



# Centralizing Data Center Security to Simplify Compliance

Centrify Corporation

[www.centrify.com](http://www.centrify.com)

(408) 542-7500

# Multiple Regulatory Issues to Address

Most organizations are subject to multiple regulations aimed at defining security best practices. But common requirements emerge:



Sarbanes-Oxley Act  
Section 404



Federal Information  
Security Management  
Act



Health Insurance  
Portability and  
Accountability Act



Basel II. FFIEC  
Information Security  
Booklet



National Industrial  
Security Program  
Operating Manual



Payment Card  
Industry Data  
Security Standard

- Enforce system security policies
- Enforce network access policies
- Encrypt data-in-motion
- Lock down privileged accounts
- Enforce "least access"
- Enforce separation of duties
- Associate privileges with individuals
- Audit privileged user activities

# Significant IT Threats Increase Business Risk

- Several high profile attacks and abuses in the News recently...
  - “Fannie Mae Logic Bomb Would Have Caused Weeklong Shutdown” – Jan 2009, wired.com
  - “Financial firm notifies 1.2M after password mistake” – Jan 2010, networkworld.com
  - “Google Hackers Targeted Source Code of More Than 30 Companies” – Jan 2010, wired.com
- Recent Data Breach statistics – verizon.com
  - 91% compromised records linked to organized crime
  - 64% resulted from hacking
  - 22% involved privilege misuse
  - 32% implicated business partners
  - 81% were not PCI-DSS compliant
- A Centrify survey confirms need for improved UNIX security
  - 40% share root passwords
  - 44% cannot immediately terminate access
  - 69% have orphaned accounts



## NETWORKWORLD

News | Blogs & Columns | Subscriptions | Videos | Events |

Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software | Data Center |

TECH DISPENSER

### Financial firm notifies 1.2M after password mistake

Lincoln National's shared passwords, dating back to 2002, could have been misused

By [Robert McMillan](#), IDG News Service  
January 15, 2010 02:01 PM ET

WIRED

SUBSCRIBE >>

SECTIONS >>

BLOGS >>

REVIEWS >>

VIDEO >>

HOW-TO

Sign In | RSS Feeds

## THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

### Google Hackers Targeted Source Code of More Than 30 Companies

By [Kim Zetter](#) | January 13, 2010 | 2:28 am | Categories: [Cybersecurity](#), [Hacks and Cracks](#)

A hack attack that targeted Google in December also hit 33 other companies, including financial institutions and defense contractors, and was aimed at stealing source code from the companies, say security researchers at iDefense.

SLIDE 3

# The Centrify Security Methodology

Leverage Active Directory as centralized security infrastructure

## Protect Systems and Data

- Enforce system security policies
- Enforce network protection policies
- Lock down privileged accounts

## Authorize User Access & Privileges

- Enforce unique identity and least access
- Associate privileges with individuals
- Enforce separation of duties

## Audit & Report on Rights & Activities

- Audit all user activity
- Report on access rights and privileges



*Establishing Security Automation for the Enterprise*

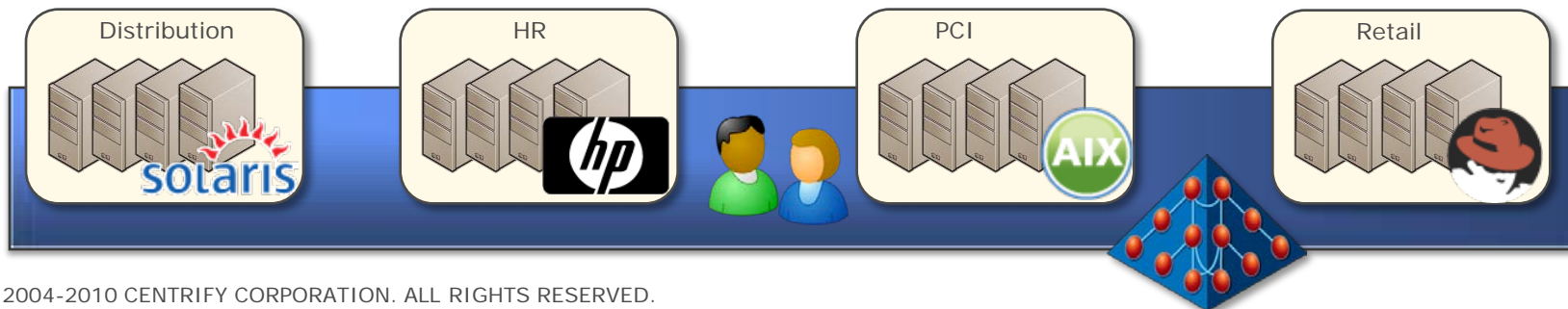
# Centralized Security Starts with Active Directory

Active Directory services provide the foundation for Enterprise security

- Highly distributed, fault tolerant directory infrastructure designed for scalability
- Supports large Enterprises through multi-Forest, multi-Domain configurations
- Kerberos-based authentication and authorization infrastructure providing SSO

Account Administration is centralized in one system

- Simplifying authentication and password management
- Leveraging existing onboard, management and offboard processes



---

# STEP 1 – PROTECT SENSITIVE SYSTEMS AND DATA

## Step 1 – Protect Sensitive Systems and Data

---

- Centrify Suite security methodology:
  - a) Establish centralized security management infrastructure
  - b) Enforce system security policies
  - c) Enforce network access policies
  - d) Encrypt data-in-motion
  - e) Lock down privileged accounts
  
- Addressing PCI-DSS requirements:
  - Requirement 1 – Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2 – Do not use vendor-supplied defaults for system passwords and other security parameters
  - Requirement 4 – Encrypt transmission of cardholder data across open, public networks

# 1a – Establish Centralized Security Management

- Join Active Directory for Identity and Access Management

- Group into Zones by administrative role

- Active Directory services:

- Enforces security policy
- Locks service accounts
- Controls authentication
- Provides Accountability

- Resulting in a secured server environment



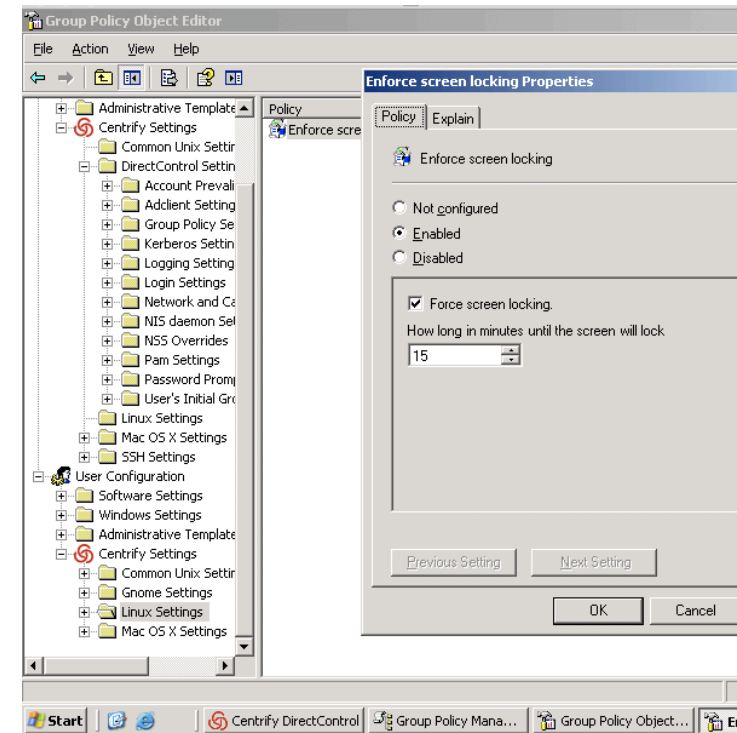
# 1b – Enforce System Security Policies

Consistent security and configuration policies need to be enforced on all Windows, UNIX, Linux and Mac systems

- Group Policy automatically enforces security policy at system join to Active Directory
- Group Policy routinely checks the system for compliance, updating as required
- Group Policy also enforces user policies at login

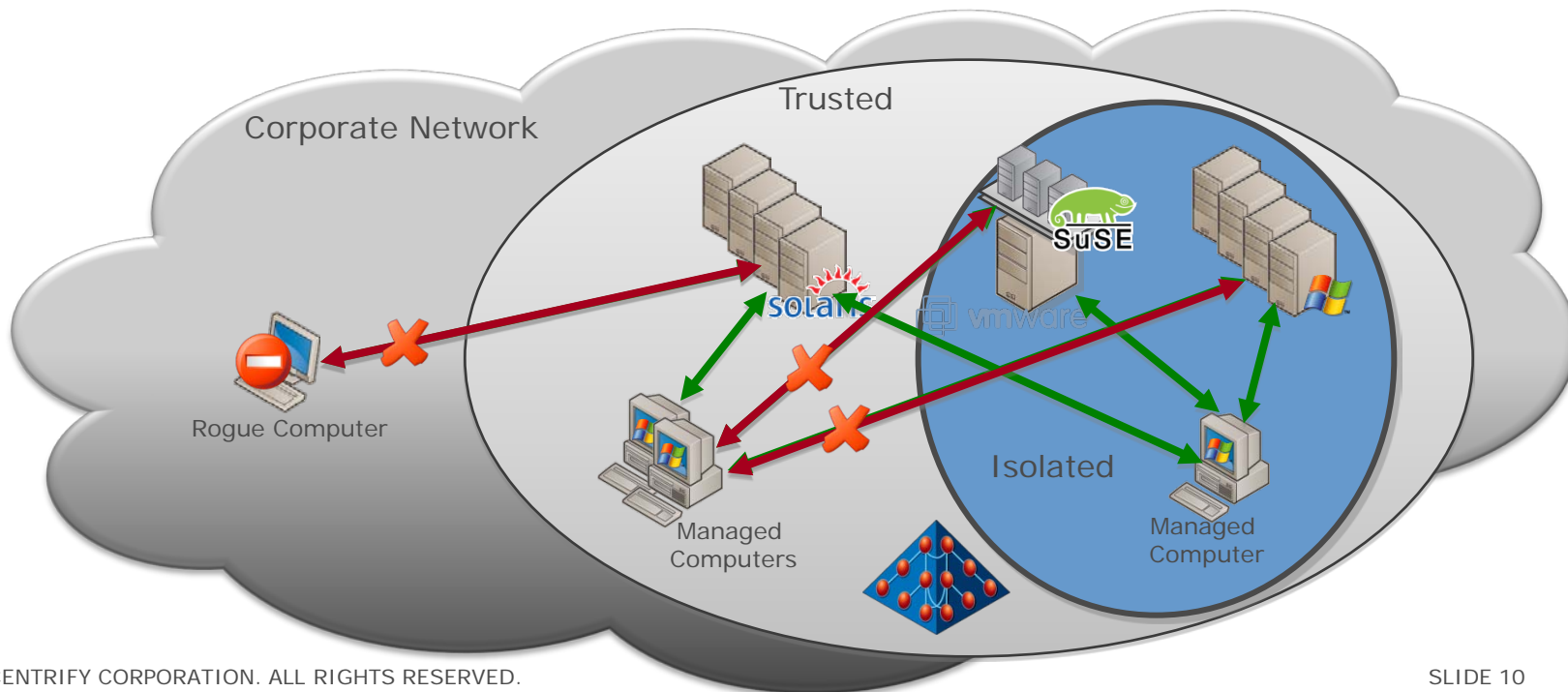
Group Policies enforce:

- System authentication configuration
- System banner settings
- Screen saver & unlock policies
- SSH policies controlling remote system access
- Firewall policies controlling machine access
- User policies controlling the user's environment



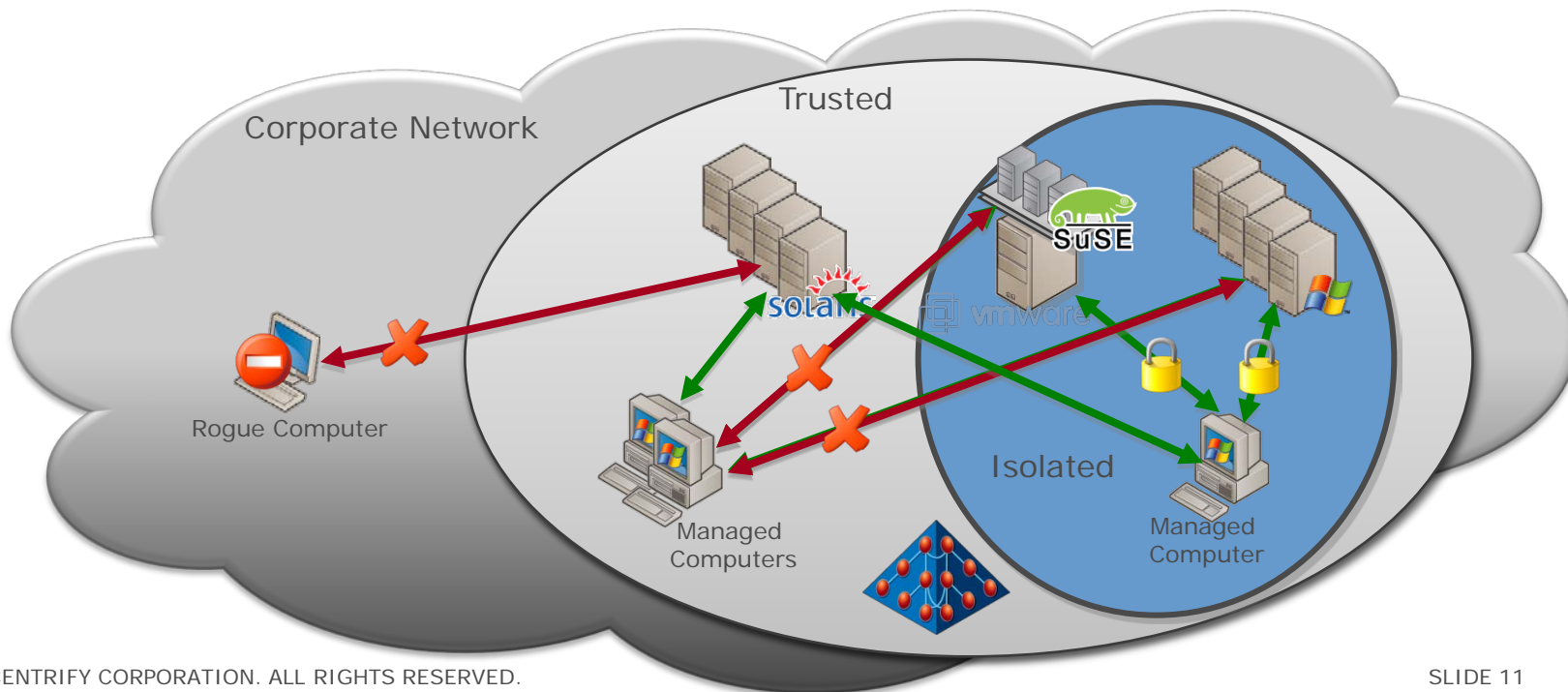
# 1c – Enforce Network Access Policies

- Prevent unauthorized access to sensitive systems
  - Enforcing IPsec authentication policy establishes the un-spoofable host-based firewall
  - Peer-to-peer authentication uses strong host credentials to prevent communications with untrusted systems
- Logically Isolate Sensitive Servers on the existing Network Infrastructure
  - Control access to systems through Active Directory group-based host authorizations



# 1d – Encrypt Data-in-Motion

- Encrypt Data-in-Motion without modifying older applications
  - Enforce port level, network layer encryption for legacy applications transporting data in the clear (e.g. ftp, telnet, sql)



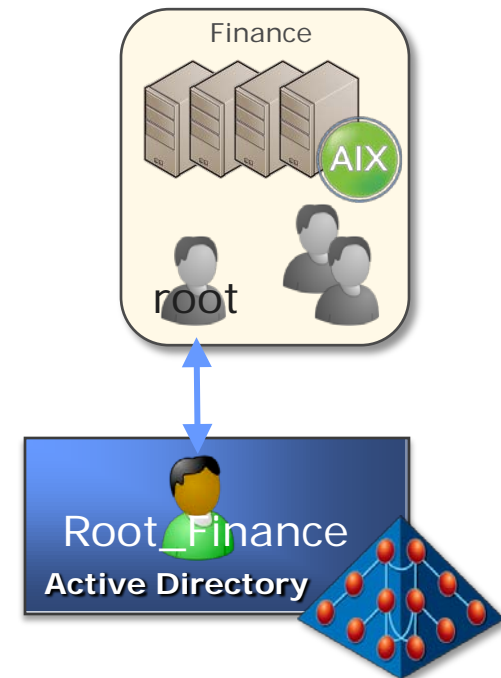
# 1e – Lock Down Privileged Accounts

Lockdown privileged and service accounts within Active Directory

- Online authentication requires AD-based password validation
- Offline authentication uses the local cached account
- Passwords are synchronized to local storage for single user mode login

Leverage role-based privilege grants to eliminate risks exposed by these accounts

- Eliminating need to access privileged accounts
- Enables locking down these account passwords



---

# **STEP 2 – CONTROL ACCESS & AUTHORIZE PRIVILEGES**

## Step 2 – Control Access & Authorize Privileges

- Centrify Suite security methodology:
  - Require user login with individual AD accounts
  - Enforce least access
  - Enforce separation of duties
  - Associate privileges with individuals
- Addressing PCI-DSS requirements:
  - Requirement 7 – Restrict access to cardholder data by business need-to-know
    - 7.1 Restrict access to cardholder data to individuals with a “need to know”
    - 7.2 Restrict access mechanism should deny all and grant access only where needed
  - Requirement 8 – Assign a unique ID to each person with computer access
    - 8.1 Identify all users with a unique username
    - 8.4 Encrypt all passwords during transmission and storage
    - 8.5 Ensure proper user authentication and password management

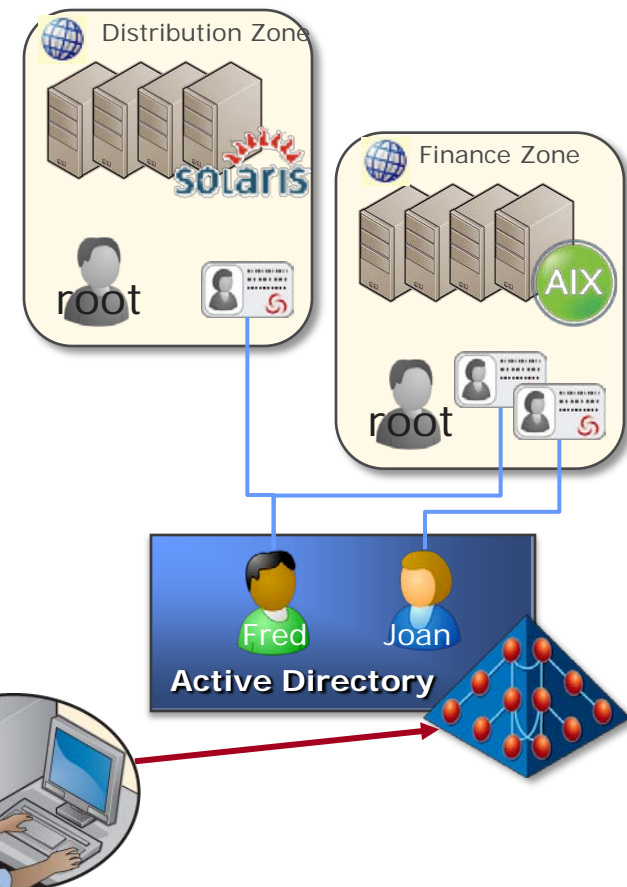
## 2a – Require User Login With Individual Accounts

Centrify empowers enterprise admins to centrally manage user accounts using existing expertise, tools and processes

- ADUC for user account, password and group management

UNIX/Linux profiles are centrally managed

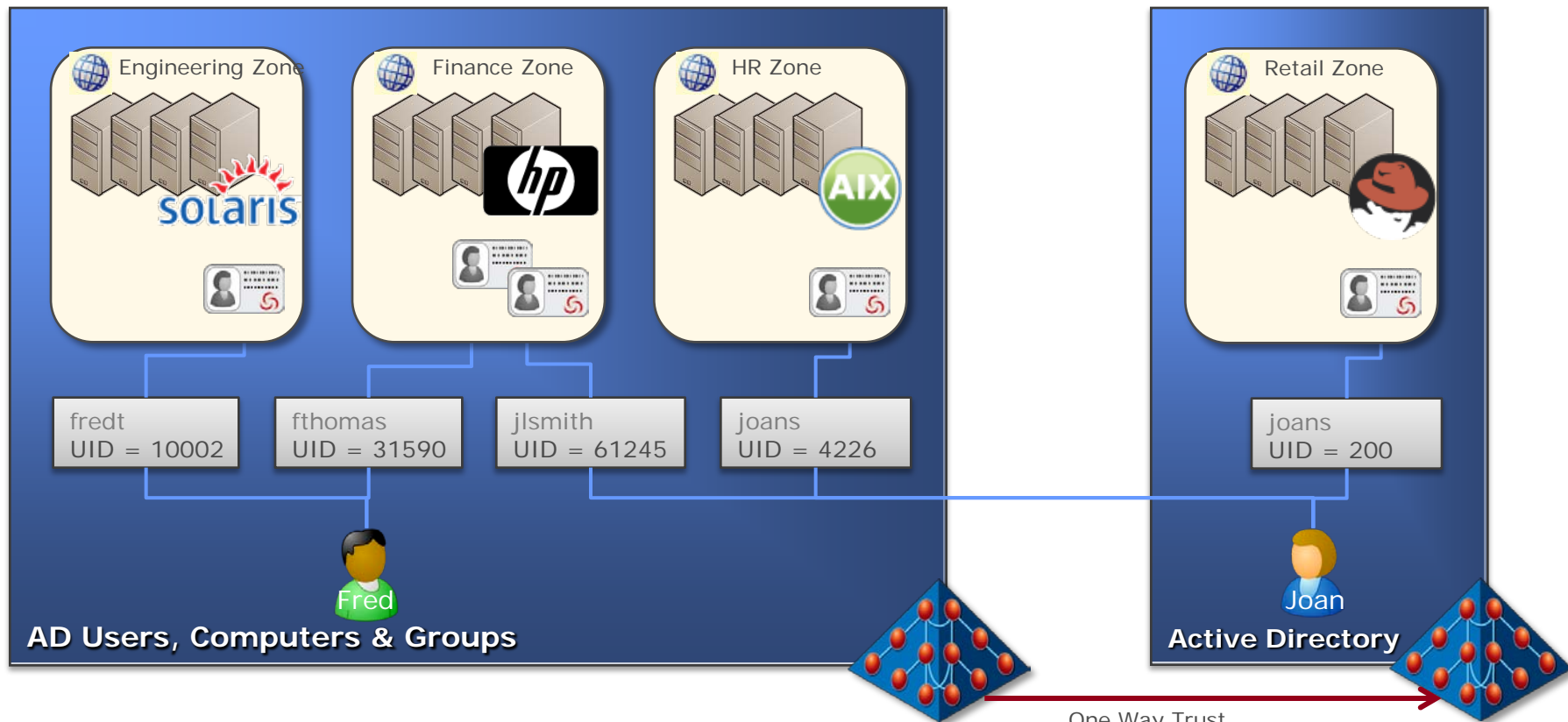
- AD account is used for authentication
  - AD password is stored in AD only
  - Multiple UNIX profiles can be associated with a single AD user account
- 
- Accountability is established for all UNIX activities by AD users



AD & Windows  
Administration

## 2b – Enforce Least Access

- System access is denied unless explicitly granted
- Access is granted to a Zone (group of systems sharing a namespace)
- Group membership can also be required to further limit access



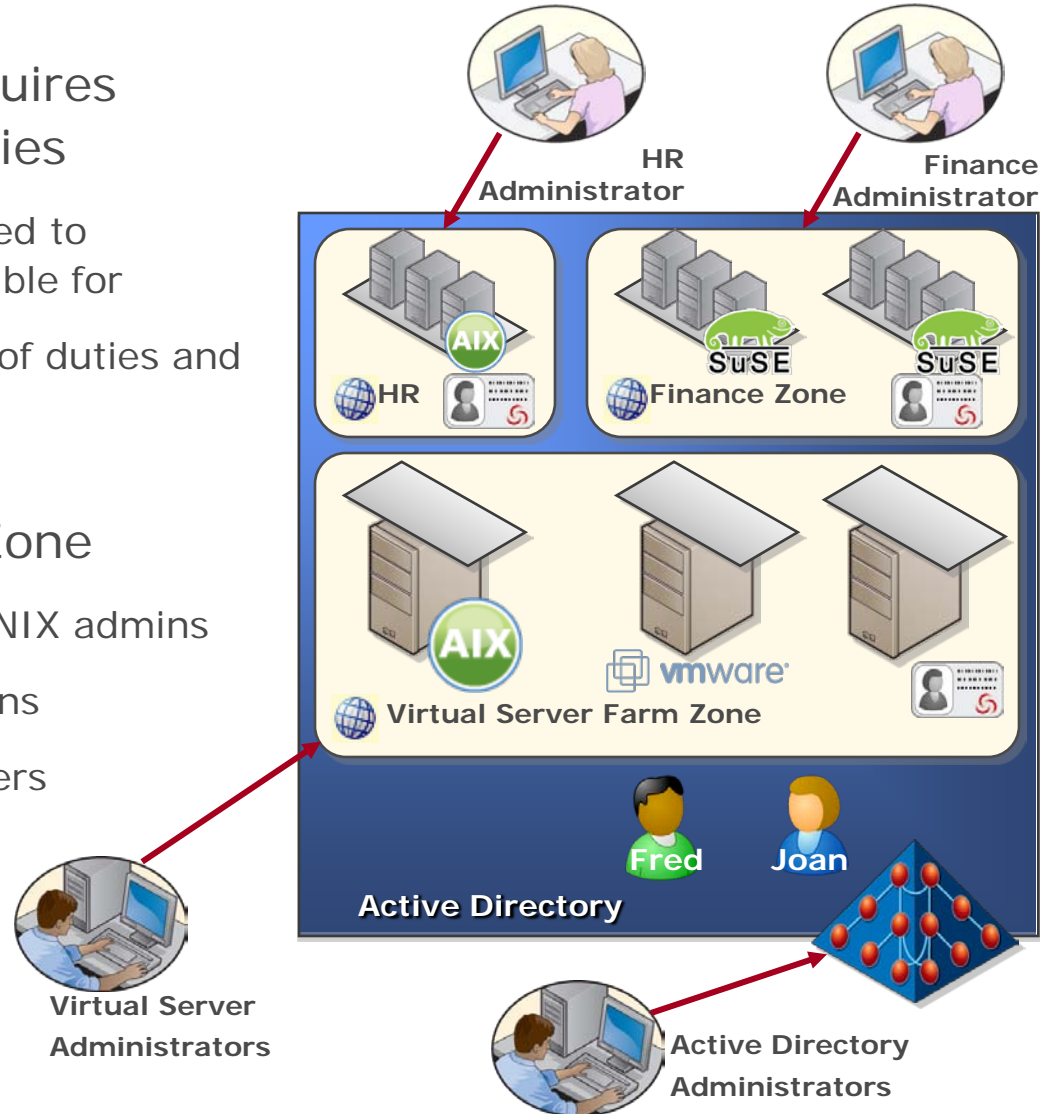
## 2c – Enforce Separation of Administrative Duties

Centralization in a Directory requires separation of administrative duties

- Administrators must only be granted to manage systems they are responsible for
- Centrify Zones provide separation of duties and access control where needed

Separation of admin duties by Zone

- Separation of Active Directory & UNIX admins
- Zones are delegated to UNIX admins
- UNIX admins don't manage AD Users



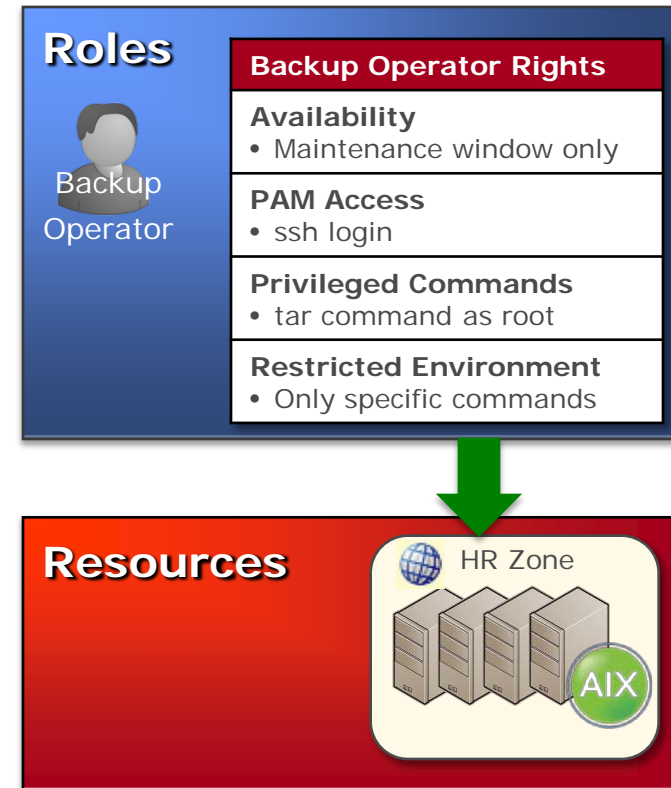
## 2d – Associate Privileges with Named Individuals

Centralized role-based policy management

- Create Roles based on job duties
- Grant specific access and elevated privilege rights
- Eliminate users' need to use privileged accounts
- Secure the system by granularly controlling how the user accesses the system and what he can do

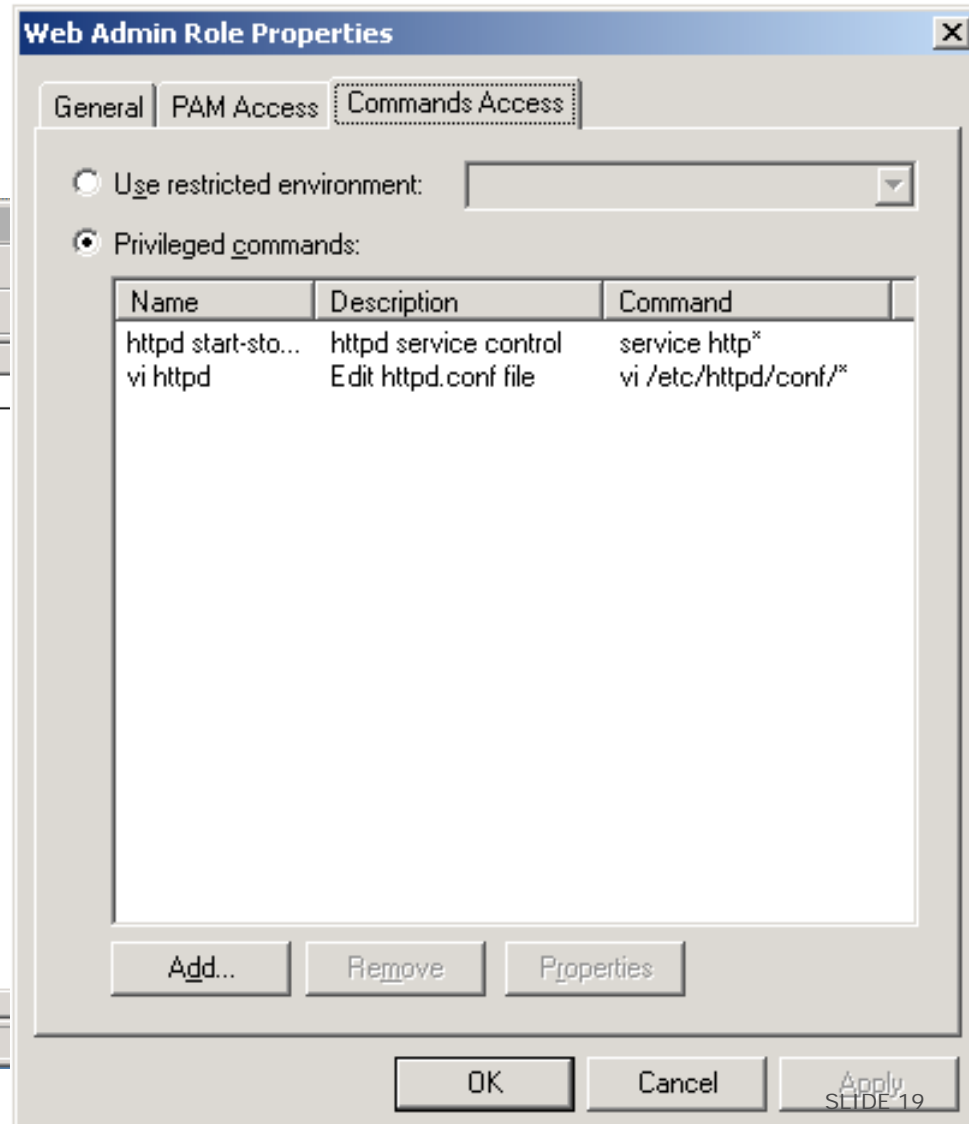
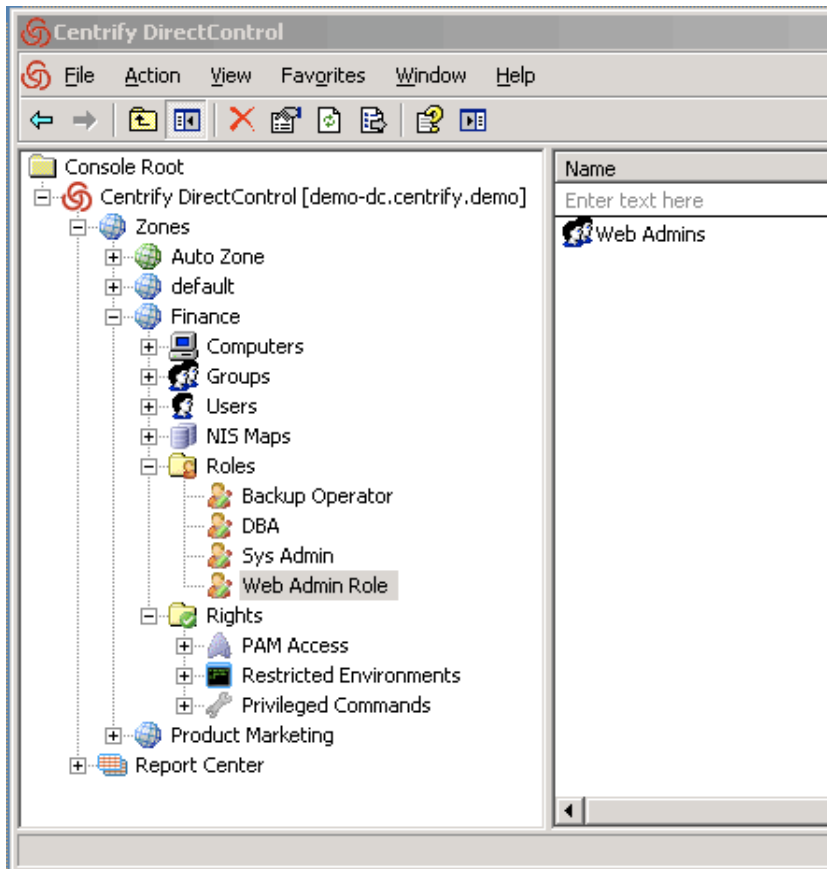
Unix rights granted to Roles

- Availability – controls *when* a Role can be used
- PAM Access – controls *how* user's access UNIX system interfaces and applications
- Privilege Commands – grants elevated privileges where needed
- Restricted Shell - controls allowed commands in the user's environment



## 2d – Grant Privileged Commands to Roles

- Web Admins need root privileges to manage Apache Services



# 2d – Role Assignments Ensure Accountability

## Role Assignment

- Active Directory Users are assigned to a Role, eliminating ambiguity, ensuring accountability
- Active Directory Groups can be assigned to a Role, simplifying management
- User assignment can be date/time limited – enabling temporary rights grants

## Assignment Scope

- Roles apply to all computers within a Zone
- Assignment can be defined for a specific Computer



## Example: Privilege Access in Current Environment

- Web Admin editing the httpd.conf requires root permissions

### User Session

```
[twilson@test-rhel5 ~]$ su root
Password:
[root@test-rhel5 twilson]# vi /etc/httpd/conf/httpd.conf
[root@test-rhel5 twilson]# /sbin/service httpd restart
Stopping httpd:                [ OK ]
Starting httpd:                 [ OK ]
[root@test-rhel5 twilson]#
```

### Security Log (/var/log/secure)

```
Oct 26 10:13:27 test-rhel5 sshd[1786]: pam_unix(sshd:session): session opened for user twilson by (uid=0)
Oct 26 10:14:45 test-rhel5 su: pam_unix(su:session): session opened for user root by (uid=10004)
```

# Example: Rights Dynamically Granted at Login

```
[twilson@test-rhel5 ~]$ id
uid=10004(twilson) gid=10001(unixuser) groups=10001(unixuser)
[twilson@test-rhel5 ~]$ adquery group -a "Web Admins"
centrify.demo/Users/Tim Wilson
centrify.demo/Users/David McNeely
[twilson@test-rhel5 ~]$
[twilson@test-rhel5 ~]$ dzinfo
Zone Status: DirectAuthorize is enabled
User: twilson
Forced into restricted environment: No

Role Name      Avail Restricted Env
-----
Web Admin Role Yes   None

PAM Application Avail Source Roles
-----
ftpd           Yes   Web Admin Role
sshd           Yes   Web Admin Role

Privileged commands:
Name           Avail Command      Source Roles
-----
vi httpd      Yes   vi /etc/httpd/conf/* Web Admin Role
httpd         Yes   service http*      Web Admin Role
start-stop-rest
art

[twilson@test-rhel5 ~]$
```

## Example: Privileged Access with Centrify Suite

- Web Admin editing the httpd.conf using DirectAuthorize privilege elevation

### User Session

```
[twilson@test-rhel5 ~]$ dzdo vi /etc/httpd/conf/httpd.conf
[twilson@test-rhel5 ~]$ dzdo /sbin/service httpd restart
Stopping httpd:                [ OK ]
Starting httpd:                [ OK ]
[twilson@test-rhel5 ~]$
```

### Security Log (/var/log/secure)

```
Oct 26 10:25:42 test-rhel5 sshd[1786]: pam_unix(sshd:session): session opened for user twilson by (uid=0)
Oct 26 10:26:03 test-rhel5 dzdo: twilson : TTY=pts/5 ; PWD=/home/twilson ; USER=root ; COMMAND=/bin/vi /etc/httpd/conf/httpd.conf
Oct 26 10:28:27 test-rhel5 dzdo: twilson : TTY=pts/5 ; PWD=/home/twilson ; USER=root ; COMMAND=/sbin/service httpd restart
```

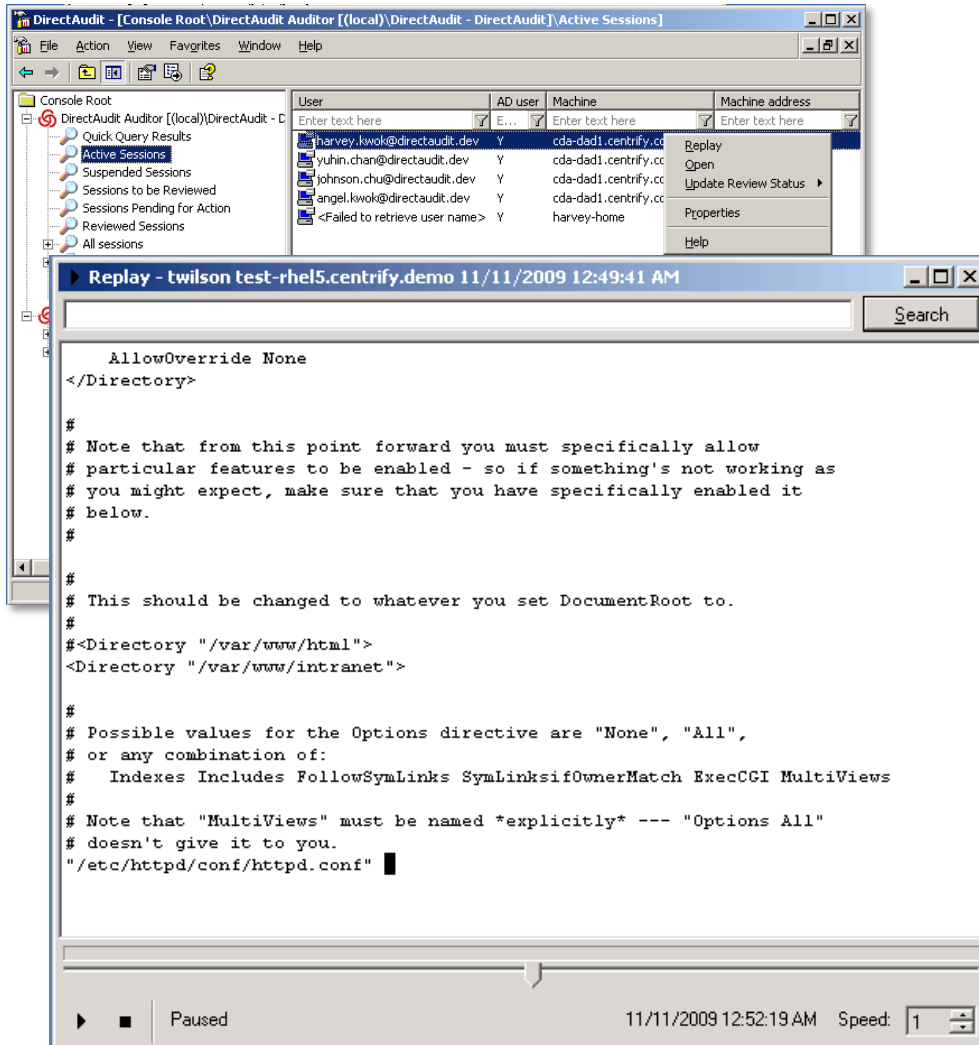
---

# STEP 3 – AUDIT & REPORT ON ACTIVITY & PRIVILEGES

## Step 3 – Audit & Report on Activity & Privileges

- Centrify Suite security methodology:
  - Audit all user activity
  - Report on access grants and privileges
- Addressing PCI-DSS requirements:
  - Requirement 10 – Track and monitor all access to network resources and cardholder data
    - 10.1 Ensure that access to a system can be linked to an individual user
    - 10.2 Auditing should enable reconstructing all user access events and sessions
    - 10.3 Record audit trail entries for all user access
    - 10.4 System clocks should all be synchronized

# 3a – Audit All User Activity



Unix system access is linked to users' unique AD account

Recording user access to systems

- Shows results of commands executed
- Shows changes made to key files

Centrally search captured sessions for interesting events

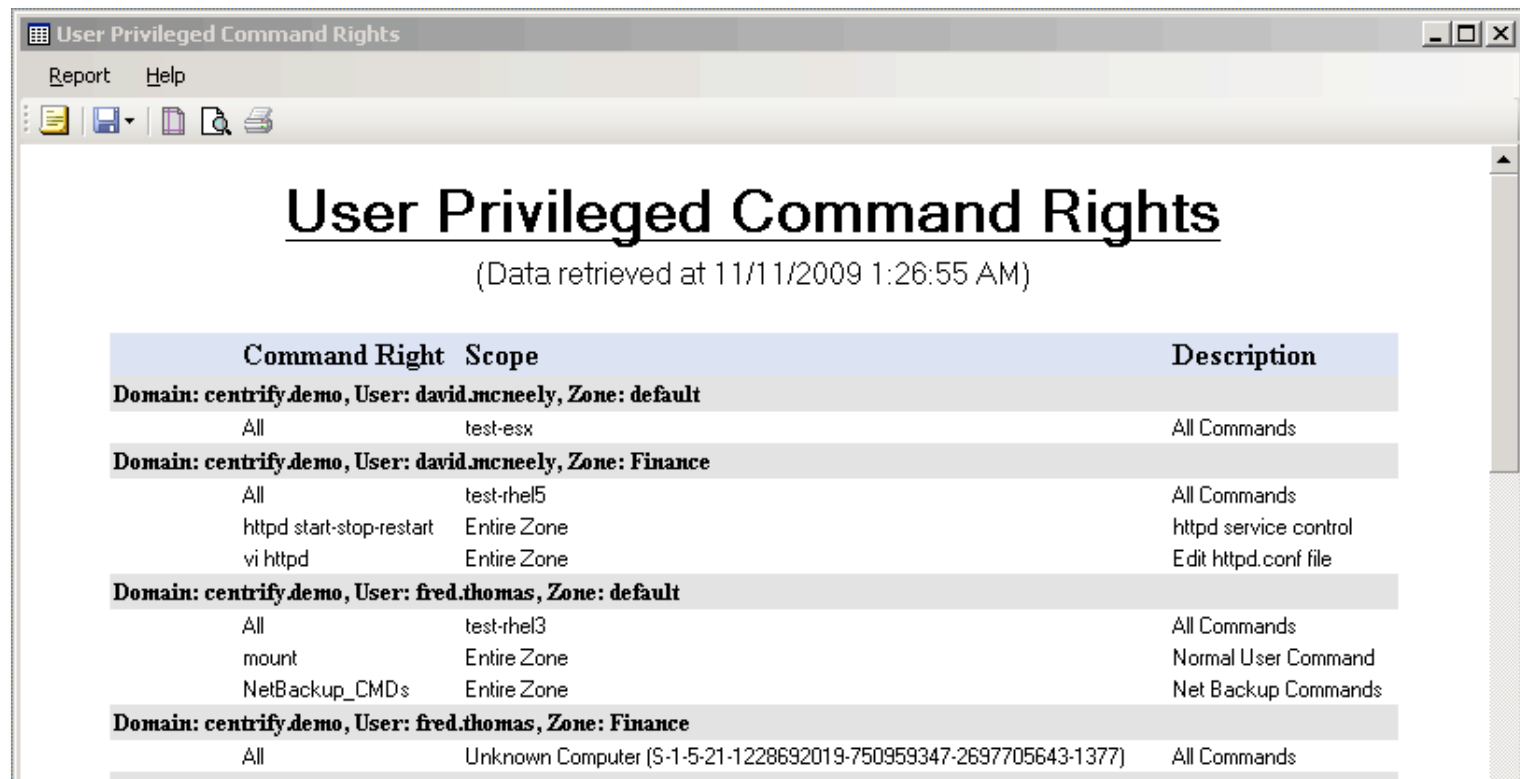
- Search across AD account correlated events within SQL
- Or rollup events to SIEM for analysis, alerting and reporting

Replay full user session activity

## 3b – Report on Privileges

Authorization and Access Rights Reports are centrally created:

- Showing user rights to computers
- Detailing user role assignments and privilege command rights



Command Right	Scope	Description
<b>Domain: centrify.demo, User: david.mcneely, Zone: default</b>		
All	test-esx	All Commands
<b>Domain: centrify.demo, User: david.mcneely, Zone: Finance</b>		
All	test-rhel5	All Commands
httpd start-stop-restart	Entire Zone	httpd service control
vi httpd	Entire Zone	Edit httpd.conf file
<b>Domain: centrify.demo, User: fred.thomas, Zone: default</b>		
All	test-rhel3	All Commands
mount	Entire Zone	Normal User Command
NetBackup_CMDs	Entire Zone	Net Backup Commands
<b>Domain: centrify.demo, User: fred.thomas, Zone: Finance</b>		
All	Unknown Computer (S-1-5-21-1228692019-750959347-2697705643-1377)	All Commands

# Centrify Solutions Enforce Best Practices



Sarbanes-Oxley Act  
Section 404



Federal Information Security Management Act



Health Insurance Portability and Accountability Act



Basel II. FFIEC Information Security Booklet



National Industrial Security Program Operating Manual



Payment Card Industry Data Security Standard

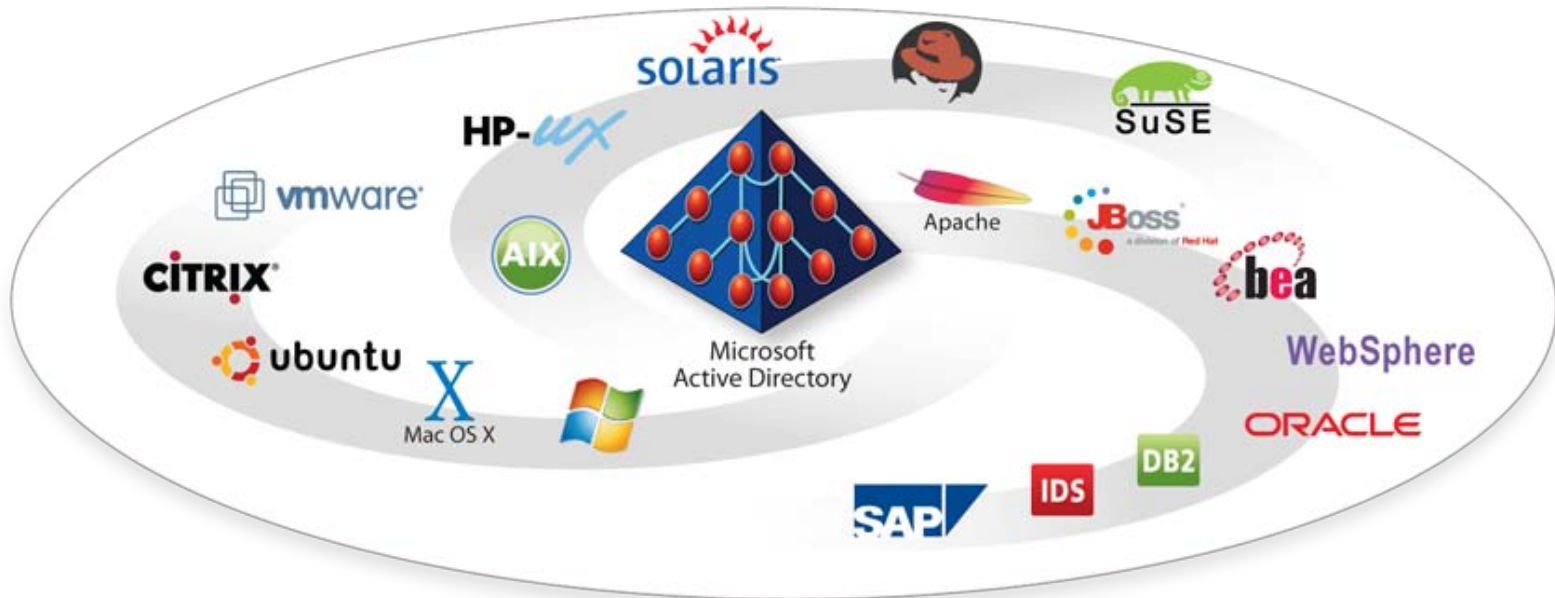
- ✓ Enforce system security policies
- ✓ Enforce network access policies
- ✓ Encrypt data-in-motion
- ✓ Lock down privileged accounts
- ✓ Enforce "least access"
- ✓ Enforce separation of duties
- ✓ Associate privileges with individuals
- ✓ Audit privileged user activities

# The Centrify Suite

Centrify Suite Products	Centrify Suite Editions			
	Standard	Enterprise	Platinum	Application
<b>DirectManage</b> <ul style="list-style-type: none"> <li>▪ <b>Discover</b> and <b>manage</b> user administration on UNIX &amp; Linux</li> <li>▪ <b>Integrate</b> with Active Directory-based tools and processes</li> </ul>	●	●	●	●
<b>DirectControl</b> <ul style="list-style-type: none"> <li>▪ Control <b>who</b> can log into which systems and applications</li> <li>▪ <b>Enforce</b> security policies and <b>consolidate</b> user accounts</li> </ul>	●	●	●	●
<b>DirectAuthorize</b> <ul style="list-style-type: none"> <li>▪ Control <b>how</b> and <b>when</b> users can access UNIX &amp; Linux</li> <li>▪ Specify exactly <b>what</b> commands they can run on those systems</li> </ul>	●	●	●	●
<b>DirectAudit</b> <ul style="list-style-type: none"> <li>▪ <b>Audit</b> in detail what users do on UNIX &amp; Linux systems</li> <li>▪ <b>Report</b> on user sessions and monitor for suspicious activity</li> </ul>		●	●	●
<b>DirectSecure</b> <ul style="list-style-type: none"> <li>▪ Dynamically <b>isolate</b> and <b>protect</b> cross-platform systems</li> <li>▪ Enable optional <b>end-to-end encryption</b> of data in motion</li> </ul>			●	
<b>Application Integration</b> <ul style="list-style-type: none"> <li>▪ Active Directory-based <b>single sign-on</b> for SAP, web applications, and databases</li> </ul>				●

# The Centrify Vision

Centrally Secure Cross-platform Data Centers Using Active Directory



Centrify enables organizations to reduce IT expenses, strengthen security and enhance compliance by centrally securing their cross-platform data centers through Active Directory-based identity and access management.



Q&A