

# Control access to your super user accounts

Dell Solutions Tour 2015

Ingvar Johansson, Dell Software

[ingvar.johansson@software.dell.com](mailto:ingvar.johansson@software.dell.com)



# What is Privileged Management?

# Privilege 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



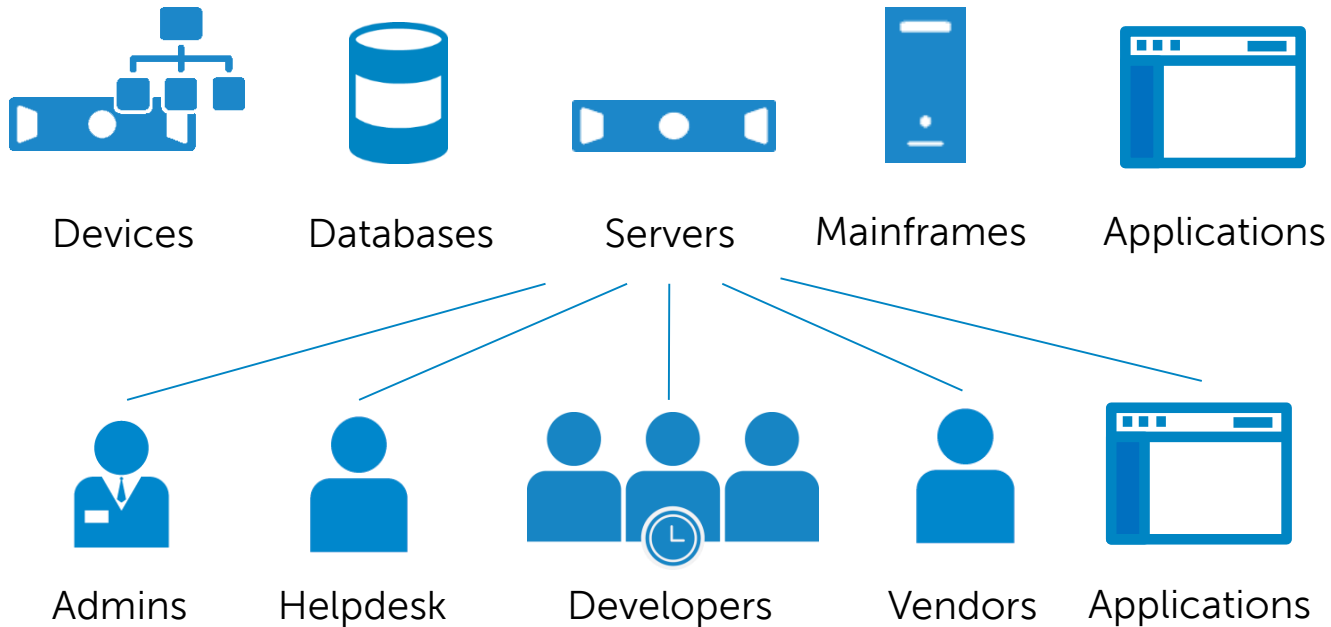
- Huge security and compliance risk



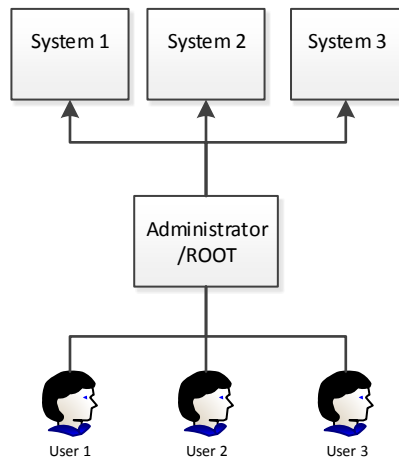
**Fact:** 69% of confirmed security incidents were perpetrated by insiders, and increased more than 300% between 2011 and 2012

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

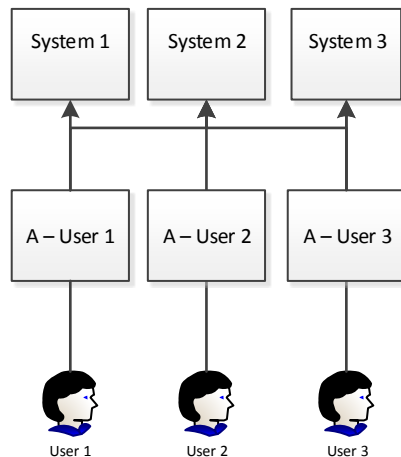
# Why are they difficult to manage?



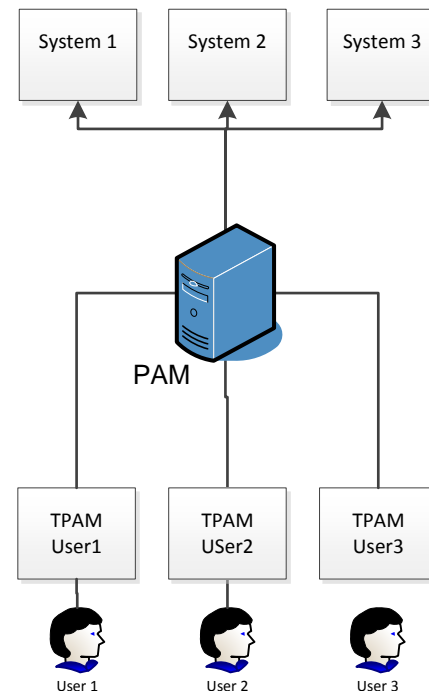
# Different Approaches



Shared  
accounts



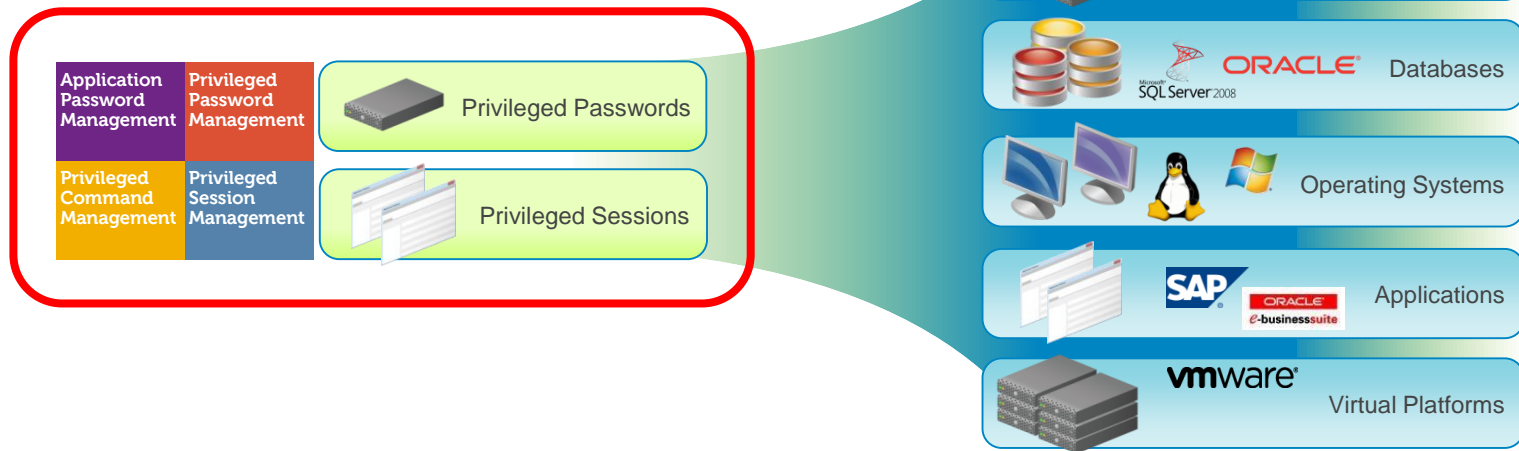
Individual  
privileged  
accounts



Managed  
Access

# Managing Privileged Accounts

- Privileged accounts exist everywhere
- Auditing privileged user sessions

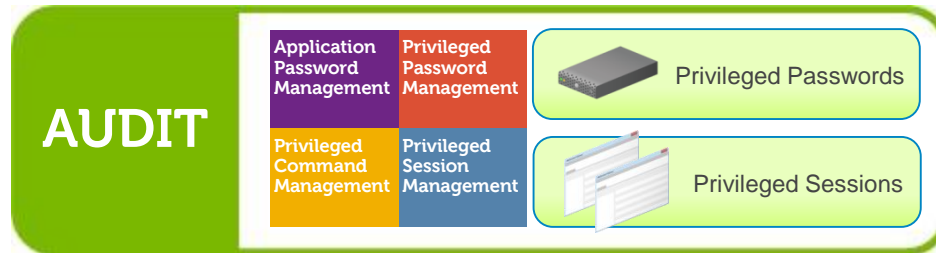


# Total Privileged Access Management (TPAM) Suite

- 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



[Add Password Request](#)

[Add File Request](#)

[Add Session Request](#)

## The Privileged Appliance

TPAM provides a secure audited method into your network (via various protocols like Telnet, SSH, Services), SSH, Telnet, and x5250 (AS400).

**Password Request Management**  
Select accounts then click Details tab.

Filter | Listing | Accounts | Details | Responses | Approvals | Password

Selected	System Name	Account Name	Access Policy	Min Appr	Max Duration	Details
<input type="checkbox"/>	ADSRV	privAccount1	Requestor	1	7d:00h:00m	Approval Required
<input type="checkbox"/>	ADSRV	privAccount2	Requestor	1	7d:00h:00m	Approval Required
<input checked="" type="checkbox"/>	Linux1	superuser	Requestor	1	7d:00h:00m	Approval Required

**Password Request Management**  
Specify details and save changes.

Filter | Listing | Accounts | Details | Responses | Approvals | Password

☒ Request Immediate Date/Time Required: (MM/DD/YYYY AM/PM) 9 / 22 / 2015 09 : 00 AM

Requested Duration: 0 Days 2 Hours 0 Minutes

Reason Code: Select a Reason Code

Request Reason: \* I need to change DNS settings

Remaining: 970

Select Accounts

Sel.	System Name Account Name	Status	Access Policy Max Duration	Locked? Last Released
<input checked="" type="checkbox"/>	Linux1 superuser	Approval Required	Requestor 7d:0h:0m	No 9/14/2015 2:05 PM



# Approval: Request a password...

Session Mgmt | Approve/Review | Reports

## Password Requests for Approval

RequestID: 1-29 Account: **superuser** System: **Linux1**

Filter Listing Details Responses Approvers Conflicts

Req. ID	PSM	UserName	User Full Name	System Name	Account Name	Access Policy	Request Release Date	Status
1-29		CAMILLAK	Karlsson, Camilla	Linux1	superuser	Requestor	9/21/2015 1:07:17 PM	Pending Approval

Session Mgmt | Approve/Review | Reports

## Password Requests for Approval

RequestID: 1-29 Account: **superuser** System: **Linux1**

Filter Listing Details Responses Approvers Conflicts

**Dates**  
Requested: 9/21/2015 1:07:17 PM  
Duration: 0 D 2 H 0 M  
Submitted: 9/21/2015 1:07:17 PM  
Approved:  
Expires: 9/21/2015 3:07:17 PM  
Close:  
Canceled:

**Other Info**  
Policy: Requestor  
Appr Req: 1  
Ticket Sys:  
Ticket #:

**Requestor Info**  
Name: CAMILLAK (Karlsson, Camilla)  
Phone: +468999 99 99  
Email: camillak@dsgdemo.com  
Groups: TPAM\_Requestors

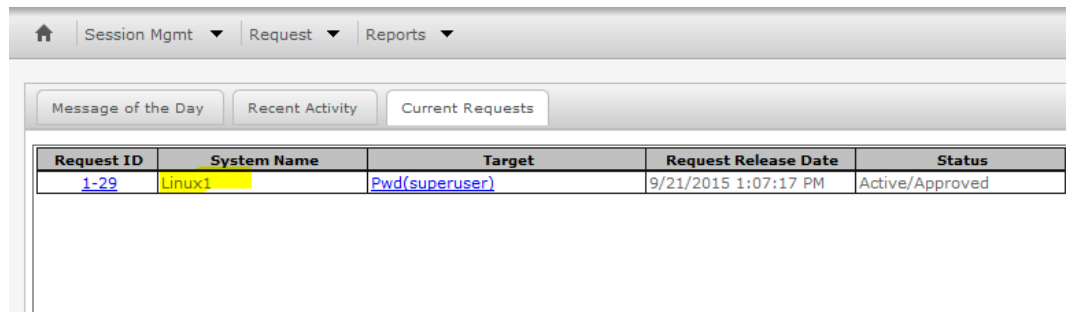
Request Reason: I need to change DNS settings

Request Response: \* That is ok.

Remaining: 244

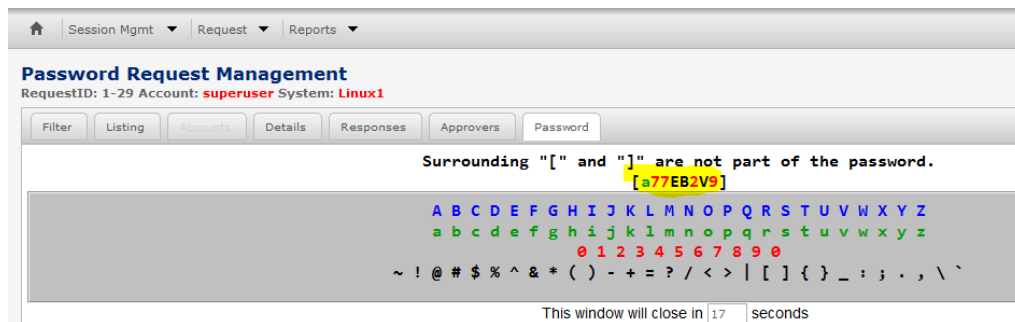


# Release: Request a password...



The screenshot shows the top navigation bar with 'Session Mgmt', 'Request', and 'Reports' menus. Below it are three tabs: 'Message of the Day', 'Recent Activity', and 'Current Requests'. The 'Current Requests' tab is active, displaying a table with the following data:

Request ID	System Name	Target	Request Release Date	Status
<a href="#">1-29</a>	Linux1	<a href="#">Pwd(superuser)</a>	9/21/2015 1:07:17 PM	Active/Approved



The screenshot shows the 'Password Request Management' interface for RequestID: 1-29, Account: superuser, and System: Linux1. The 'Password' tab is active, displaying a password generation screen. The screen shows a message: 'Surrounding "[" and "]" are not part of the password.' followed by a highlighted password: '[a77EB2V9]'. Below this is a grid of characters for selection, including uppercase and lowercase letters, numbers, and special characters. At the bottom, a timer indicates 'This window will close in 17 seconds'.



# 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

[Home](#) | [Session Mgmt](#) | [Request](#) | [Reports](#)

Message of the Day

[Add Password Request](#)

[Add File Request](#)

[Add Session Request](#)

The Privil

TPAM provides a se

the session is reco

Services), SSH, Te

[Home](#) | [Session Mgmt](#) | [Request](#) | [Reports](#)

## Session Request Management

RequestID: 1-30 Account: **privAccount1** System: **ADSRV**

[Filter](#) | [Listing](#) | [Accounts](#) | [Details](#) | [Responses](#) | [Approvers](#) | [Connect Options](#)

**Request Info**

Status:

Appr Req:

Ticket Sys:

Ticket #:

**Dates**

Requested:

Duration:  D  H  M

Submitted:

Approved:

Expires:

Close:

Canceled:

**Policy Info**

Policy:

Cmd Name:

Request Reason:

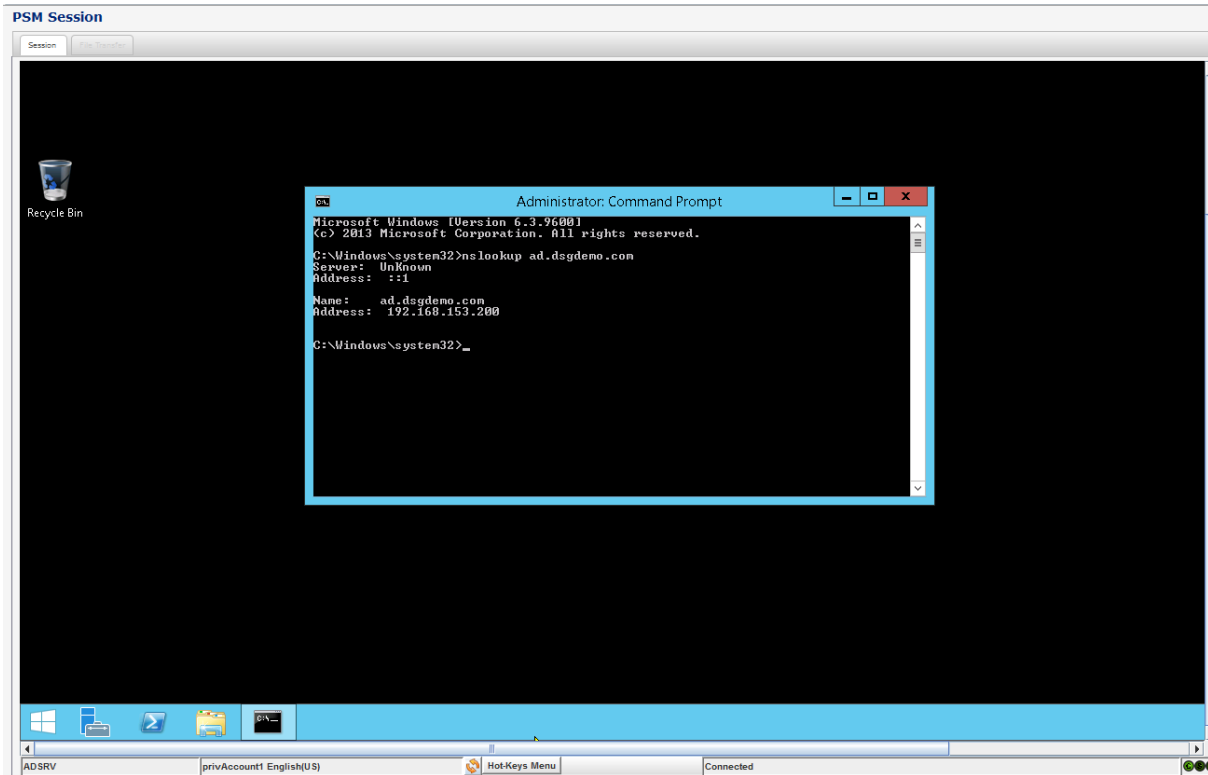
Cancel/Expire Reason:\*

Characters remaining: 255

[Save Changes](#) | [New Request](#) | [Export to Excel](#) | [Export to CSV](#) | [New Accounts](#) | [Connect](#) |  | [Terminate](#) | [Cancel](#)



# 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





# Command Control

- 
- The diagram consists of four colored squares arranged in a 2x2 grid. The top-left square is purple and contains the text 'Application Password Management'. The top-right square is red and contains the text 'Privileged Password Management'. The bottom-left square is yellow and contains the text 'Privileged Command Management'. The bottom-right square is blue and contains the text 'Privileged Session Management'.
- |                                 |                                |
|---------------------------------|--------------------------------|
| 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)



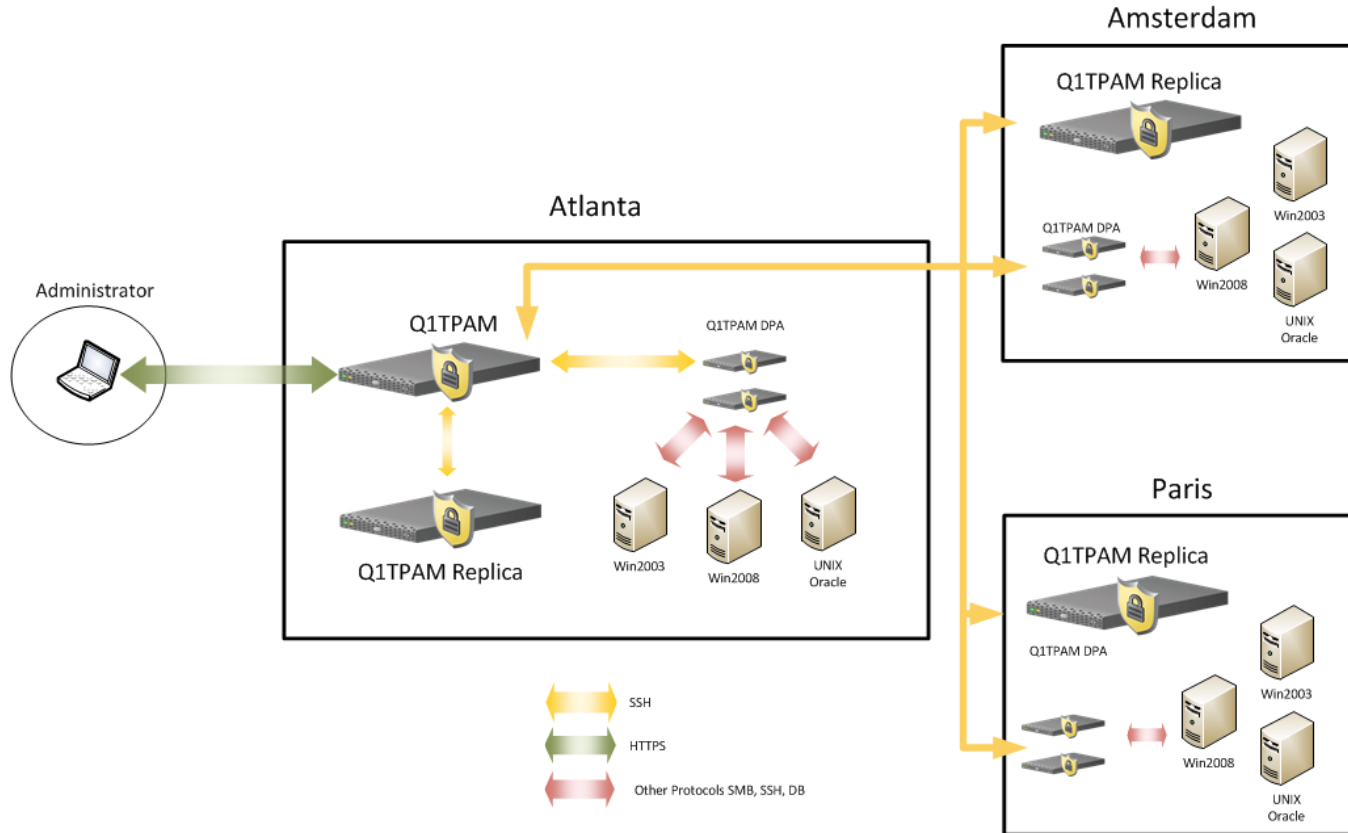
- Datacenter PSM Scaling
- Concurrent Session limit + 150
- Store session recordings
- Required for
  - Command restriction
  - Meta-Data Capture

ParCache

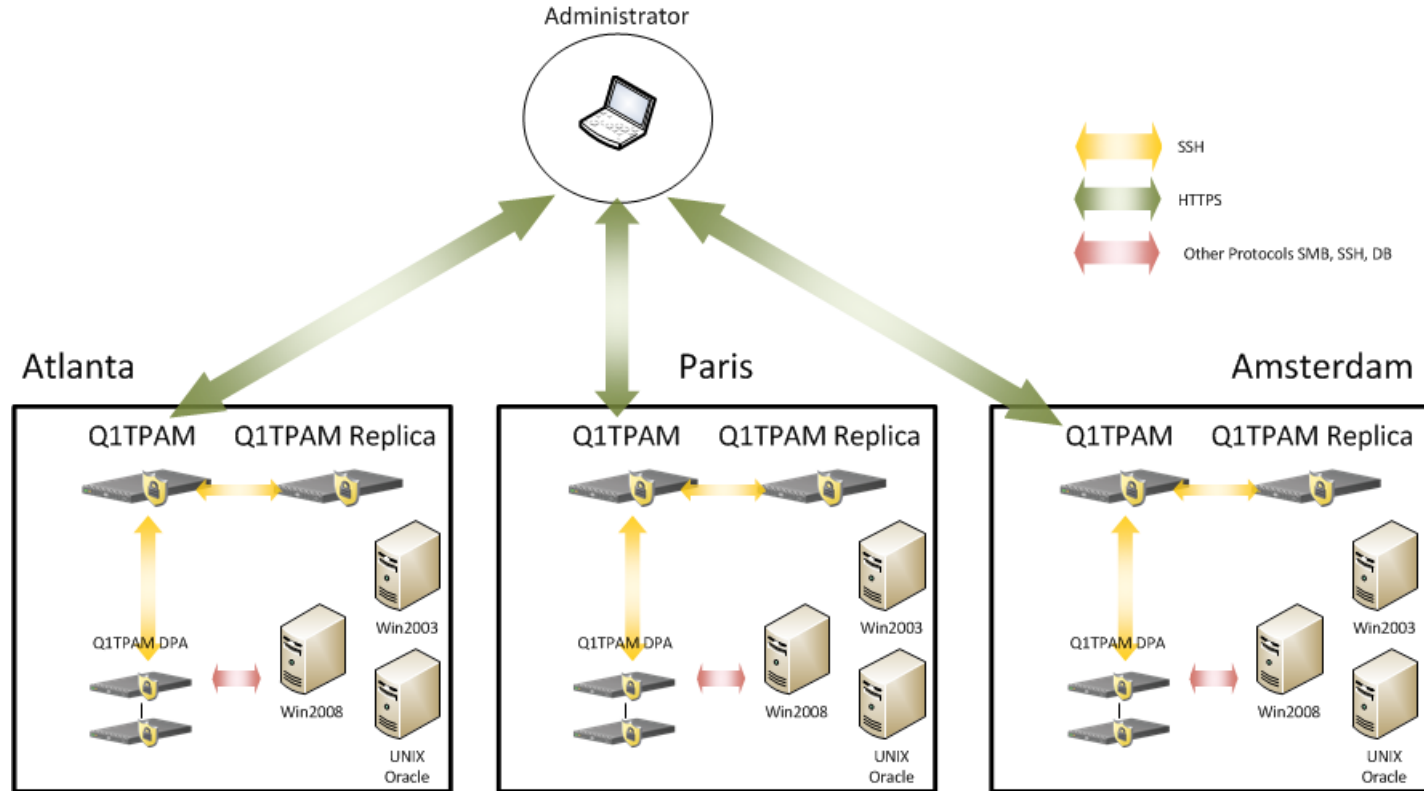


- Datacenter PPM Scaling
- Up to 5,000 password requests per second, per appliance

# Architecture Example : Distributed Management



# Architecture Example : Decentralized Management



# Frågor?



# Tack för mig

Ingvar Johansson

Dell Software, Sweden

