

Total Privileged Account Management

특권계정 및 공유계정 패스워드의 관리



Total Privileged Account Management

안전하고 자동화된 패스워드 보존 및 관리 솔루션



Quest TPAM

❖ 특권계정 패스워드 암호화 저장 장치 (Password Vault)

- 계정 패스워드를 암호화하여 저장 (AES256 암호화 프로토콜 사용) 및 디스크 전체 암호화

❖ 패스워드의 기밀성 보장

- 사용시간 경과 후 제공된 패스워드 자동 변경 (제공된 패스워드 회수)
- 정기적으로 패스워드 자동 변경

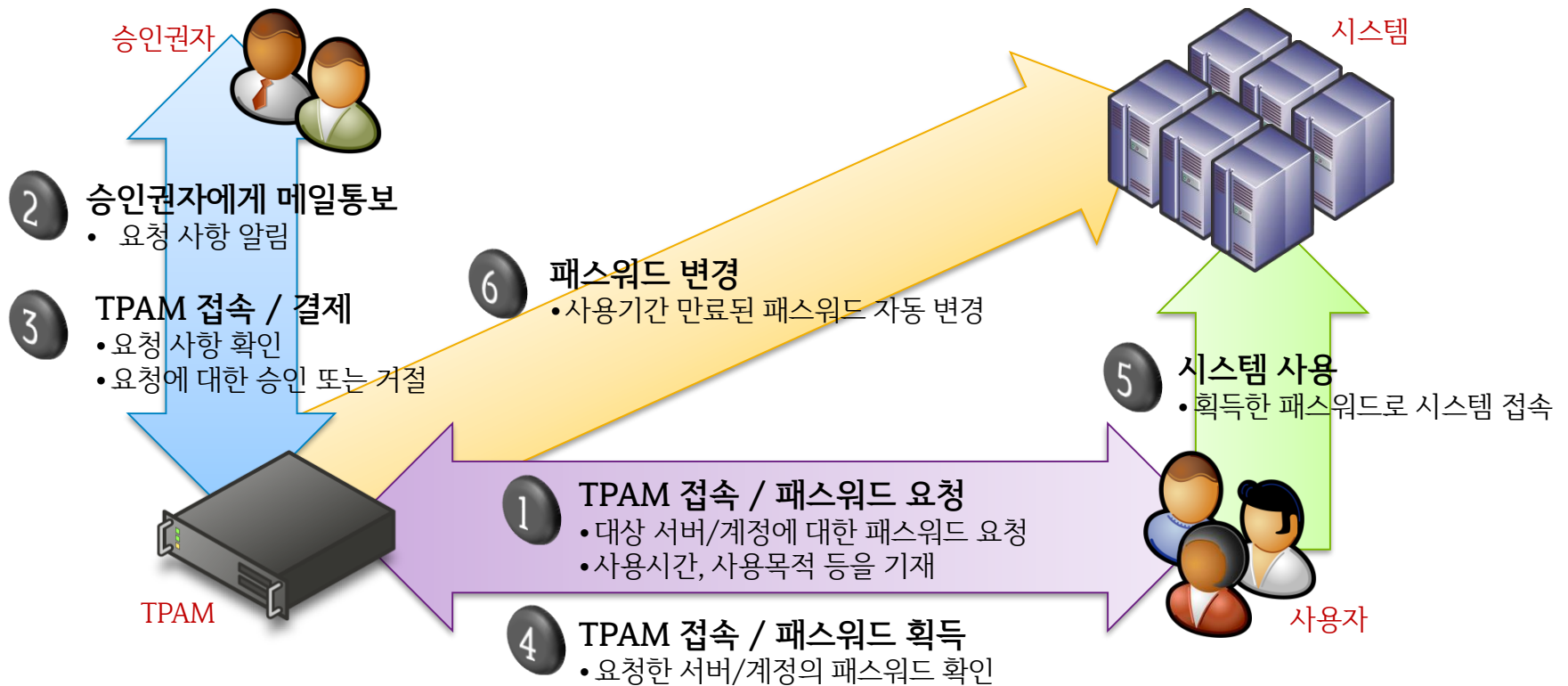
❖ 특권계정 패스워드 공유 관리

- 패스워드 공유에 워크플로우 적용
- 패스워드 변경 및 발급 이력 저장 및 보고서 생성

❖ 최상의 보안성 확보

- 콘솔 접근조차 되지 않는 어플라이언스 형태의 제품으로 공급

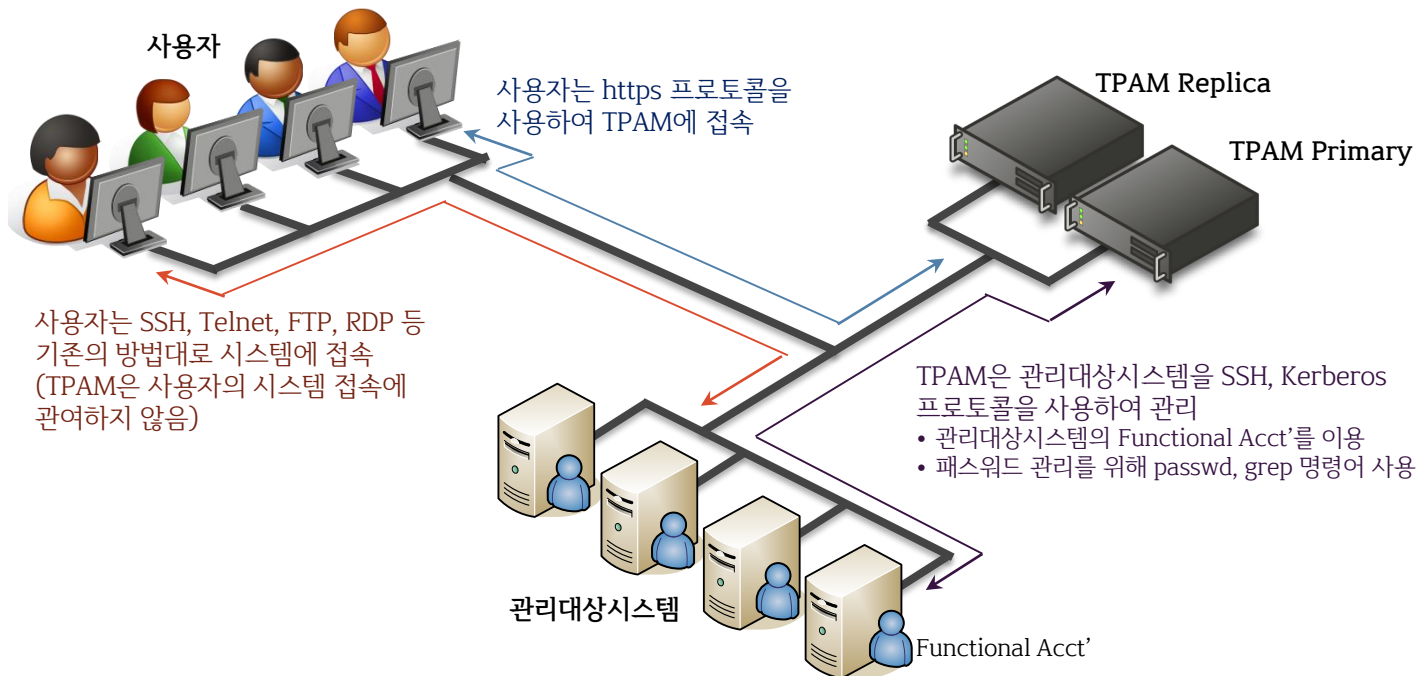
TPAM 사용방식



- ❖ 사용자에게 패스워드 발급을 위한 승인단계는 0회 이상으로 설정 가능 (0회=자동승인)
- ❖ 사용자는 승인된 기간 동안 제공받은 패스워드로 대상 서버에 여러 번 접속이 가능
- ❖ 사용자의 사용 승인 기간이 종료되면 TPAM은 해당 계정의 패스워드를 자동으로 변경 (옵션)
- ❖ 사용자의 접속 여부와 상관없이 TPAM은 관리하는 모든 계정의 패스워드를 주기적으로 변경 (옵션)

TPAM 구성 및 동작 방식

- ❖ 관리대상서버에 탑재되는 TPAM 에이전트는 없음. 단, TPAM이 관리대상서버에 접속하기 위한 전용계정(Functional Account)이 관리대상서버에 생성됨
- ❖ 사용자는 TPAM에서 제공받은 계정 패스워드를 이용하여 직접 SSH, Telnet, FTP 등을 통해 서버에 접속 (사용자가 서버에 접속 시 TPAM을 경유하지 않음)
- ❖ TPAM이 서버에 SSH 접속이 가능해야 하므로 서버가 복수의 분리된 네트워크에 분산되어 위치할 경우 물리적으로 분리된 네트워크마다 TPAM 장비가 필요



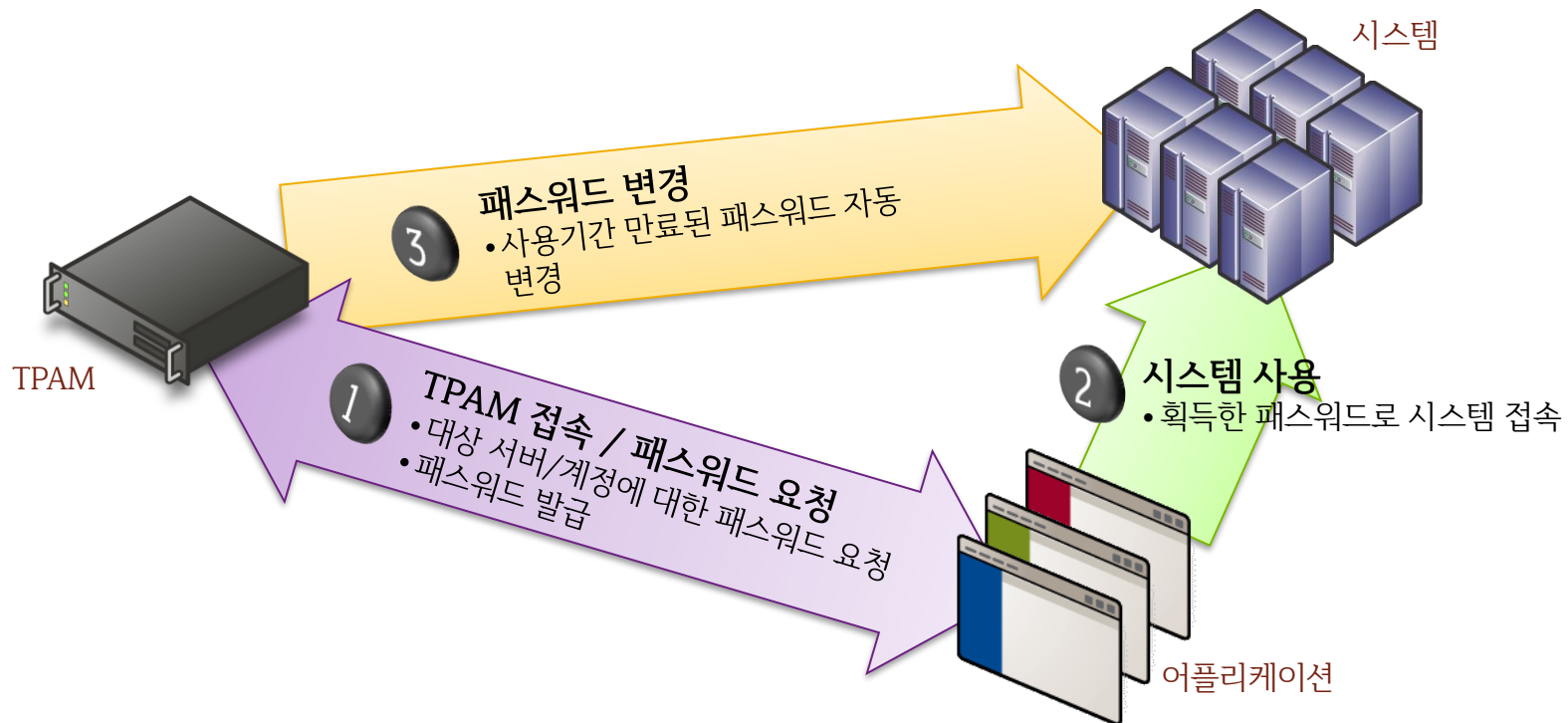
TPAM 지원플랫폼

구 분	플랫폼
OS	<ul style="list-style-type: none"> ❖ AIX, HP-UX, HP-UX Shadow, HP-UX Untrusted, Solaris ❖ FreeBSD, Linux, MAC OS X, SCO OpenServer, Tru64 Enhanced Security, Tru64 Untrusted, UnixWare, UnixWare 7.X ❖ Windows, Windows 2012, Windows Desktop ❖ AS400, HP Tandem NonStop ❖ Mainframe, Mainframe ACF2, Mainframe LDAP ACF2, Mainframe LDAP RACF, Mainframe LDAP TS, Mainframe TS ❖ Open VMS, IBM 4690 POS, Stratus VOS
DBMS	<ul style="list-style-type: none"> ❖ MS SQL Server, MySQL, Oracle, Sybase, Altibase, Tiberio
Network / Security Device	<ul style="list-style-type: none"> ❖ Cisco CatOS, Cisco PIX, Cisco Router (SSH), Cisco Router (TEL) ❖ H3C, NetApp Filer ❖ Check Point SP, CyberGuard, ForeScout CounterACT, Fortinet, Juniper (JUNOS), NetScreen, Nokia IPSO, PAN-OS, Proxy SG, SonicWALL (SonicOS)
Directory	<ul style="list-style-type: none"> ❖ LDAP, LDAPS, NIS+, Novel NDS, Active Directory
Etc	<ul style="list-style-type: none"> ❖ Dell Remote Access, HP iLO, HP iLO2, IBM HMC ❖ BoKS, PowerPassword, SAP, Teradata, VMWare vSphere 4/5

어플리케이션 내 하드코딩된 패스워드의 제거

어플리케이션에게도 실시간으로 시스템 접속에 필요한 계정 패스워드 발급

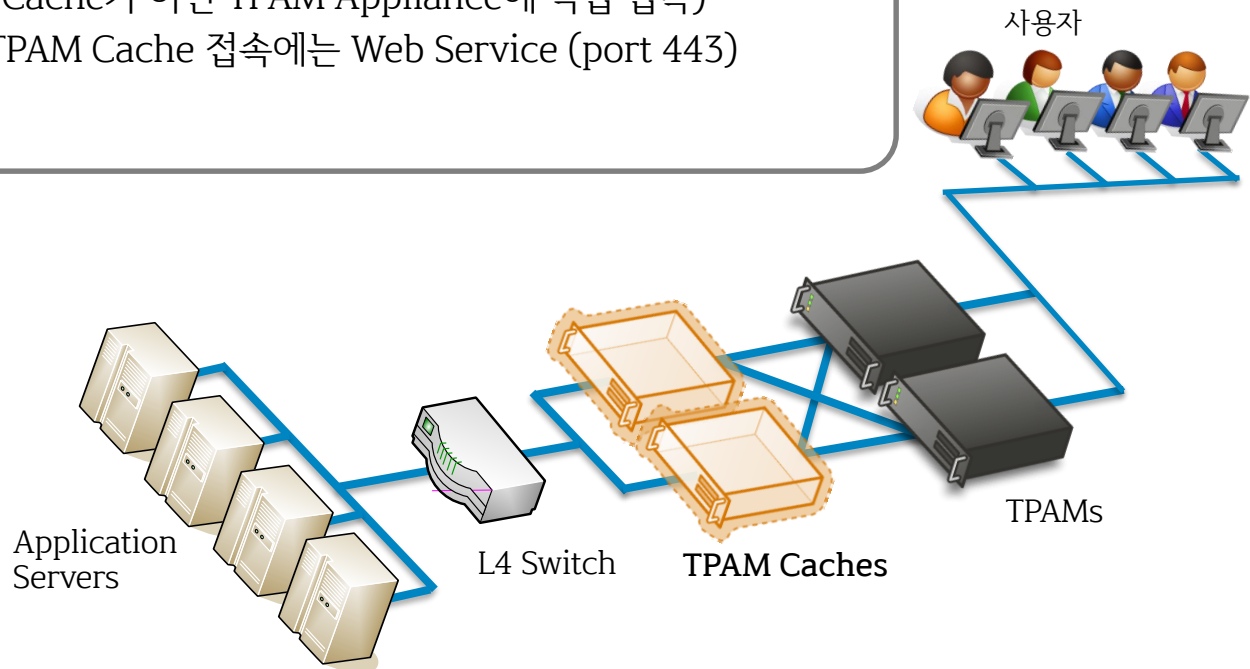
- ❖ 어플리케이션이 시스템 접속에 필요한 패스워드를 상시 내장하고 있을 필요 없음 (필요시 즉시 발급 사용)
- ❖ 어플리케이션이 TPAM에 패스워드 요청에 필요한 API 제공



어플리케이션 패스워드 요청의 고속 처리

고속 처리를 위한 TPAM Add-on Cache Appliance

- ❖ Application의 Password 요청에 대해 TPAM을 대신하여 고속 Password 응답 서비스를 제공하는 전용 Appliance (초당 1,000건 이상 처리)
- ❖ Application은 Password가 필요할 경우 TPAM이 아닌 TPAM Cache에 접속하여 Password를 신청
- ❖ TPAM Cache는 일반 사용자의 TPAM 접속에는 사용되지 않음 (일반 사용자는 TPAM Cache가 아닌 TPAM Appliance에 직접 접속)
- ❖ Application의 TPAM Cache 접속에는 Web Service (port 443) 프로토콜을 사용



어플리케이션에서의 패스워드 요청 및 발급

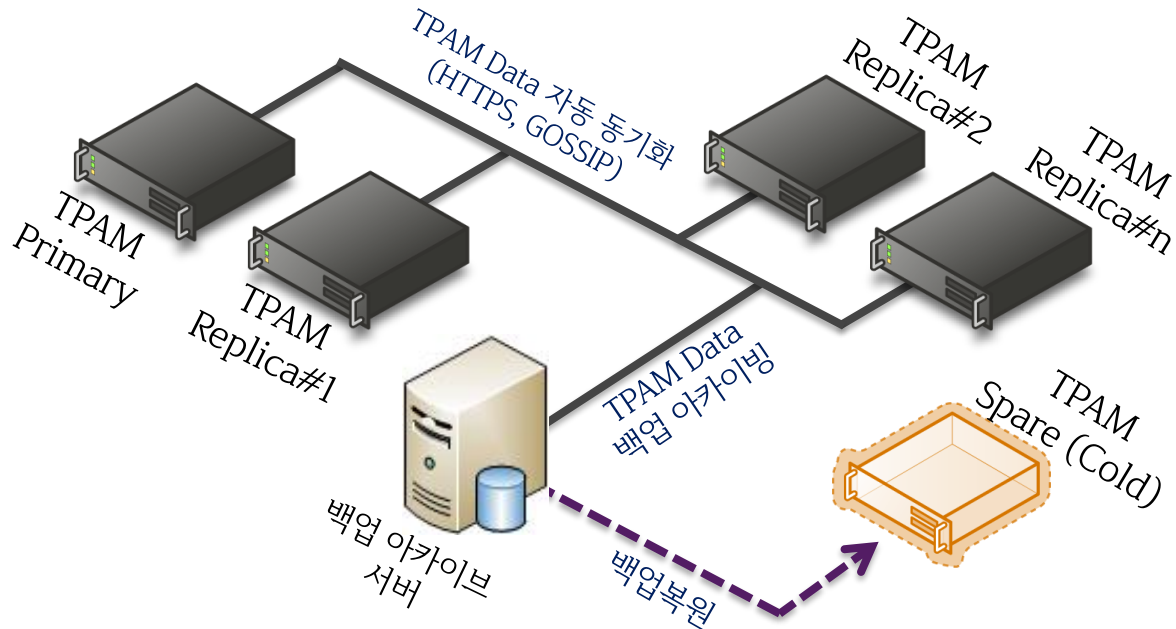
어플리케이션의 패스워드 요청 및 발급을 위한 다양한 API 제공

- ❖ Base Appliance: CLI 및 API (C/C++, Java, .NET, Perl) 지원
- ❖ Add-on Cache: Web Service 지원 (Programming Language와 상관없이 지원)

Web Service를 통한 패스워드 요청 예 (Java)

```
// Need to convert parRootCA.crt downloaded from TPAM into jks type truststore using Java's keytool.  
// keytool -importcert -trustcacerts -file parRootCA.crt -keystore truststore.jks  
System.setProperty("javax.net.ssl.keyStore", "path\wwwto\wwwcacheuser.p12");  
System.setProperty("javax.net.ssl.keyStoreType", "pkcs12");  
System.setProperty("javax.net.ssl.keyStorePassword", "CertPassword");  
System.setProperty("javax.net.ssl.trustStore", "path\wwwto\wwwtruststore.jks");  
System.setProperty("javax.net.ssl.trustStoreType", "jks");  
System.setProperty("javax.net.ssl.trustStorePassword", "TruststorePassword");  
  
HandlePWRequestService service = new HandlePWRequestService();  
HandlePWRequest port = service.getHandlePWRequestPort();  
Holder<String> pw = new Holder<String>();  
  
int rc = port.handleRequestWS("server_name", "account_name", pw);  
if (rc == 0) System.out.println("Password is " + pw.value);
```


TPAM 고가용성 확보 및 장애대응 방안



- ❖ TPAM은 고가용성을 위한 n-노드 HA(High Availability) 구성을 지원
- ❖ TPAM Primary와 각 Replica 간에는 주기적으로 자동 데이터 동기화가 이루어짐
- ❖ TPAM Primary 에서 장애가 발생할 경우 자동으로 TPAM Replica로 순차적으로 Failover됨
- ❖ Primary 장비의 데이터 백업을 외부의 스토리지에 정기적으로 자동 아카이브하여 유사시 복원 사용 가능

TPAM의 보안성 - 1

TPAM은 허가되지 않은 장비 접근 시도 및 악의적인 해킹 등으로부터 장비 내 정보를 보호하기 위해 최고 수준의 보안 기술이 적용되어 있습니다.

장비 접근 보안

- ❖ TPAM 장비에 콘솔 접속 및 로그인이 불가. 장비로의 접근은 지정된 웹 인터페이스를 통해서만 허용
- ❖ 따라서, TPAM 장비에 물리적인 접근이 가능한 사용자에 의한 TPAM OS 또는 내부 데이터베이스 레벨의 해킹 방지

장비 자체 방화벽

- ❖ TPAM 내에 자체 방화벽을 내장하여 네트워크를 통한 외부 공격에 대한 방어

장비 내 데이터 보안

- ❖ TPAM 내에 저장된 데이터는 AES256 Encryption 프로토콜로 암호화되어 있음
- ❖ TPAM 사용자의 암호는 SHA256 Hash 및 PBKDF2 Salt 프로토콜로 암호화되어 있음
- ❖ TPAM 장비 내 하드디스크는 BitLocker Drive Encryption 프로토콜로 암호화되어 있음

TPAM의 보안성 - 2

TPAM은 허가되지 않은 장비 접근 시도 및 악의적인 해킹 등으로부터 장비 내 정보를 보호하기 위해 최고 수준의 보안 기술이 적용되어 있습니다.

장비 통신 보안

- ❖ 장비와 사용자와의 모든 통신은 HTTPS/SSLv3이 적용됨
- ❖ HTTPS 인증서는 고객사 인증서 적용 가능
- ❖ 장비와 API 통신은 DSS asymmetric 인증 기반의 SSH2가 적용됨

장비 내 DB 보안

- ❖ TPAM 내 DB 객체 또는 데이터로의 직접적인 접근 불가능
- ❖ 오직 웹 인터페이스를 통해 저장된 Stored Procedure 실행을 통한 DB 액세스만 허용되고, 별도 SQL 쿼리 실행 불가

어플리케이션 보안

- ❖ 역할 기반 접근 제어(RBAC)를 통한 권한 분리(SoD) 적용

TPAM 제공 보고서

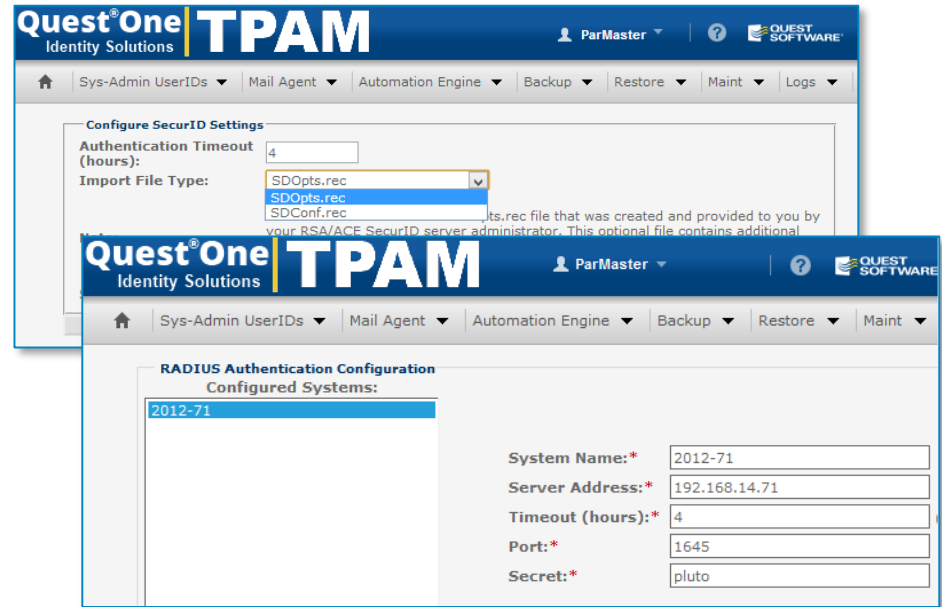
- ❖ TPAM은 패스워드 관련 컴플라이언스 및 보안 감사를 위한 다양한 보고서를 제공합니다.
- ❖ 보고서는 Excel 형태로 제공되어 쉽게 가공하여 활용될 수 있습니다.
- ❖ 보고서는 정기적으로 지정된 사용자에게 자동으로 전달되거나, 외부 문서 저장소에 자동 저장되도록 설정할 수 있습니다.

주요 보고서	설 명
패스워드 발급 요청 내역	사용자의 패스워드 발급 요청 내역 보고서
패스워드 사용 승인 내역	패스워드 발급 승인 내역 보고서
패스워드 조회 (발급)	일간, 주간 별 발급된 모든 패스워드 내역 보고서
패스워드 변경	패스워드 변경 내역 보고서
패스워드 변경 실패 (일간)	패스워드 변경 작업 실패 내역 보고서
패스워드 불일치 (일간)	임의로 무단 변경된 패스워드 내역 보고서
패스워드 특권 발급 내역	특권자에 의한 무승인 패스워드 발급 내역 보고서
사용자 권한	시스템/계정에 부여된 사용자 권한 보고서
시스템 관리 (일간)	TPAM 시스템 관리자의 모든 관리 행위 내역 보고서
시스템 사용 로그	TPAM 사용자의 모든 행위 내역 보고서

TPAM과 외부 OTP 연동

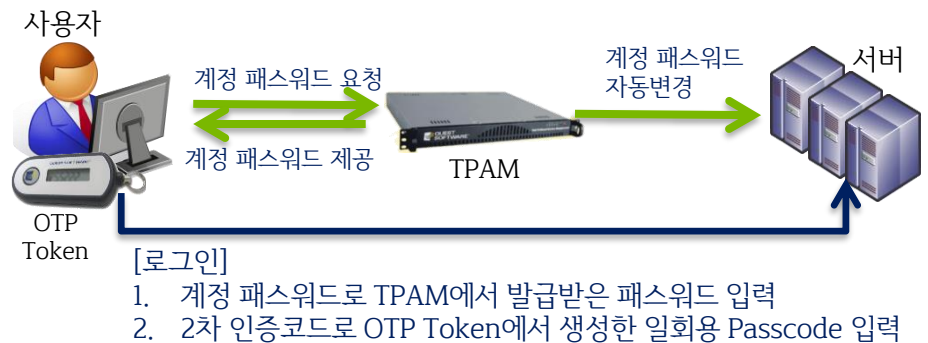
TPAM 로그인 시 외부 인증 수단으로 OTP 적용

- ❖ TPAM은 외부 인증 수단으로 RSA SecureID, Safeword 및 표준 RADIUS OTP를 모두 지원
- ❖ TPAM의 OTP 연동은 관리자 설정 항목에서 해당 OTP 관련 설정만으로 구축 완료

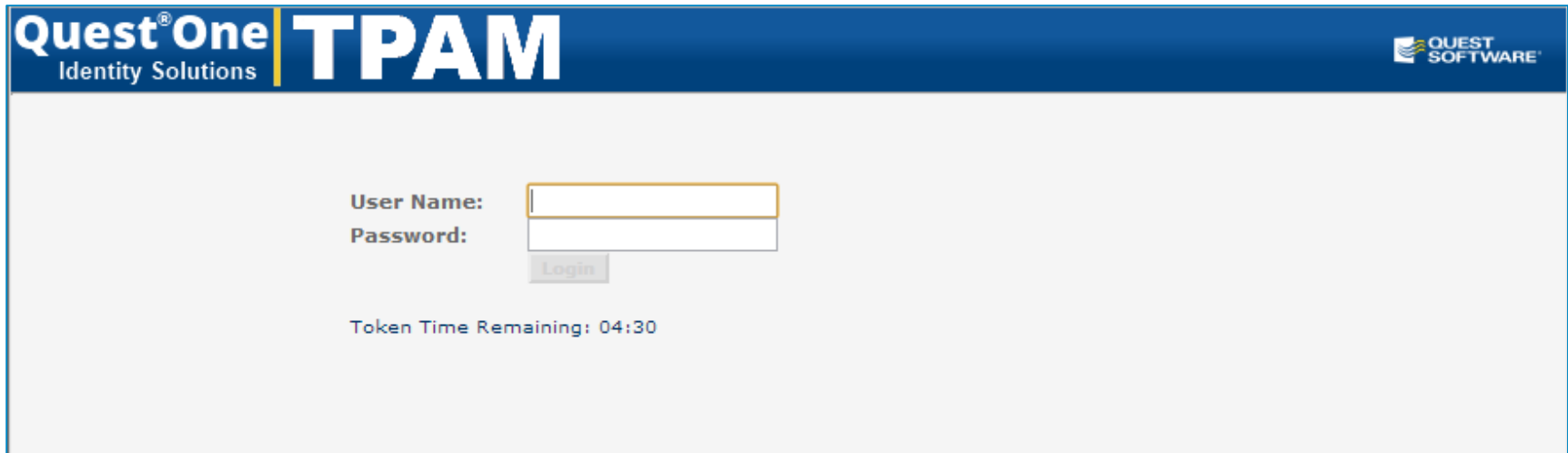


OTP가 적용된 서버 계정 비밀번호 관리

- ❖ 관리대상 서버 계정에 2차 인증 수단으로 OTP가 적용되어 있는 경우에도 TPAM으로 계정 비밀번호 관리 가능
- ❖ 이 경우 1차 인증(계정의 비밀번호 인증)은 TPAM으로부터 발급받은 비밀번호를 사용하고, 2차 인증은 OTP Token으로 생성한 일회용 Passcode를 사용 가능



TPAM 화면 예시 - 로그인



Quest[®] One Identity Solutions | **TPAM** QUEST SOFTWARE

User Name:

Password:

Login

Token Time Remaining: 04:30

- ❖ 사용자는 웹 인터페이스를 통해 TPAM에 접속 (HTTPS)
- ❖ TPAM에서의 사용자 인증
 - 1차 인증: 자체인증 또는 AD인증
 - 2차 인증: 외부 LDAP인증 또는 OTP

TPAM 화면 예시 - 패스워드 요청

Quest One TPAM
Identity Solutions

user2 | ? | QUEST SOFTWARE

Session Mgmt | Request | Approve | Reports

Password Request Management

Select accounts then click Details tab.

Filter | Listing | **Accounts** | Details | Responses | Approvers | Password

Selected	System Name	Account Name	Access Policy	Min Appr	Max Duration	Details
<input type="checkbox"/>	2008-53	quest53	P1 (REQ, APR)	1	7d:00h:00m	Approval Required
<input checked="" type="checkbox"/>	RHEL5-1	root	P1 (REQ, APR)	1	7d:00h:00m	Approval Required

- ❖ 패스워드를 요청할 계정을 선택
 - 사용자가 요청 가능한 계정만이 표시됨
 - 복수의 계정 동시 요청 가능

TPAM 화면 예시 - 패스워드 요청

Quest[®]One

Identity Solutions

TPAM

user2

QUEST SOFTWARE

Session Mgmt

Request

Approve

Reports

Password Request Management

Specify details and save changes.

Filter

Listing

Accounts

Details

Responses

Approvers

Password

☒ Request Immediate

Date/Time Required: (MM/DD/YYYY AM/PM) 11 / 17 / 2012 09 : 00 AM

Requested Duration: 0 Days 2 Hours 0 Minutes

Reason Code: Software Installation

Request Reason: Install patches

Remaining: 985

패스워드 사용 기간

요청 사유 코드 (옵션)

패스워드 요청 사유 (옵션)

Select Accounts

Sel.	System Name Account Name	Status	Max Duration	Locked? Last Released
<input checked="" type="checkbox"/>	RHEL5-1 root	Approval Required	P1 (REQ, APR) 7d:0h:0m	No n/a

패스워드 요청 대상 계정

Save Changes

New Request

Export to Excel

Export to CSV

New Accounts

Cancel

TPAM 화면 예시 - 승인자의 요청확인 및 승인

Quest[®] One Identity Solutions | **TPAM**

user3

QUEST SOFTWARE

Session MgmtRequestApproveReports

Password Requests for Approval

RequestID: 1-1 Account: **root** System: **RHEL5-1**

FilterListingDetailsResponsesApproversConflicts

Dates

Requested: 11/16/2012 5:34:48 AM

Duration: 0 D 2 H 0 M

Submitted: 11/16/2012 5:34:48 AM

Approved:

Expires: 11/16/2012 7:34:48 AM

Close:

Canceled:

Other Info

Policy: P1 (REQ, APR)

Appr Req: 1

Ticket Sys:

Ticket #:

Reason Cd: Software Installation

Requestor Info

Name: user2 (User, 2)

Phone:

Email:

Groups: Req/App Group For Col-1

Request Reason: Install patches

Request Response: * Thank you

Remaining: 246

Approve RequestDeny RequestExport to ExcelExport to CSV

승인 또는 거부

TPAM 화면 예시 - 요청자의 패스워드 확인

Quest One Identity Solutions | **TPAM** user2 ? QUEST SOFTWARE

Session Mgmt Request Approve Reports

Password Request Management

RequestID: 1-1 Account: **root** System: **RHEL5-1**

Filter Listing Accounts Details Responses Approvers Password

Surrounding "[" and "]" are not part of the password.
[0mZhh6m]

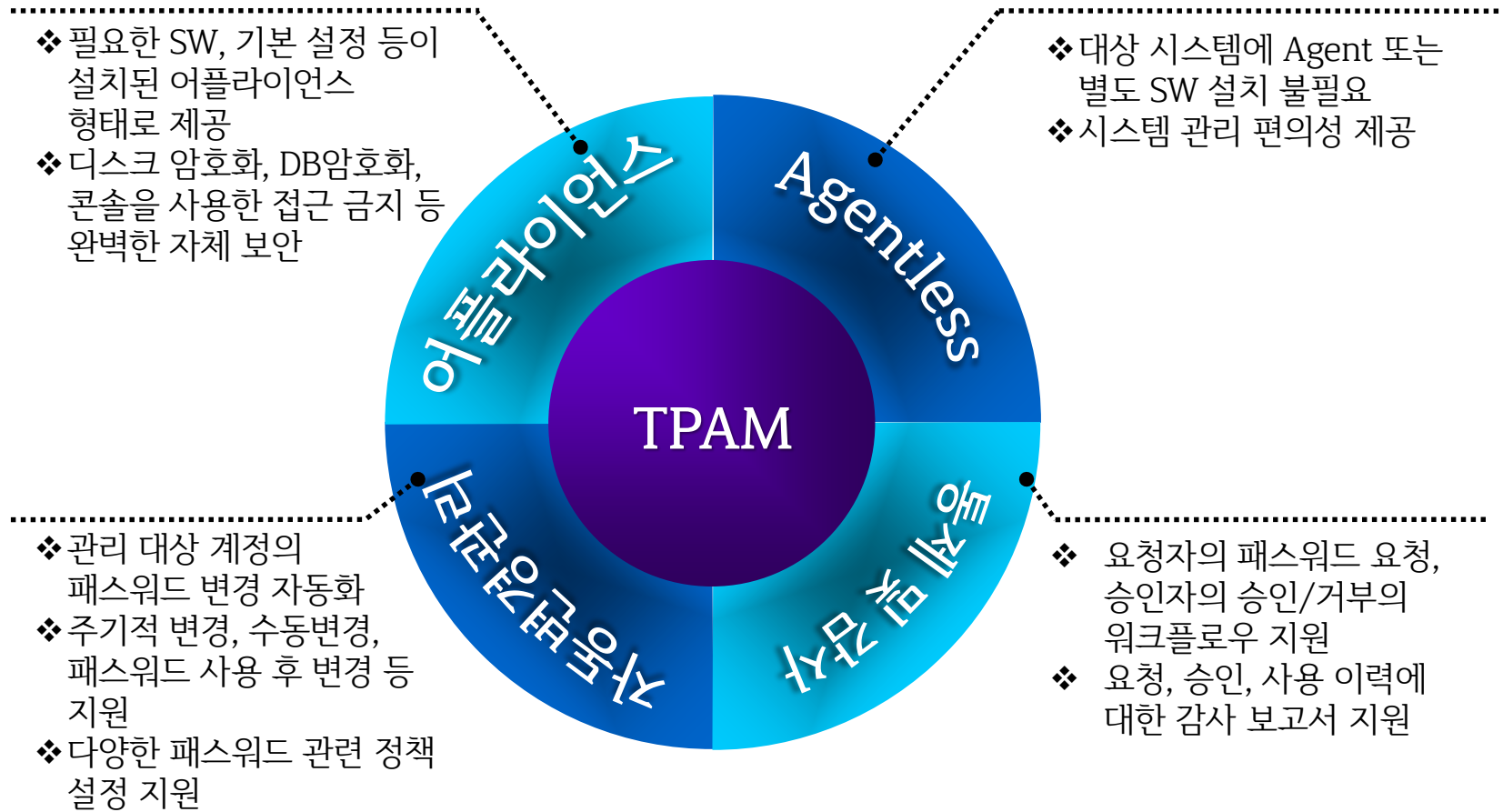
Blue Letters, Red Numbers, Uppercase i = I, Uppercase o = O, Lowercase L = l, zero/one = 0/1

This window will close in 16 seconds

Save Changes New Request Export to Excel Export to CSV New Accounts Cancel

- ❖ 요청 시 설정한 기간 동안 언제든지 패스워드 확인 가능
- ❖ 패스워드 문자열에 대한 Cut & Paste 가능

TPAM 특장점



TPAM 도입 효과

TPAM은 전문적인 패스워드 저장소 (Password Vault) 솔루션으로, 계정 패스워드의 안전한 보관 및 변경 통제를 통한 자동화된 관리를 실현합니다.



실제 시스템 접속이 필요한 사람에게 필요한 기간 동안만 시스템 접속 권한을 제공



사전 승인 후 시스템에 접속하고 사용 후 권한을 회수함으로써 권한 상시 소유 방지



시스템 패스워드는 암호화되어 전용장치에 안전하게 보존되고, 비정상적 접근이 차단



보안 규정에 따라 자동 패스워드 변경 관리

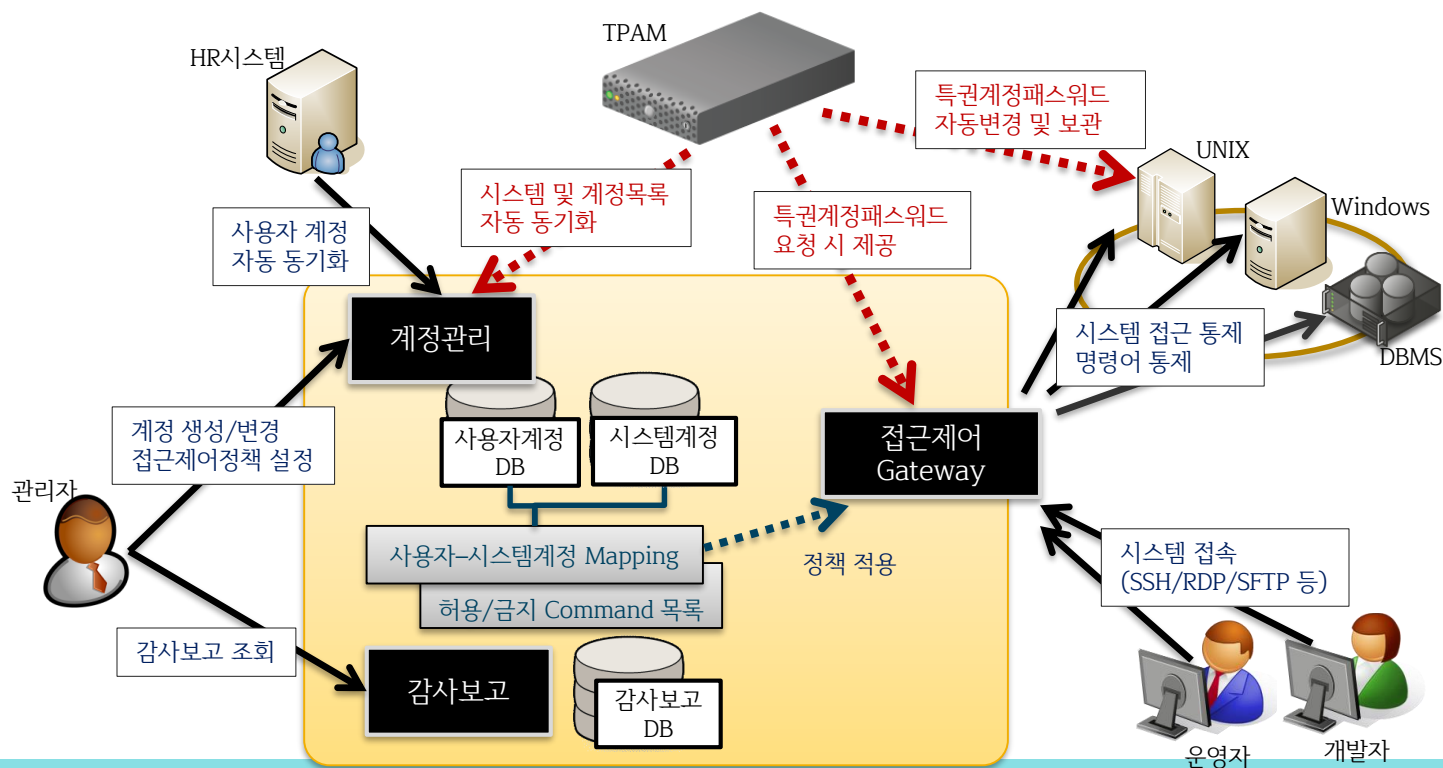


모든 접속 권한의 신청 및 부여 과정이 기록되고, 정기적 보고 및 감사 가능

접근통제(계정관리)와 TPAM 연계구축

TPAM은 접근통제(계정관리) 시스템에 특권계정의 패스워드 보관 및 관리 서비스를 제공함으로써 전체 시스템의 보안성을 획기적으로 증대시킴

- ❖ 접근통제(계정관리) 시스템은 사용자별 접근 가능 시스템의 계정 정보를 내부적으로 유지
- ❖ 보안적으로 가장 민감한 특권계정 패스워드를 TPAM에 안전하게 보관하고, 특권계정에 대한 접근 행위 필요 시 실시간으로 대상 계정의 패스워드를 TPAM으로부터 발급 받음



TPAM 주요 국내 고객사

은행



보험



보험



카드



증권/캐피탈



제조



공공

