Control access to your super user accounts

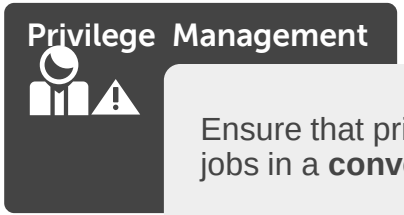
Dell Solutions Tour 2015

Ingvar Johansson, Dell Software

ingvar.johansson@software.dell.com

What is Privileged Management?

Privilege Management



Ensure that privileged users can get to the resources they need to do their jobs in a **convenient, secure, and compliant** manner

Privilege Management Challenges

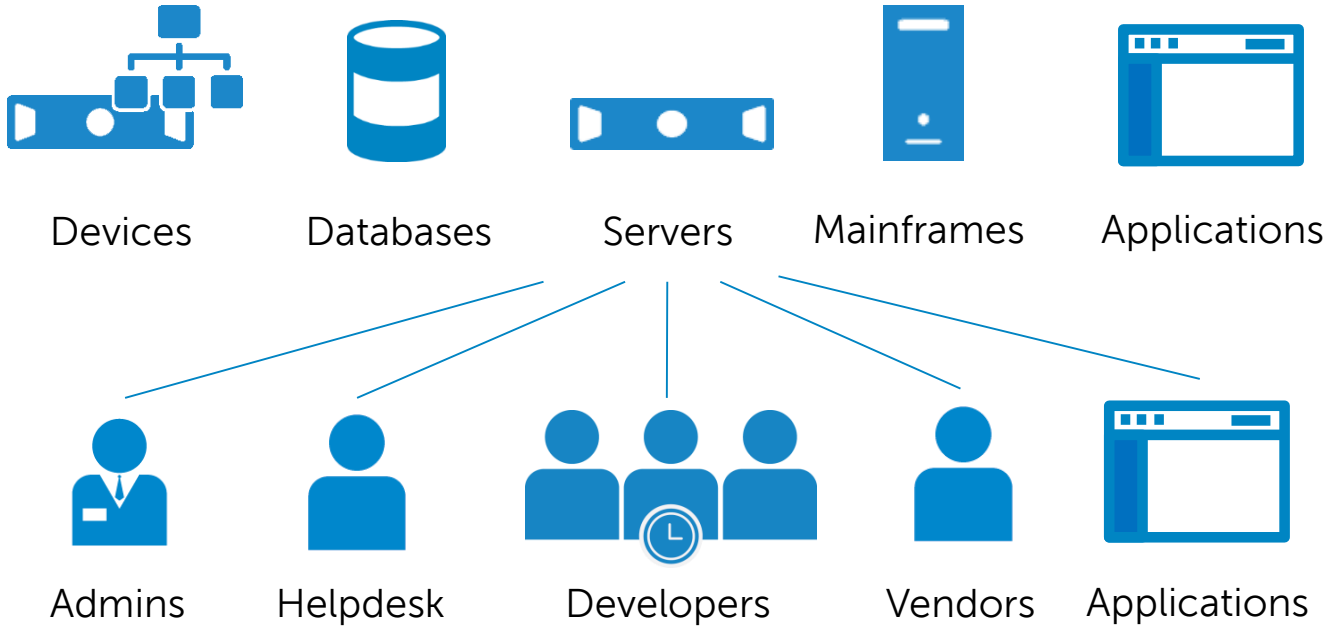
- Difficult to manage

- Huge security and compliance risk

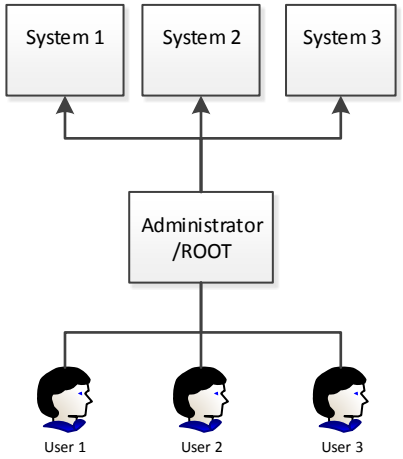
Fact: *69% of confirmed security incidents were perpetuated by insiders, and increased more than 300% between 2011 and 2012*

Fact: *More than half were former employees who regained access via backdoors or corporate accounts that were never disabled*

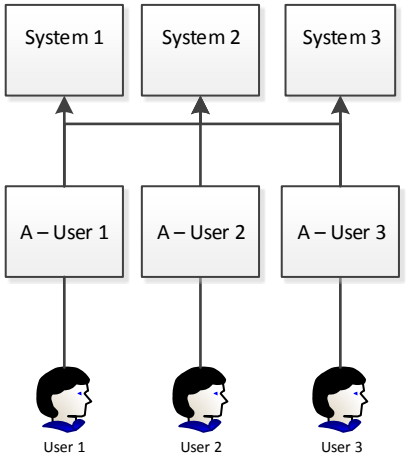
Why are they difficult to manage?



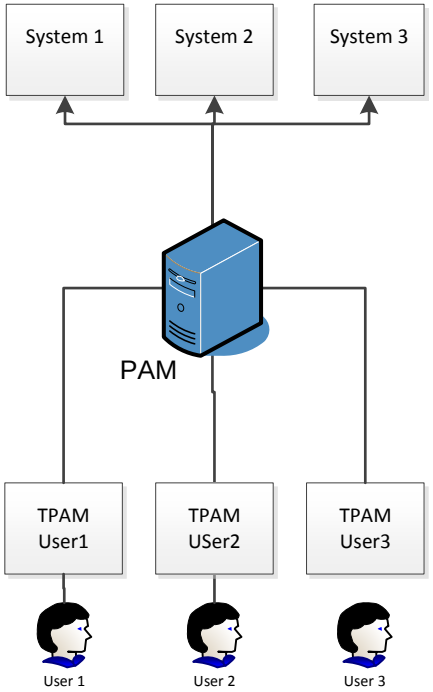
Different Approaches



Shared accounts



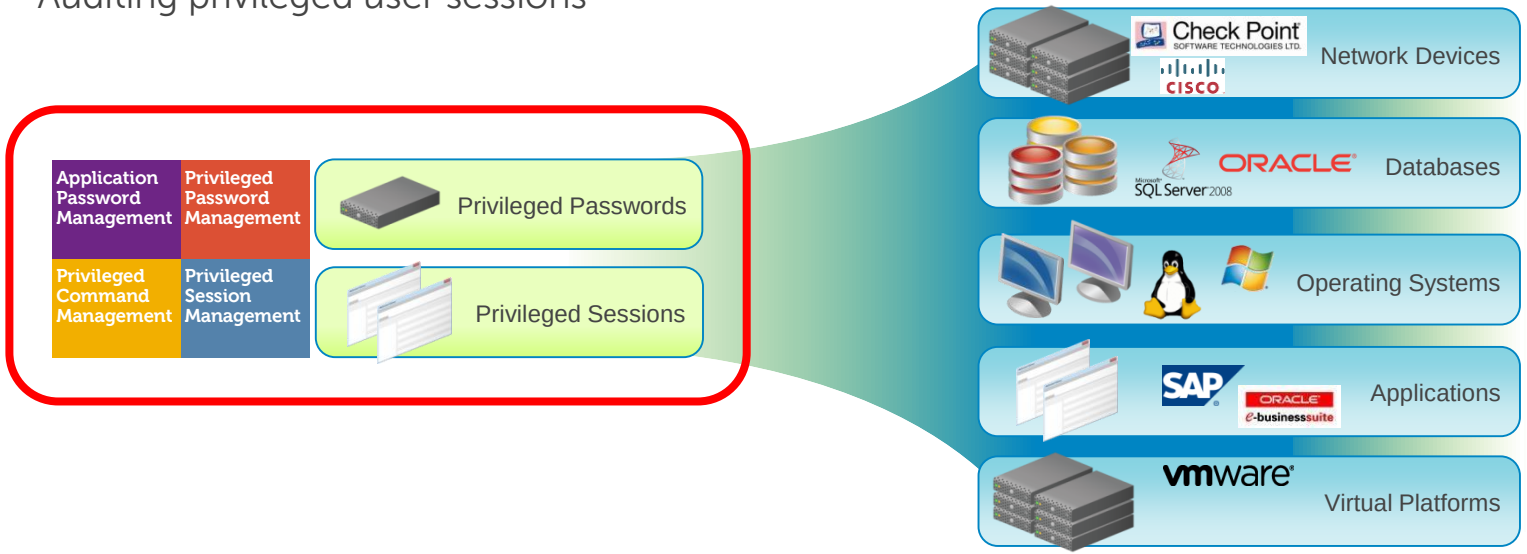
Individual privileged accounts



Managed Access

Managing Privileged Accounts

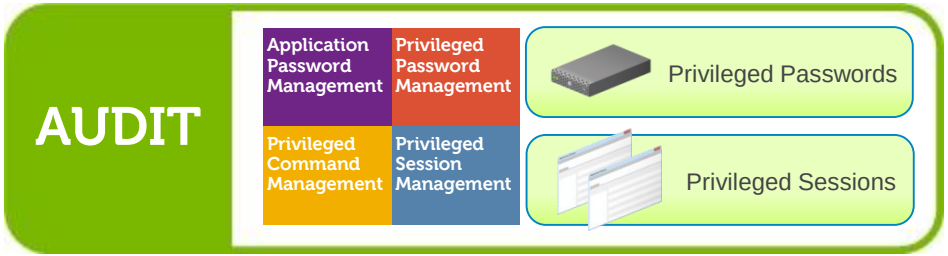
- Privileged accounts exist everywhere
- Auditing privileged user sessions



Total Privileged Access Management (TPAM) Suite

- Hardened Appliance
- Full AES Disk encryption
- Fips 140-2 & ISO 27001
- Embedded hardware firewall
- Purpose built for security
- No direct access of any kind

- Highly Available Architecture
- Scalable Clustering
- Small 1u footprint
- Hardware redundancy
- Secure audit backup
- SYSLOG integration



Privileged Password Management

Dual Release Control

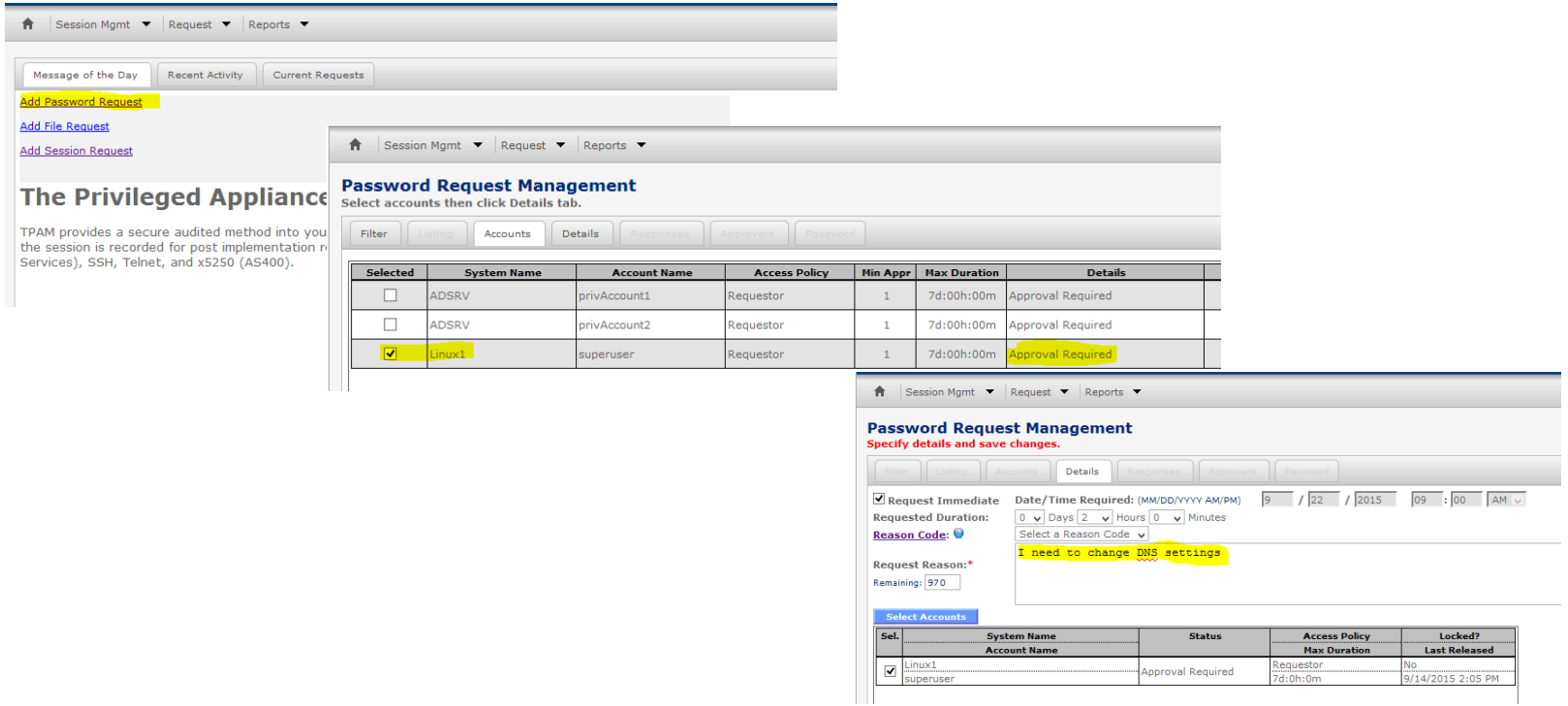
Change Control

Enterprise Integration

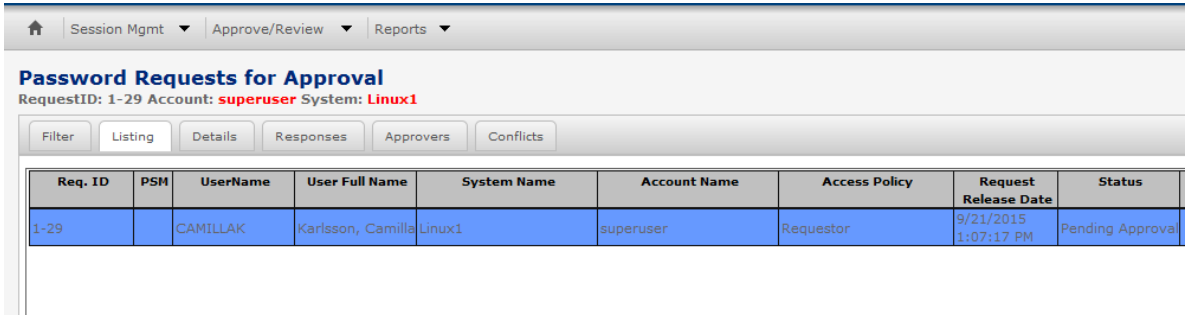
Effective Workflow

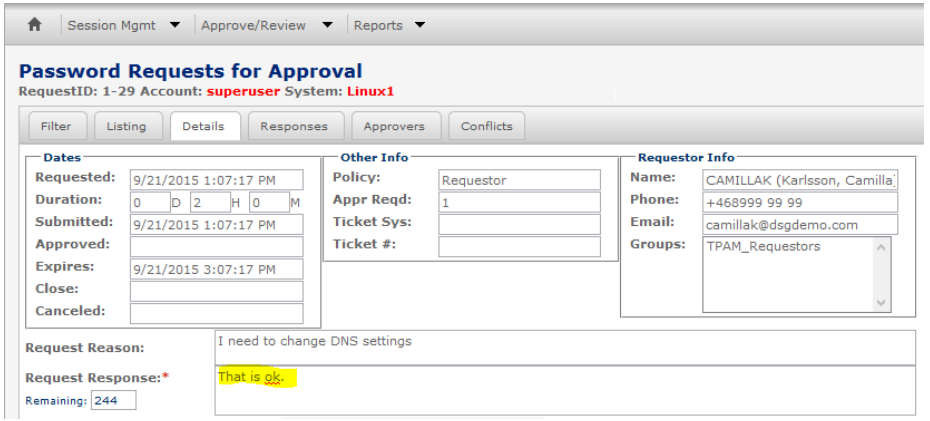
- Dual or more release controls
- Automated change control
  - Time based
  - Last-use based
  - Force change
  - Apply complexity to groups
  - Detect new systems and passwords
- Extensive integration
  - Account auto discovery
  - Conflict remediation
  - Strong authentication solutions
  - Ticketing systems

Request a password

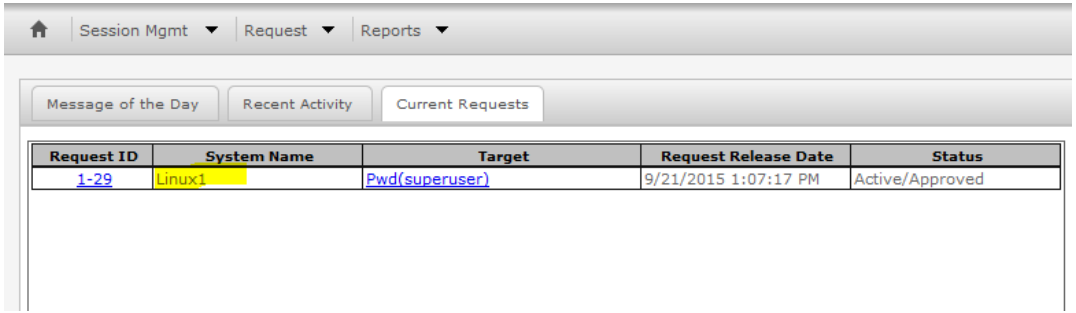


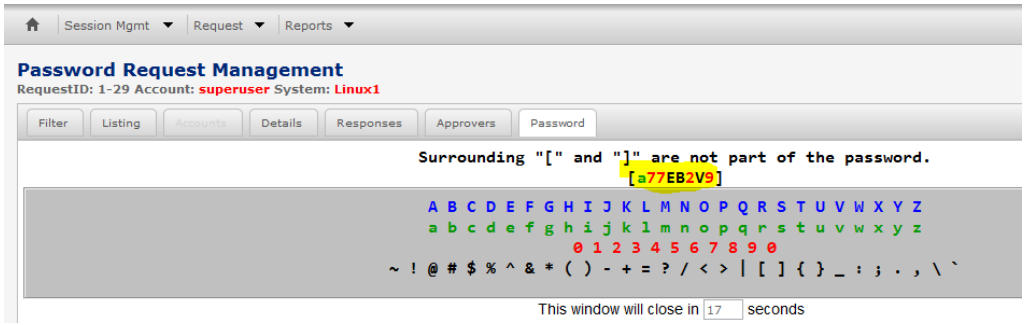
Approval: Request a password…





Release: Request a password…





Privileged Session Management

Granular access

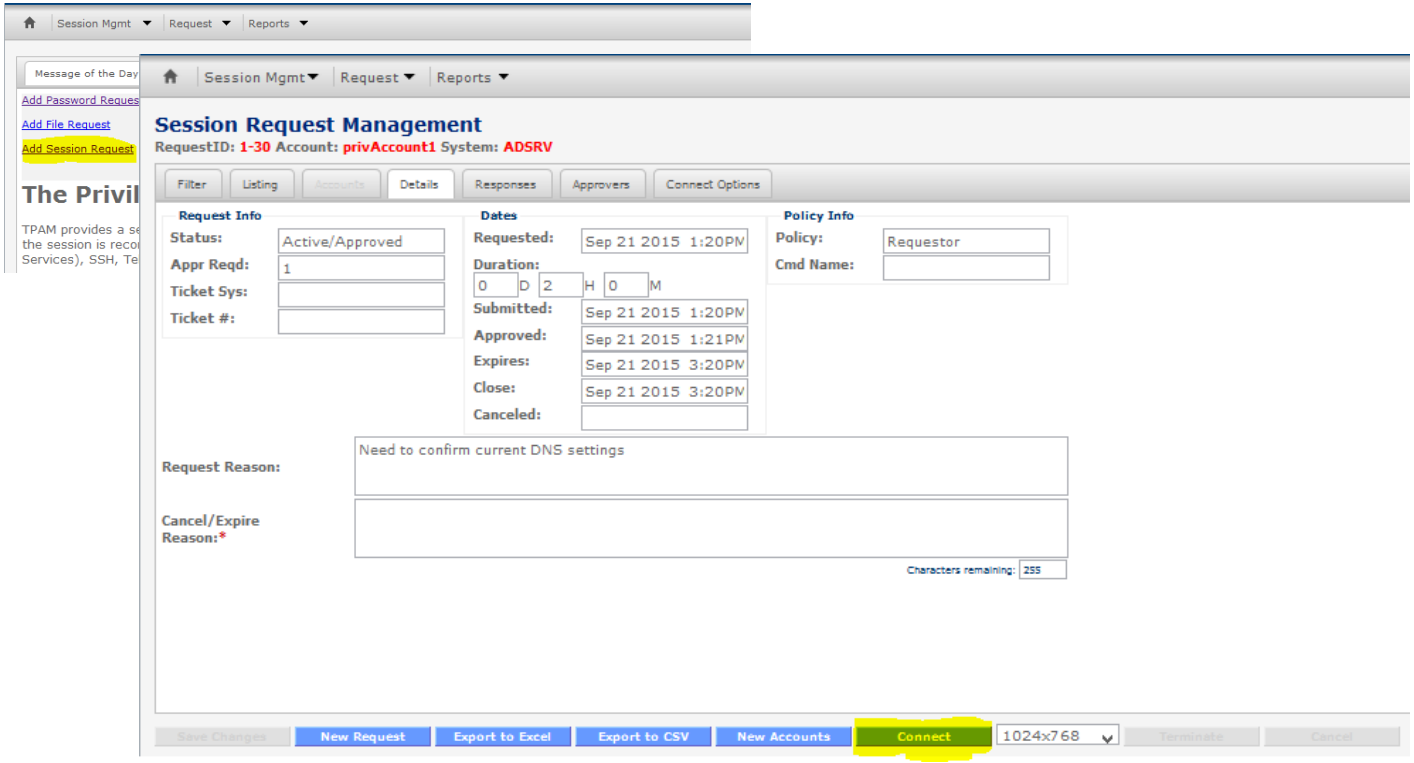
Connection Controls

Hidden passwords

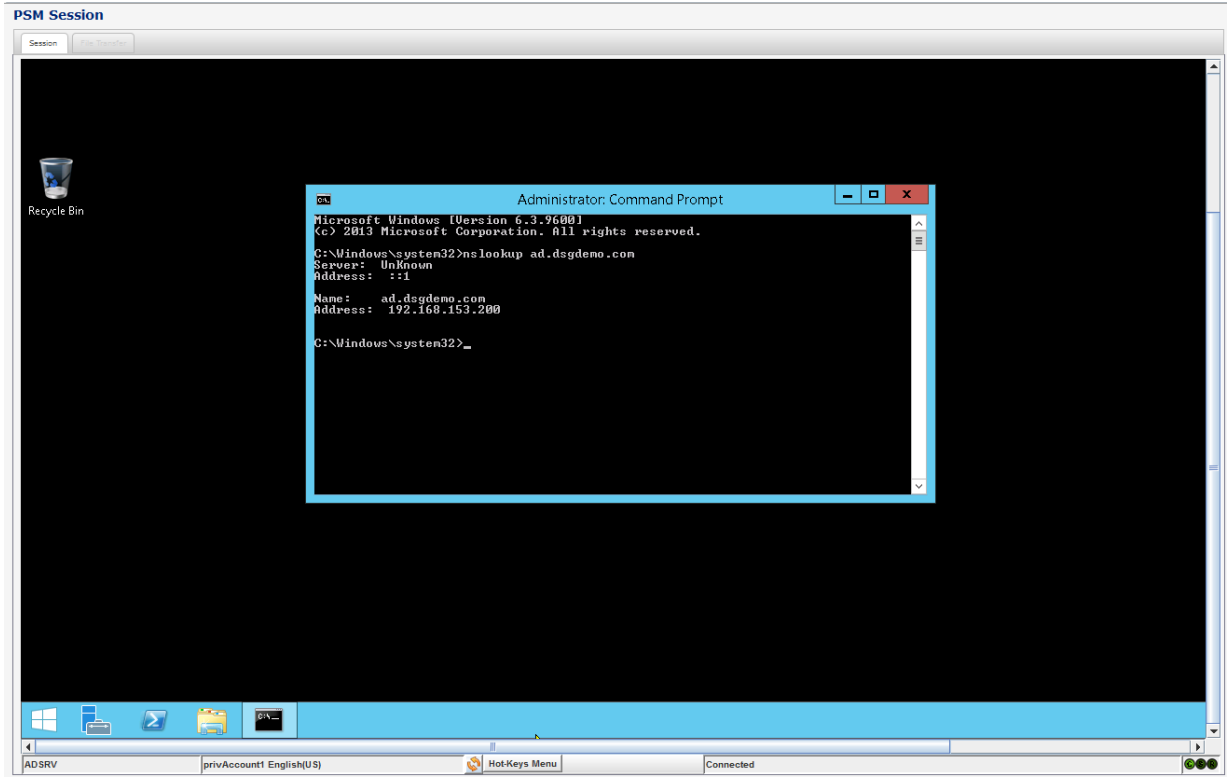
Real time monitoring

- Fine grain access control
  - Limits view based on role
- Full control over connections
  - Dual authorization controls
  - Session time limits
  - Alarm notification session overrun
  - Event logging & searching
- Remove passwords from the equation
  - Users will never need to know the password to open a session
- Monitor sessions in real time

Request a session



Privileged Session:



Application Password Management

Embedded Passwords

Connection Controls

Hidden passwords

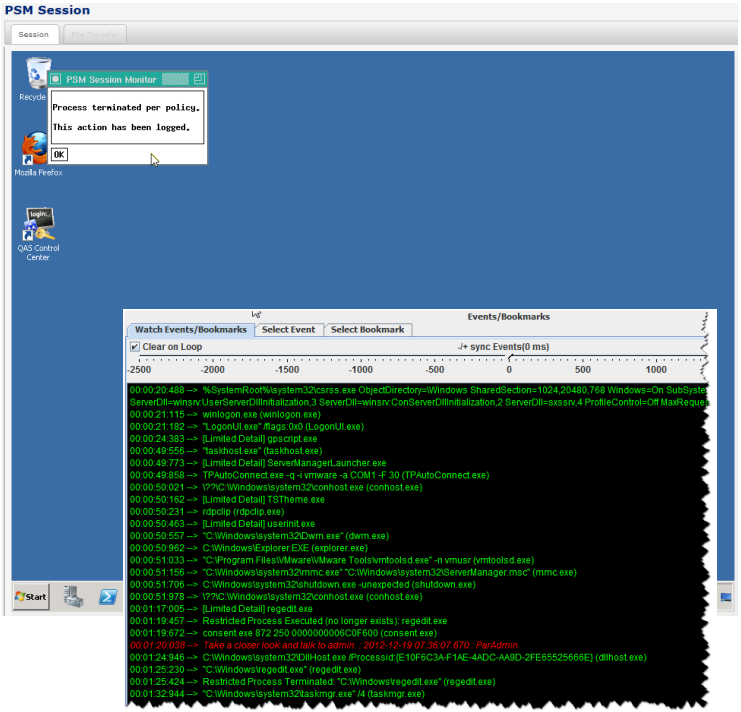
Agentless

- Replace embedded passwords
  - C/C++
  - Java
  - .NET
  - Perl
- Remove passwords from the code
  - Users will never need to know the password to open a session
  - API or CLI based
- Service Account Management
- Scheduled Task Management

Privileged Command Management

Command Control

- Command Level Access Control
  - Blacklist or Whitelist
  - Least and/or Most privileged model



Application Password Management | Privileged Password Management | Privileged Command Management | Privileged Session Management

Classes of Appliance

Base Appliance

- All Core Functionality
  - Logging
  - Configuration
  - Policy Enforcement
  - HTTPS Hosting
  - API/CLI point of access
- Up to 20 Concurrent Sessions
- Account limits
  - 25,000 standard
  - 250,000 Enterprise

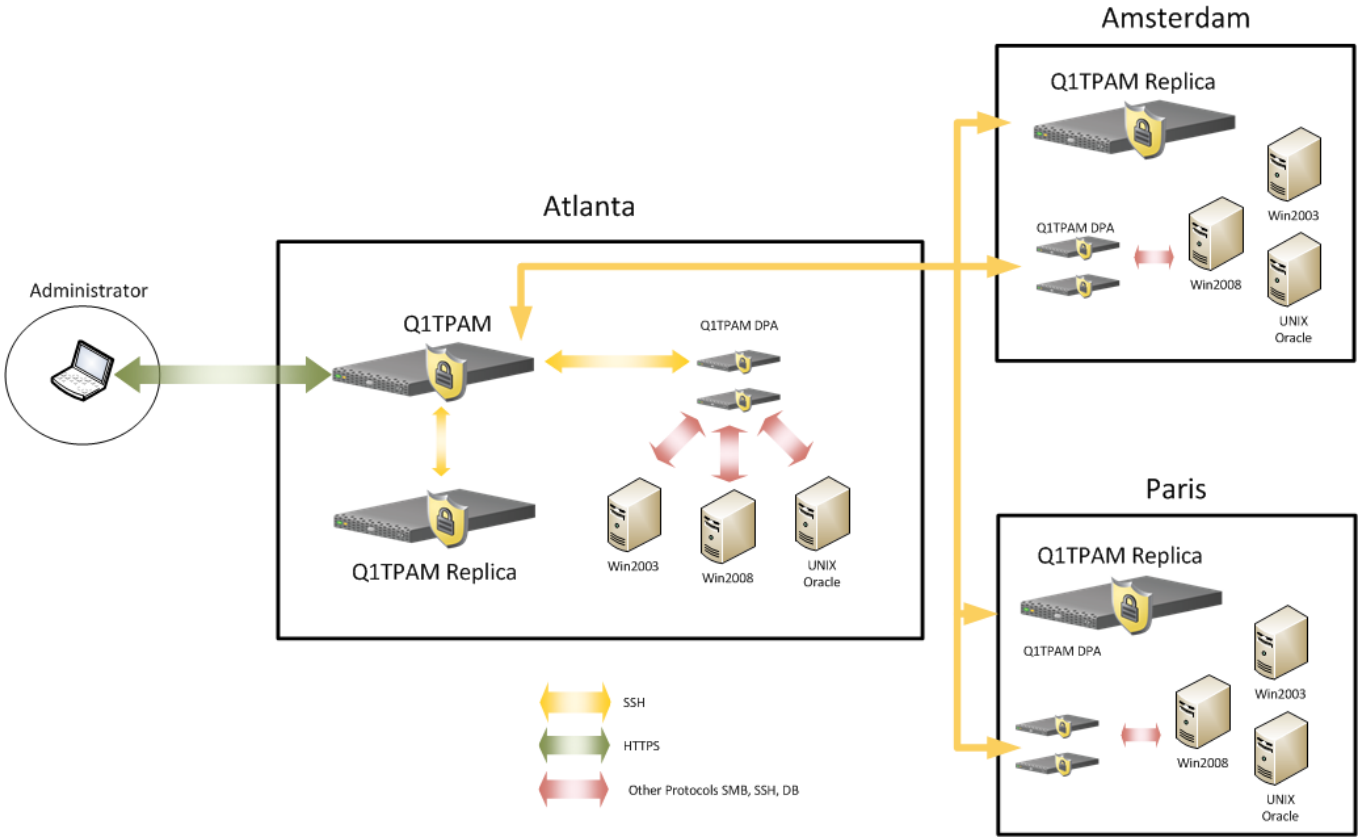
Distributed Processing Appliance (DPA)

- Datacenter PSM Scaling
- Concurrent Session limit + 150
- Store session recordings
- Required for
  - Command restriction
  - Meta-Data Capture

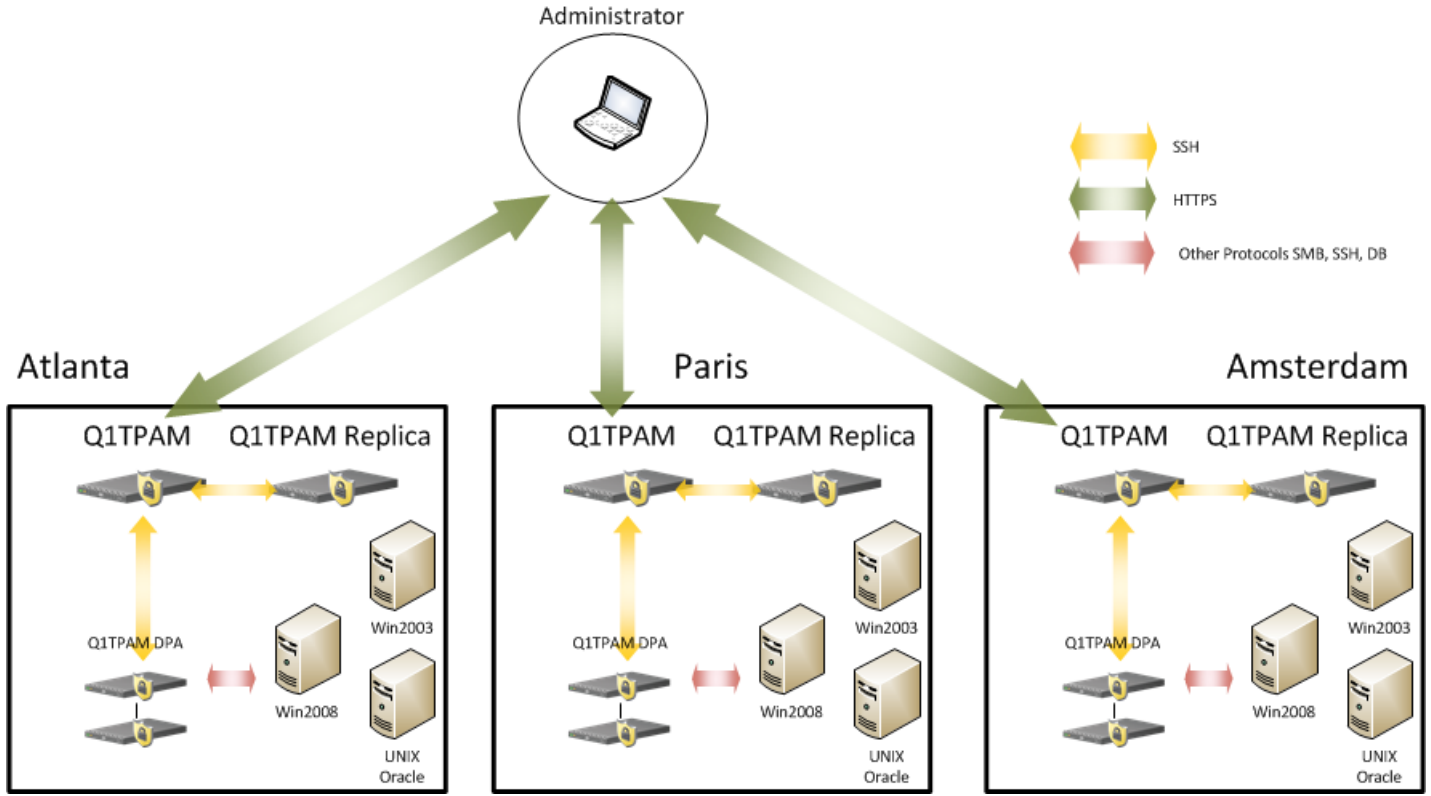
ParCache

- Datacenter PPM Scaling
- Up to 5,000 password requests per second, per appliance

Architecture Example : Distributed Management



Architecture Example : Decentralized Management



Frågor?



Tack för mig

Ingvar Johansson

Dell Software, Sweden