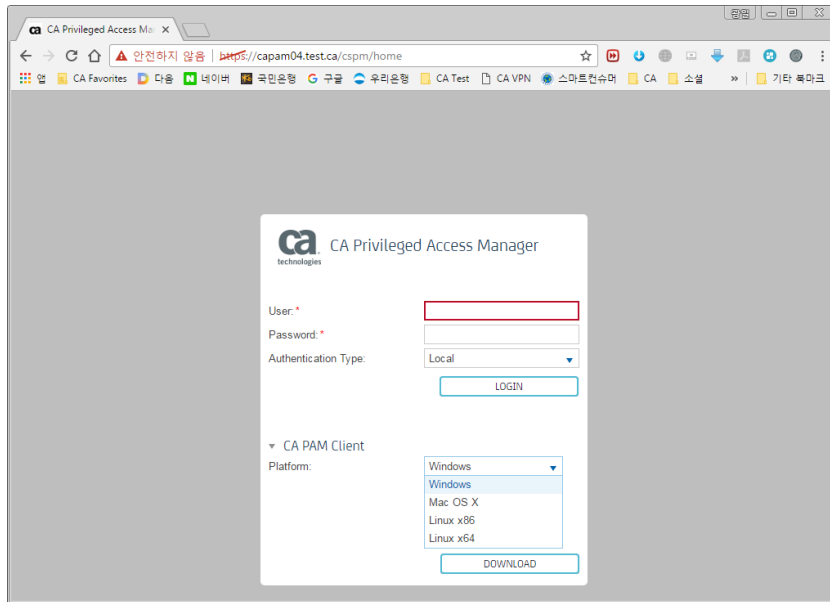
접근 경로 단일화

접근제어

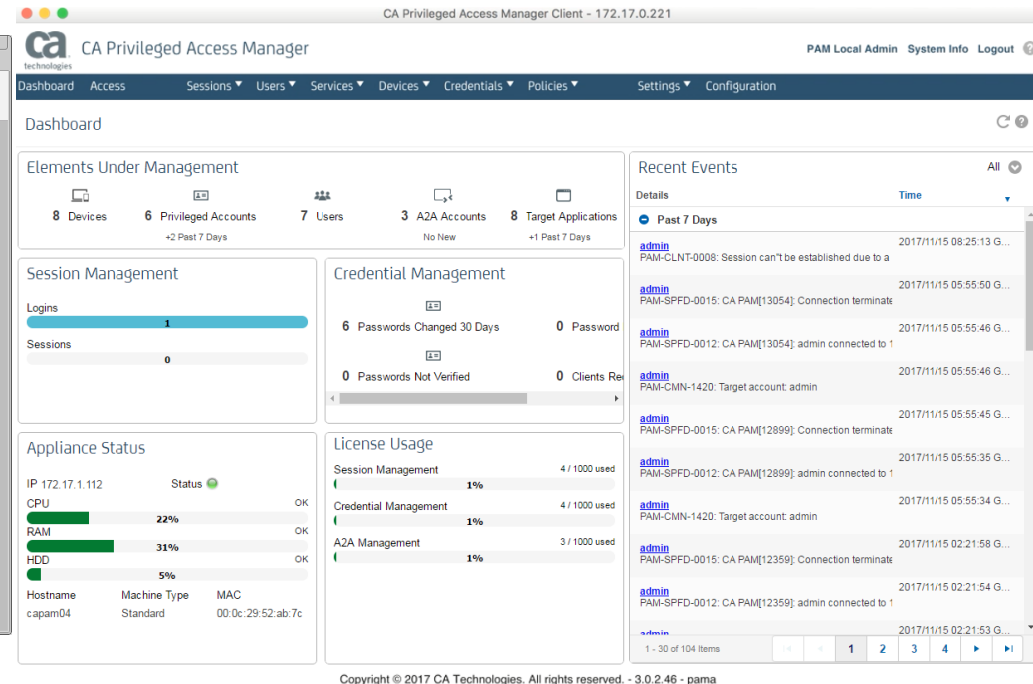


Windows/Linux/MAC 전용 Client 지원

접근제어



Login Page



Mac 전용 Client

RDP Application 접근 제한

접근제어

CA Privileged Access Manager Client - capam04.test.ca

admin admin System Info Logout

Dashboard Access Sessions Users Services Devices Credentials Policies Settings Configuration

Access

Column: Value: FILTER RESET ADD FILTER MY VIEWS RESTART SESSION

Device Name	Address	Operating System	Access Methods	Web Portal	RDP Applications	Services	Target Applications
xceedium.aws.amazon.com	xceedium.aws.amazon.com	Other		AWS CONSOLE			
AWS-SEOUL-WINODWS01 (i-038b92fc9c7513f5d)	ec2-13-124-54-163.ap-northeast-2.compute.amazonaws.com	Windows 2008	RDP				
AWS-SEOUL-LINUX01 (i-02957072c9c70dabc)	ec2-13-125-45-67.ap-northeast-2.compute.amazonaws.com	Linux	SSH				
apikey.xceedium.com	apikey.xceedium.com	Other					
1.254-WIN-AD-SQL	172.17.1.254	Windows 2012	RDP		MS-SQL 2014 MGMT CONSOLE	FILEZILLA	

Win2012 서버에 RDP 접근을 MSSQL Management Studio 2014로 제한

Microsoft SQL Server Management Studio (관리자)

Windows Server에 Login 후 MS-SQL Server Management Studio만 사용 가능

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

접근제어

CA Privileged Access Manager Client - capam04.test.ca

admin admin System Info Logout

Dashboard Access Sessions Users Services Devices Credentials Policies Settings Configuration

Access

Column: Value: FILTER RESET ADD FILTER MY VIEWS RESTART SESSION

Device Name	Address	Operating System	Access Methods	Web Portal	RDP Applications	Services	Target Applications
1.254-WIN-AD-SQL	172.17.1.254	Windows 2012	RDP				
apikey.xceedium.com	apikey.xceedium.com	Other			MS-SQL 2014 MGMT CONSOLE	FILEZILLA	
AWS-SEOUL-LINUX01 (i-02957072c9c70dabc)	ec2-13-125-45-67.ap-northeast-2.compute.amazonaws.com	Linux	SSH				
AWS-SEOUL-WINDOWS01 (i-038b92fc9c7513f5d)	ec2-13-124-54-163.ap-northeast-2.compute.amazonaws.com	Windows 2008	RDP				
Splunk Server	www.splunk.com	Other					
xceedium.aws.amazon.com	xceedium.aws.amazon.com	Other					

SELECT

- ✗ Splunk (Learn)
- Splunk

Learn mode for Web SSO: Splunk

Login | Splunk

splunk>enterprise

Username Sign in

- Mark Accountname Field
- Mark Password Field
- Mark Submit Button
- Copy
- Paste
- Back
- Forward
- Reload
- Print

First time signing in?
© 2005-2015 Splunk Inc. Splunk

Copyright © 2017 CA Technologies. All rights reserved. - 3.0.2.46 - capam04

VMware vCenter 콘솔 (HTML5) 접근 연동

접근제어

The image displays two overlapping windows. The left window is the CA Privileged Access Manager interface, showing a table of devices and a dropdown menu for selecting a web portal. The right window is the vSphere Client interface, showing the vCenter console for a specific VM.

CA Privileged Access Manager - 172.16.33.232

CA Technologies CA Privileged Access Manager

Dashboard Access Sessions Users Services Devices Credentials Policies

Access

Column: Value: FILTER RESET ADD FILTER

Device Name	Address	Operating	Access Methods	Web Portal
vCenter	172.16.33.100	Other		

SELECT

- vCenter_Console-flash
- vCenter_Console-flash
- vCenter_Console-HTML5
- vCenter_Console-HTML5

vCenter_Console-HTML5

vSphere - JBIZ-CA-Wi...

인벤트리에 라이선스가 만료되었거나 곧 만료되는 vCenter Server 시스템이 있습니다. 라이선스 관리 세부 정보

vm vSphere Client 메뉴 검색 Administrator@VSPHERE.LOCAL

JBIZ-CA-Windows 작업

요약 모니터 구성 사용 권한 데이터스토어 네트워크

네트워크 VMnet_MGMT

스토리지 GIT-NAS vsanDatastore

vSphere HA 보호: 보호됨

VM 스토리지 정책

태그

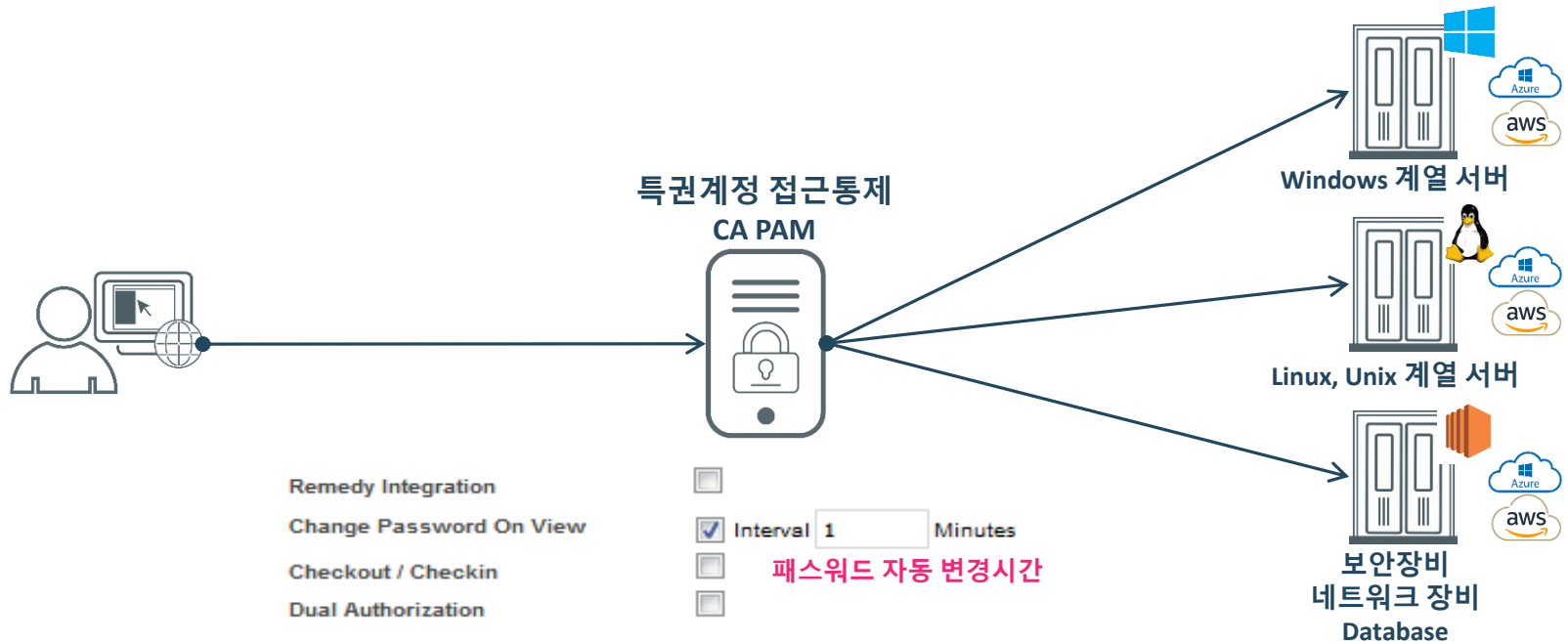
할당된 태그	범주	설명
Xsuiteignore	Vsphereinte...	

최근 작업 정보

Copyright © 2018 CA Technologies. All rights reserved.

패스워드 관리 정책

패스워드 관리



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)

AS-IS (개념도)



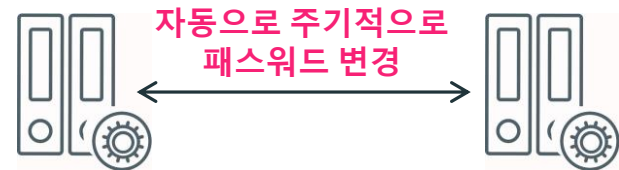
Application (CS, WEB 등)

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



관리자



CA PAM



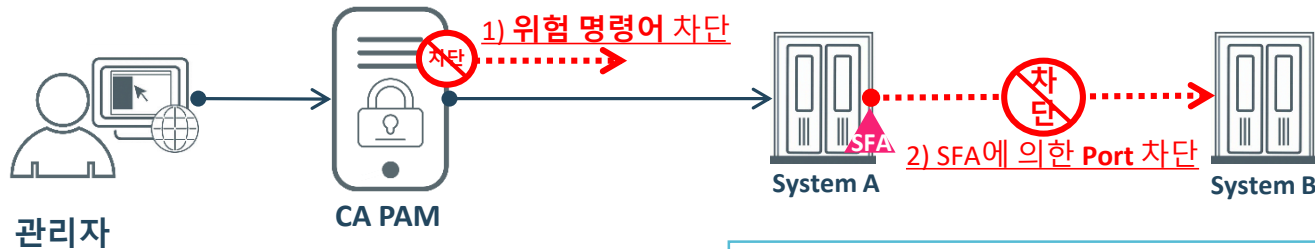
Time of event	Description
15:58:46	Blocked Acce...
15:58:59	Blocked Acce...
15:59:36	Blocked Acce...
15:59:49	Blocked Acce...
15:59:56	Blocked Acce...
16:00:11	Blocked Acce...
16:00:14	Blocked Acce...
16:00:16	Blocked Acce...

총 8회 위반 기록

위반 발생 시점 표시

- ✓ 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 타이핑 관리와 프로토콜 레이어 기반 녹화로 효율적인 녹화 파일 크기 제공

명령어 통제 / 경유 접속 차단



Add Socket Filter

Name: * Socket Filter Blacklist

Type: * Blacklist

Whitelist

Whitelist

Enter a Host

IP Address/Netmask	Ports
192.168.0.0/24	22.3389.23

- **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

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	

Socket Filter Agent (SFA)
상태 모니터링

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 PAM 운영고객 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

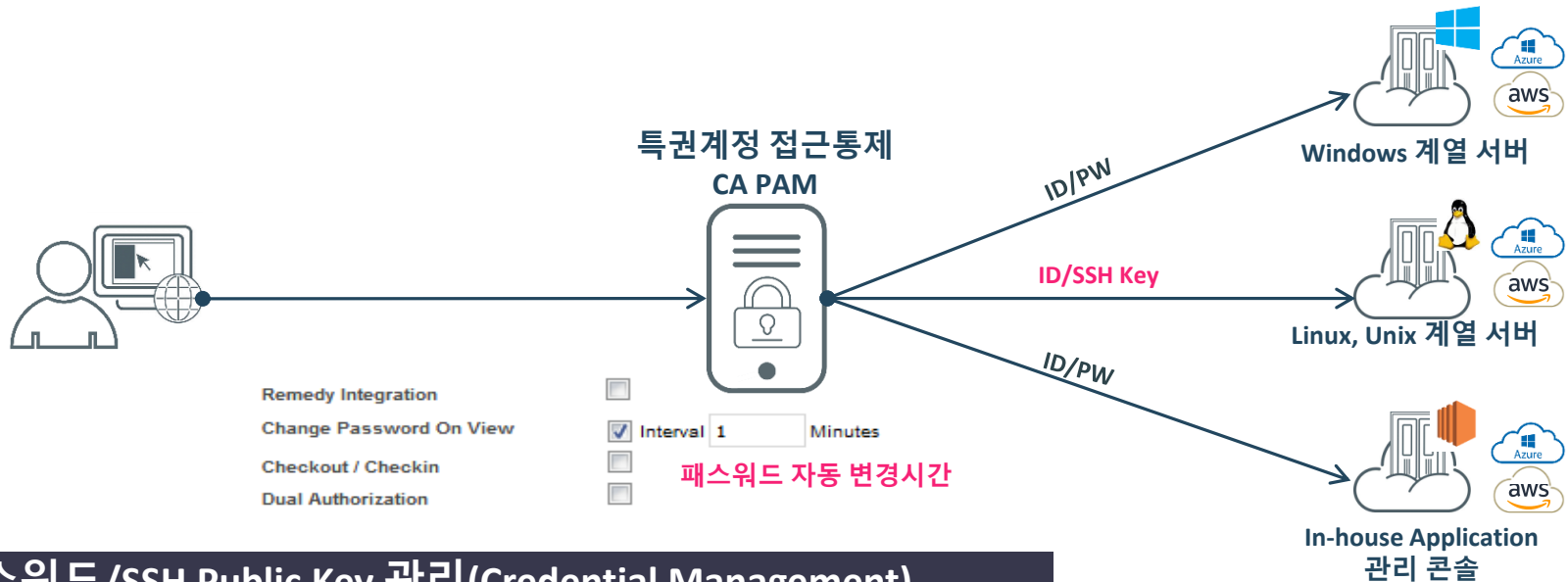


5 AWS, Azure 환경의 배포 유연성
(물리, 가상화, Cloud 지원)



6 Cloud 환경의 통합 접근 통제

패스워드/SSH Public Key 관리



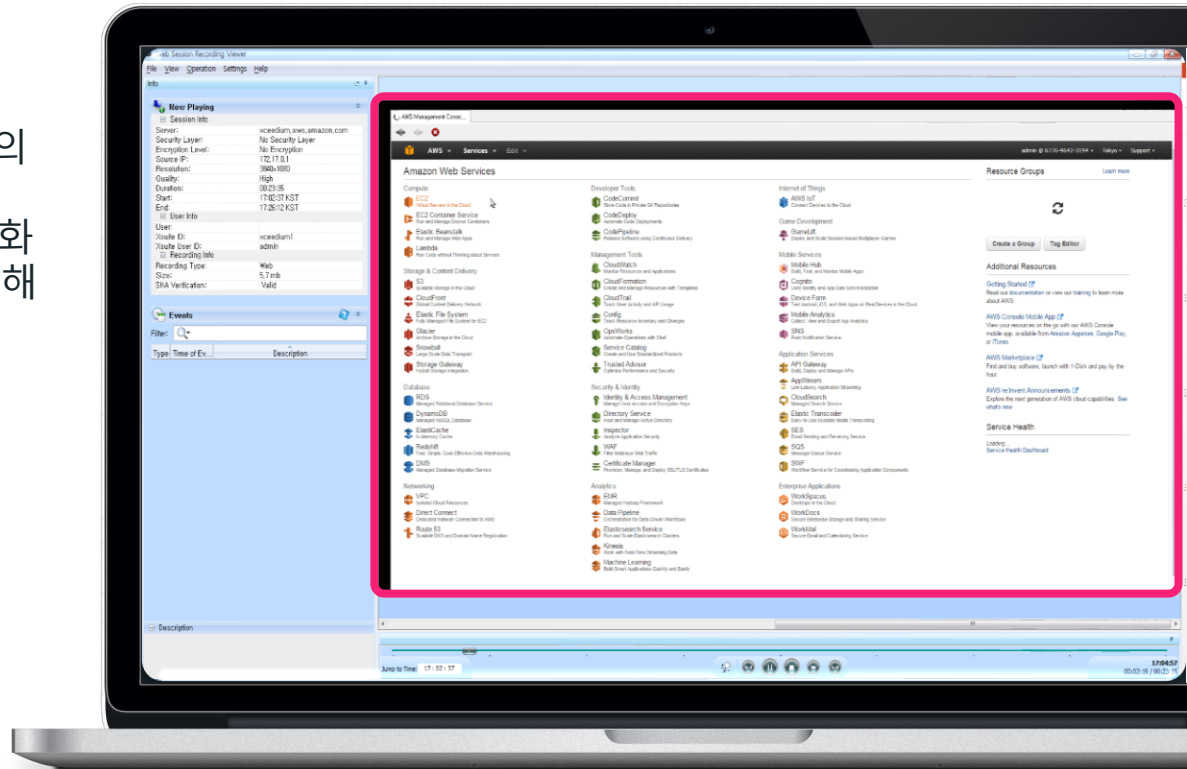
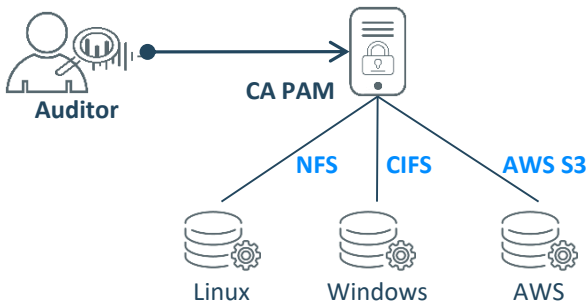
패스워드/SSH Public Key 관리(Credential Management)

- ✓ 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

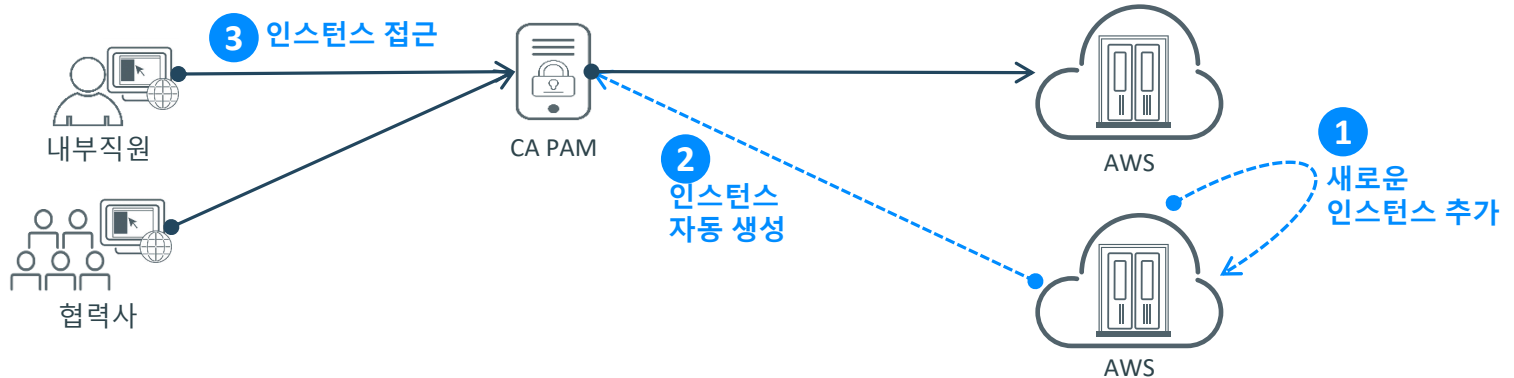
웹 관리 콘솔 활동 내역 기록

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



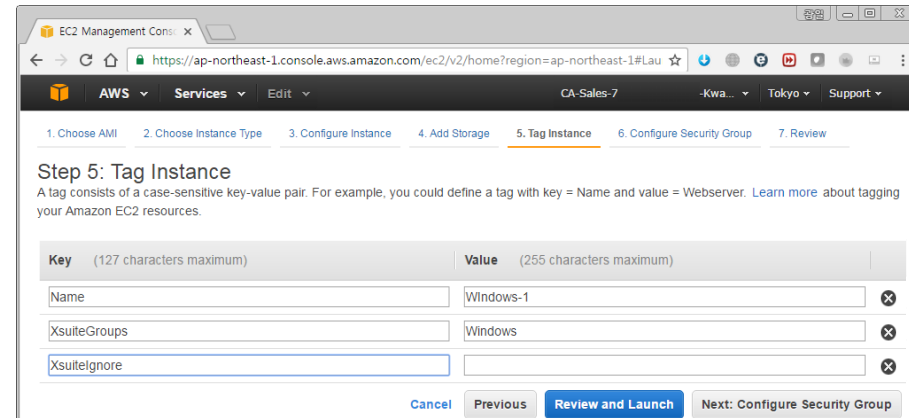
Dynamic 인스턴스 통제 및 보호



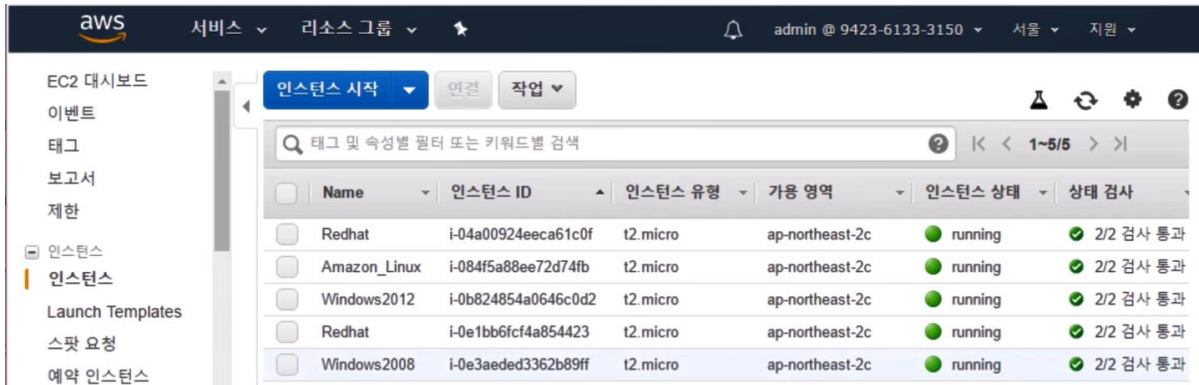
Dynamic 인스턴스 통제 및 보호

- ✓ 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



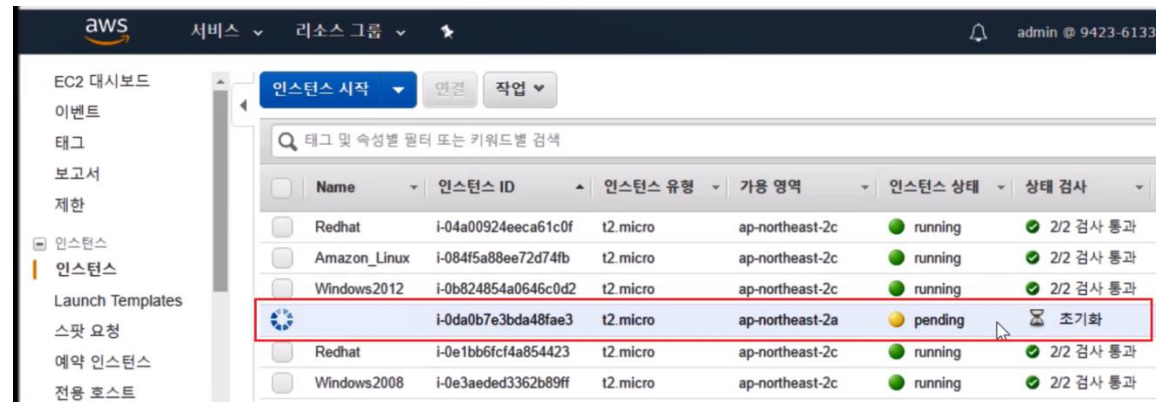
Dynamic 인스턴스 통제 및 보호(계속 1)



The screenshot shows the AWS Management Console interface. The left sidebar contains navigation options like 'EC2 대시보드', '이벤트', '태그', '보고서', '제한', '인스턴스', '인스턴스', 'Launch Templates', '스팟 요청', and '예약 인스턴스'. The main content area displays a table of EC2 instances. The table has columns for Name, 인스턴스 ID, 인스턴스 유형, 가용 영역, 인스턴스 상태, and 상태 검사. All instances listed are in a 'running' state with a green dot icon and a checkmark in the status check column.

Name	인스턴스 ID	인스턴스 유형	가용 영역	인스턴스 상태	상태 검사
Redhat	i-04a00924eeca61c0f	t2.micro	ap-northeast-2c	running	2/2 검사 통과
Amazon_Linux	i-084f5a88ee72d74fb	t2.micro	ap-northeast-2c	running	2/2 검사 통과
Windows2012	i-0b824854a0646c0d2	t2.micro	ap-northeast-2c	running	2/2 검사 통과
Redhat	i-0e1bb6fc4a854423	t2.micro	ap-northeast-2c	running	2/2 검사 통과
Windows2008	i-0e3aeded3362b89ff	t2.micro	ap-northeast-2c	running	2/2 검사 통과

1 AWS 새로운 인스턴스 추가(Auto Scaling)



The screenshot shows the AWS Management Console interface, similar to the first one. The table of EC2 instances now includes a new entry in a 'pending' state. This instance is highlighted with a red box. The 'pending' state is indicated by a yellow dot icon and the text 'pending' in the status column, with a '초기화' (Reset) button next to it.

Name	인스턴스 ID	인스턴스 유형	가용 영역	인스턴스 상태	상태 검사
Redhat	i-04a00924eeca61c0f	t2.micro	ap-northeast-2c	running	2/2 검사 통과
Amazon_Linux	i-084f5a88ee72d74fb	t2.micro	ap-northeast-2c	running	2/2 검사 통과
Windows2012	i-0b824854a0646c0d2	t2.micro	ap-northeast-2c	running	2/2 검사 통과
	i-0da0b7e3bda48fae3	t2.micro	ap-northeast-2a	pending	초기화
Redhat	i-0e1bb6fc4a854423	t2.micro	ap-northeast-2c	running	2/2 검사 통과
Windows2008	i-0e3aeded3362b89ff	t2.micro	ap-northeast-2c	running	2/2 검사 통과

Dynamic 인스턴스 통제 및 보호(계속 2)

2 PAM에서 인스턴스 자동 생성

CA Privileged Access Manager

Access

Column: [] Value: [] FILTER RESET ADD FILTER MY VIEWS

Device Name	Address	Operating	Access Methods	Web Portal	RDP Applications	Services
Amazon_Linux (i-084f5a88ee72d74fb)	ec2-13-125-253-107.ap-northeast-2.compute.amazonaws.com	Linux	SSH			PUTTY
i-0da0b7e3bda48fae3	ec2-13-125-67-129.ap-northeast-2.compute.amazonaws.com	Linux	SSH			PUTTY
Redhat (i-04a00924eeca61c0f)	ec2-52-78-1-134.ap-northeast-2.compute.amazonaws.com	Linux	SSH			PUTTY
Redhat (i-0e1bb6f4a854423)	ec2-13-125-159-198.ap-northeast-2.compute.amazonaws.com	Linux	SSH			PUTTY
Windows2008 (i-0e3aed3362b89ff)	ec2-54-180-24-38.ap-northeast-2.compute.amazonaws.com	Windows 2008	RDP		MSSQL_MGMT	
Windows2012 (i-0b824854a0646c0d2)	ec2-13-125-165-249.ap-northeast-2.compute.amazonaws.com	Windows 2012	RDP			
xceedium.aws.amazon.com	xceedium.aws.amazon.com	Other				

3 인스턴스 접근 및 통제

```
ec2-user@ip-172-31-3-162:~ ***Warning: you are being m...
File Edit Plugins Help

***Warning: you are being monitored***

Connected to server running SSH-2.0-OpenSSH_7.4

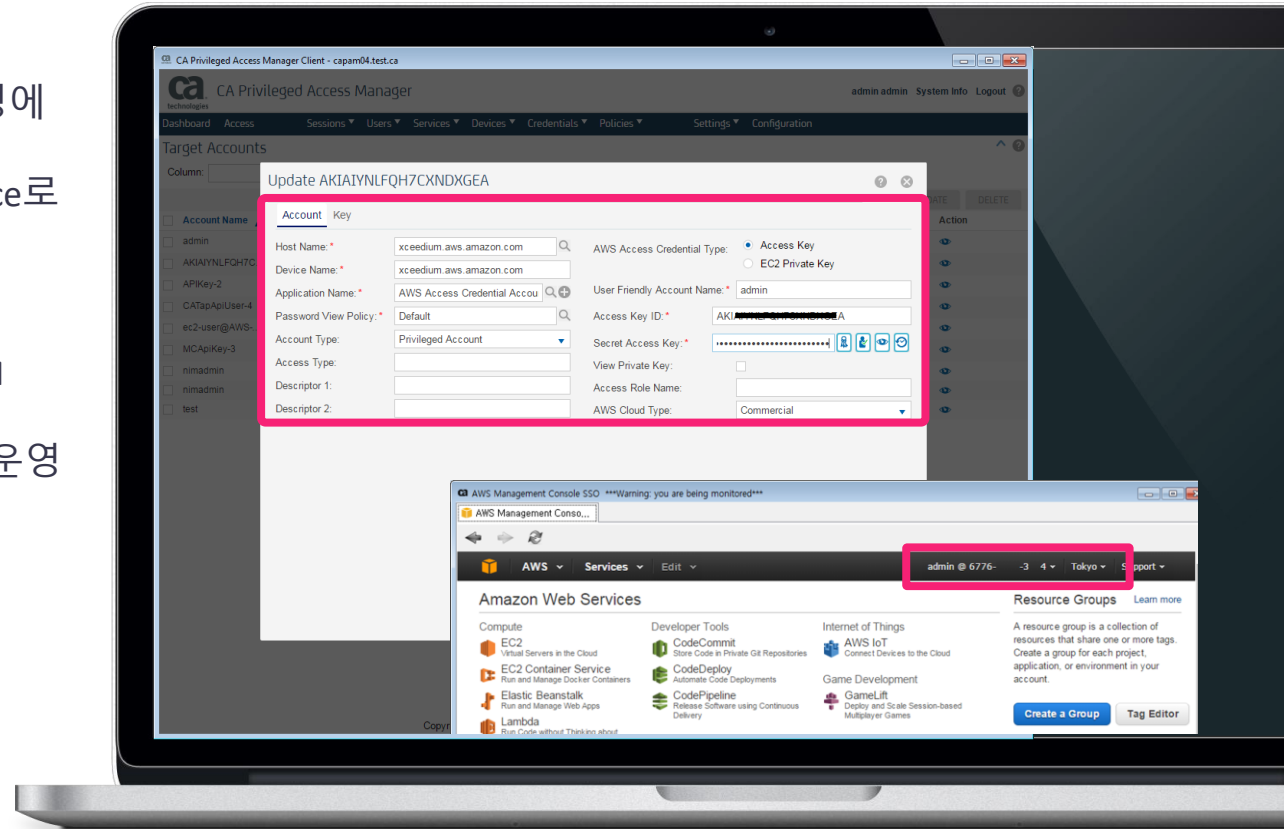
Server's hostkey (ecdsa-sha2-nistp256) fingerprint:
openssh md5: 1a:7d:49:e6:f5:96:4d:bb:13:9e:7d:f2:a9:ee:52:45
bubblebabble: xinig-katat-ryfch-fizok-nerit-hagub-fuzat-gidug-mecim-mufif-raxyx

Last login: Sun Sep 2 23:42:23 2018 from 1.220.213.138
[ec2-user@ip-172-31-3-162 ~]$
[ec2-user@ip-172-31-3-162 ~]$
[ec2-user@ip-172-31-3-162 ~]$ pwd
/home/ec2-user
[ec2-user@ip-172-31-3-162 ~]$
[ec2-user@ip-172-31-3-162 ~]$ rm
Warning: rm is an unauthorized command.
You have 1 violations. Your session will be terminated or account deactivated should violations continue.
Please contact the administrator if you have any questions
```

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

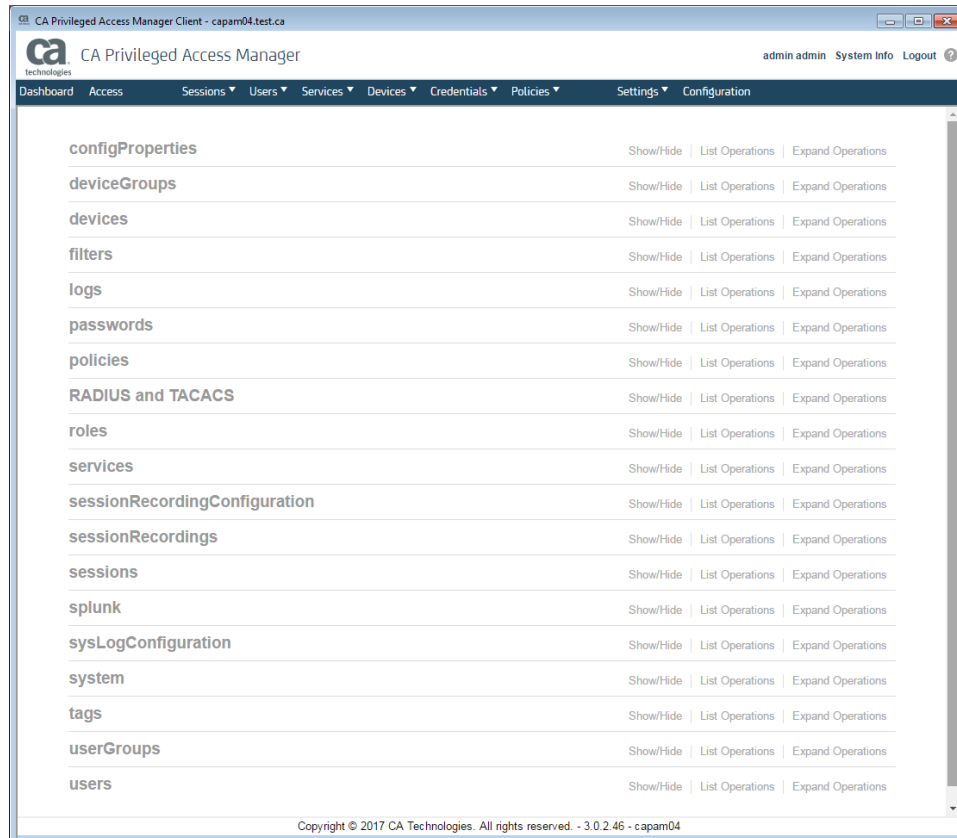


AWS 환경의 배포 유연성

- ✓ 다양한 배포 아키텍처 (On-premise / AWS/Azure)
- ✓ 통합 특권 계정 접근 관리
- ✓ AWS API 지원
- ✓ AMI 및 계정에 대한 Auto Discovery
- ✓ AWS Region별 관리 효율성



Policy Automation을 위한 External API



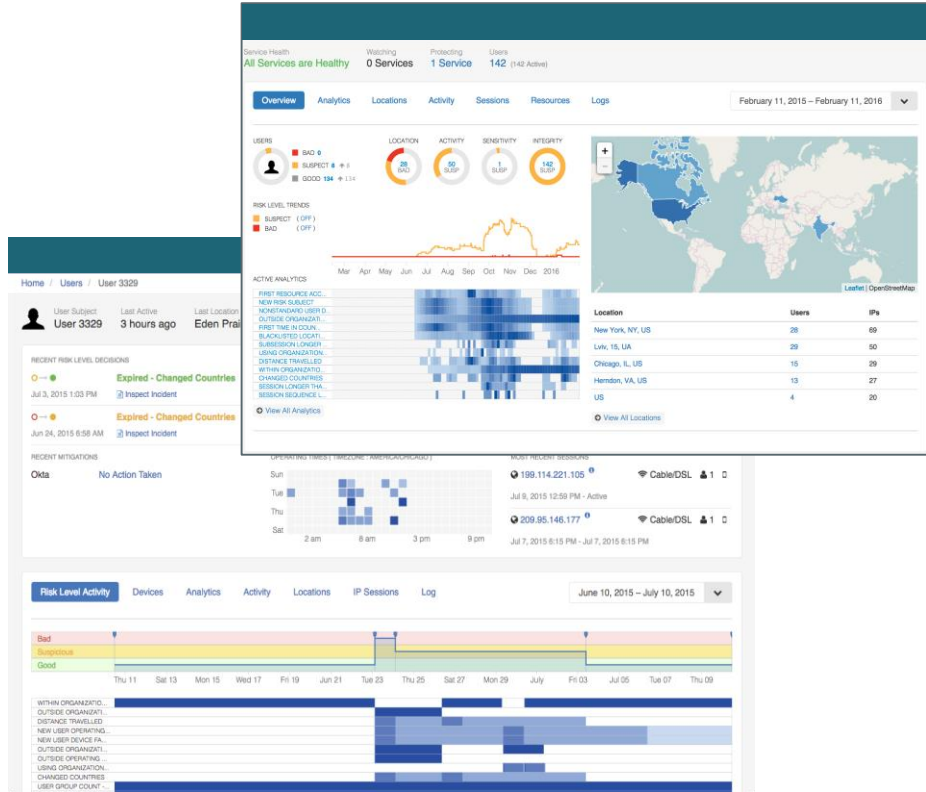
CA PAM에서의 External API

- ✓ 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

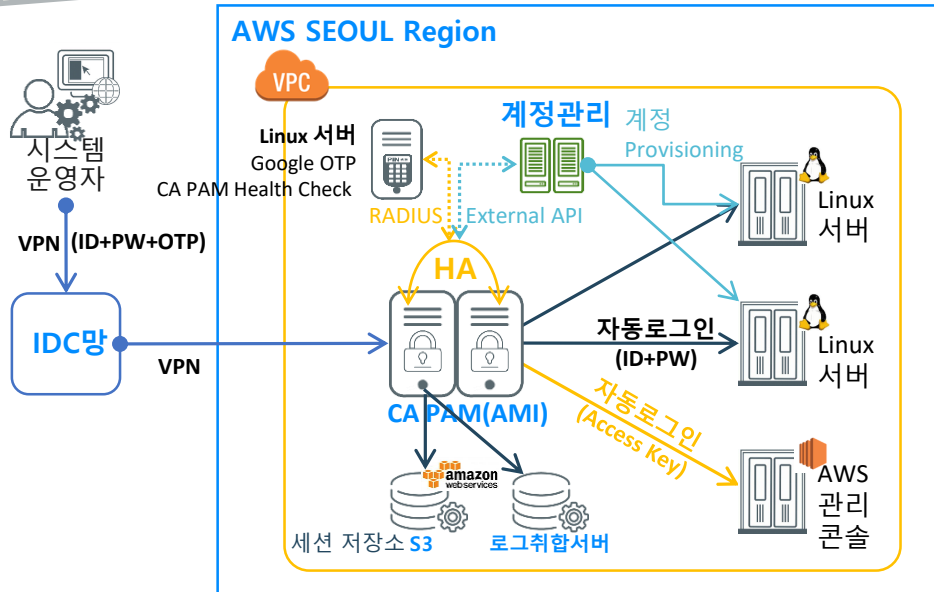
- 위협 탐지(Detection)
- 자동화된 완화 조치(Automated Mitigation)
- 운영 가시성(Operational Insights)



A 제조사 구축 사례 (CA PAM)

A 제조사 운영 환경

사업 기간 : 2018.04 ~ 현재(약 4개월)
 대상 서버 수: 총 000대
 대상 서버 종류 : Linux(000)
 운영자 : 약 000명 (00명 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.
