

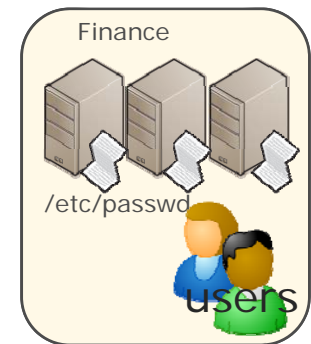
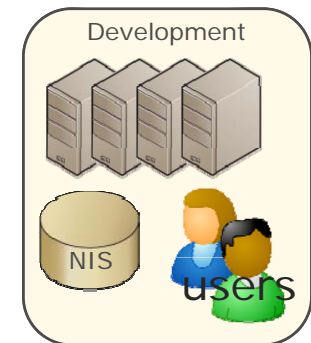


# Executing a Strategy to Manage Identity, Access and Privilege

David McNeely  
Director of Product Management  
Centrify Corporation  
[David.McNeely@Centrify.com](mailto:David.McNeely@Centrify.com)  
(408) 542-7518

# Common UNIX Security IAM Challenges

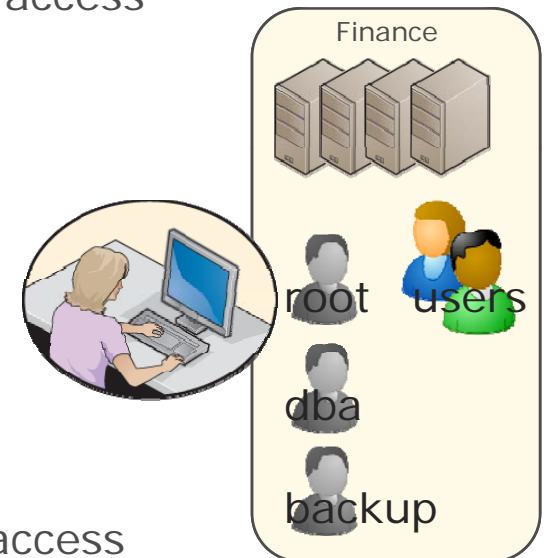
- Identity and access management challenges are common across most heterogeneous enterprises
  - Completely missing account and password policies
  - Weak password security
  - Lack of stringent user authentication and access controls
  - Limited privilege management
  - Syslog auditing is limited, lacking accountability
- Current solutions are not secure and don't provide management controls
  - /etc/passwd and NIS are passive systems
  - No delegation, change controls or auditing of administration actions



# UNIX Administration & Privilege Challenge

Privileged accounts are a core part of every system

- Privileged accounts grant complete control and full access
- Account passwords are typically shared within IT
- The system cannot track who uses these accounts
- These systems hold business sensitive data



Administration requires privileged access

- Many daily administrative tasks require privileged access
- Admins are trusted with privileged access

## Privileged Access in Current Environment

- Web Admin editing the httpd.conf requires root permissions

### User Session

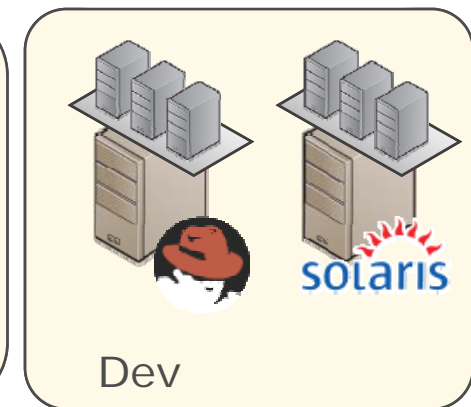
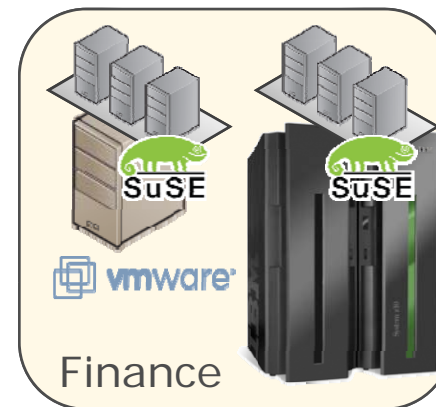
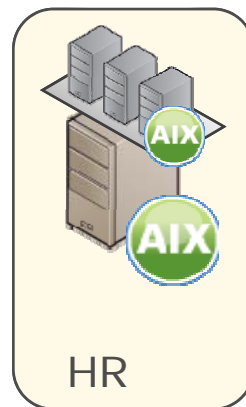
```
[twilson@test-rhel5 ~]$ su root
Password:
[root@test-rhel5 twilson]# vi /etc/httpd/conf/httpd.conf
[root@test-rhel5 twilson]# /sbin/service httpd restart
Stopping httpd:          [ OK ]
Starting httpd:          [ OK ]
[root@test-rhel5 twilson]#
```

### 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)
```

## Virtualizing Servers Amplifies IAM Issues

- Server virtualization causes exponential growth in the number of servers that need to be managed
- Privileged access to VM Hosts grants full access to the virtual data center
  - Virtual Servers are only protected by the VM host file system ACLs
- Some admin duties on the VM Host are shared with LOB Admins
  - LOB admins need to start/stop their servers



# Common Requirement for Security Best Practice



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

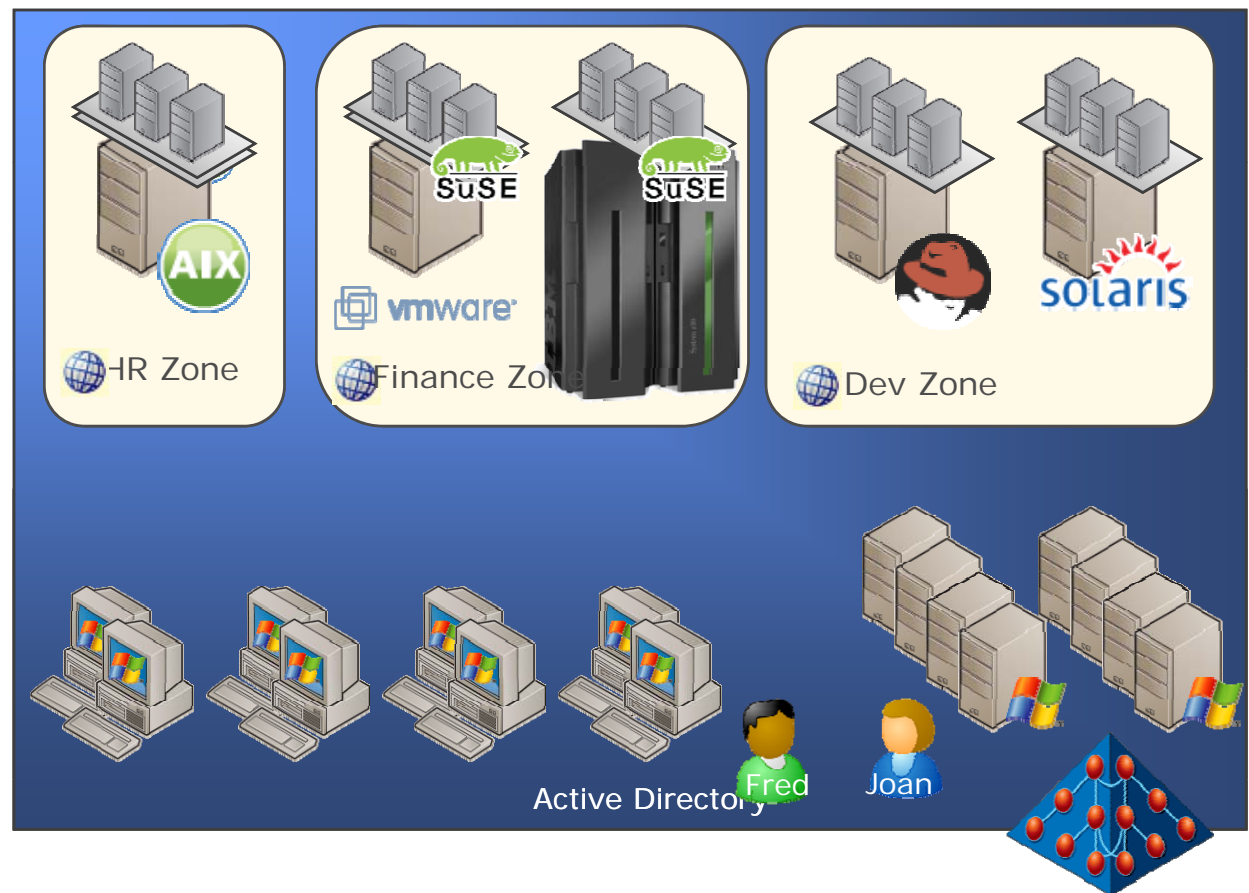


Payment Card Industry Data Security Standard

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

# Secure The Heterogeneous Environment

- Join physical and virtualized servers to Active Directory for Identity and Access Management
- Group into Zones by administrative role
- Active Directory services:
  - Controls authentication
  - Enforces security policy
  - Locks service accounts
  - Provides SSO
- Resulting in a secured server environment



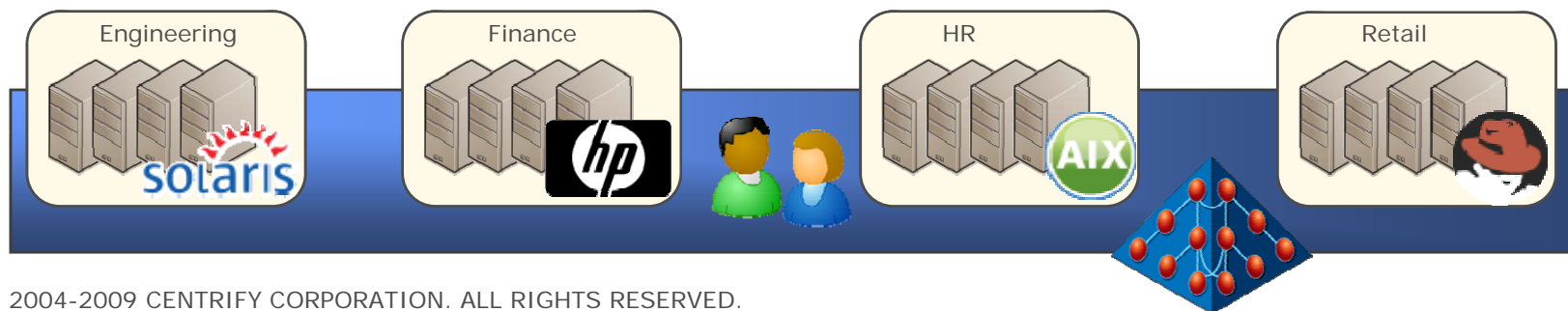
# Centralized Security Starts with Active Directory

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



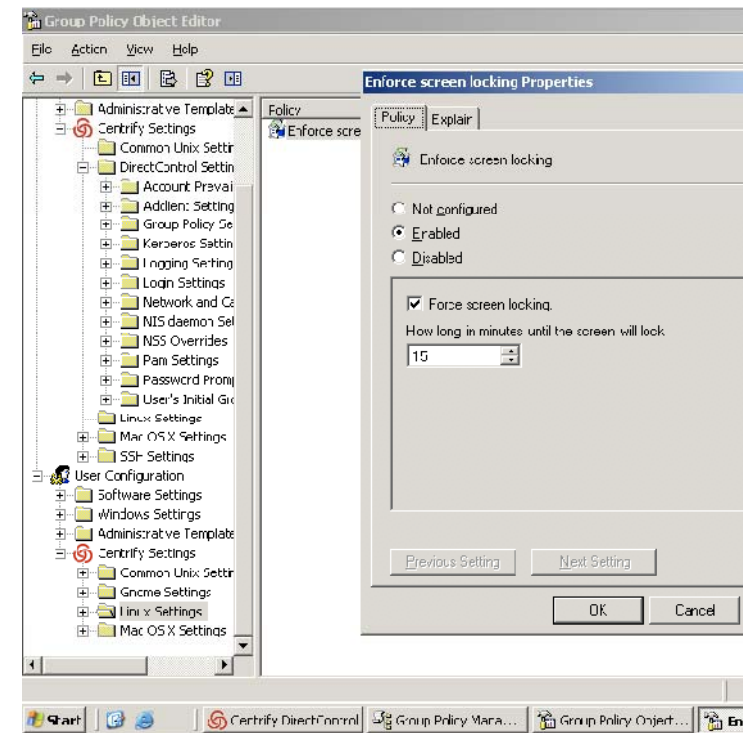
# Enforce System Security Policies

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

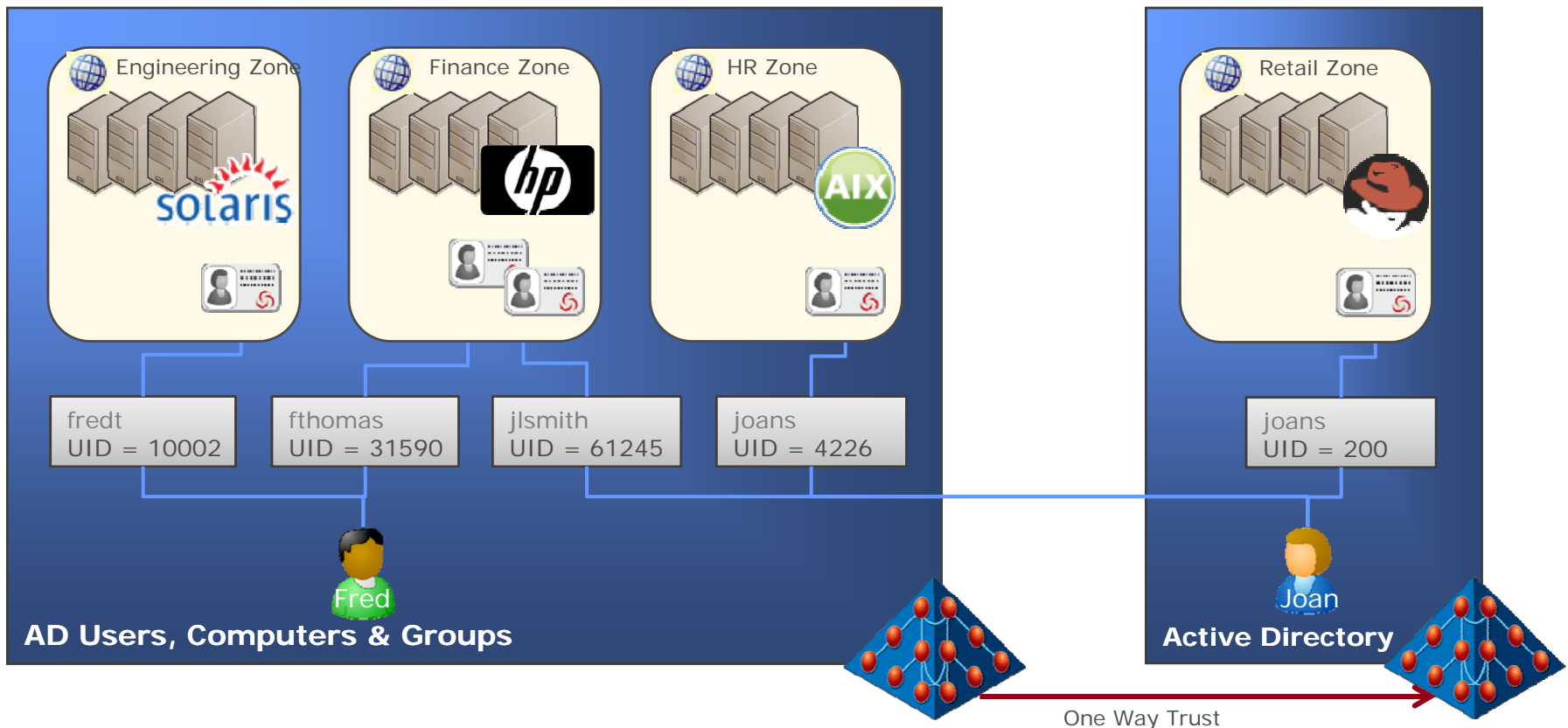
Group Policies enforce:

- 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



# Grant Access Only Where Required by Business

- 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



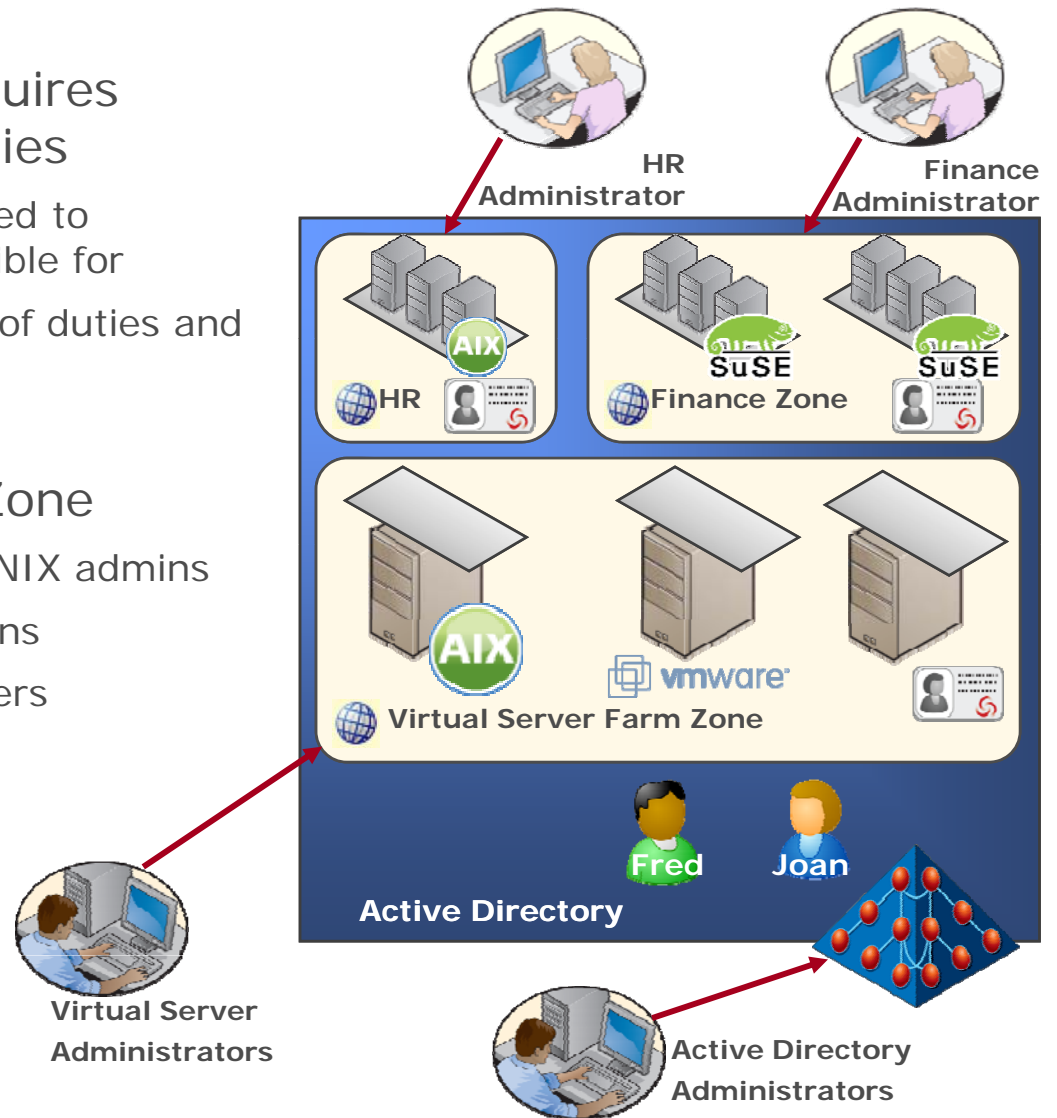
# Enforce Separation of Administrative Duties

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



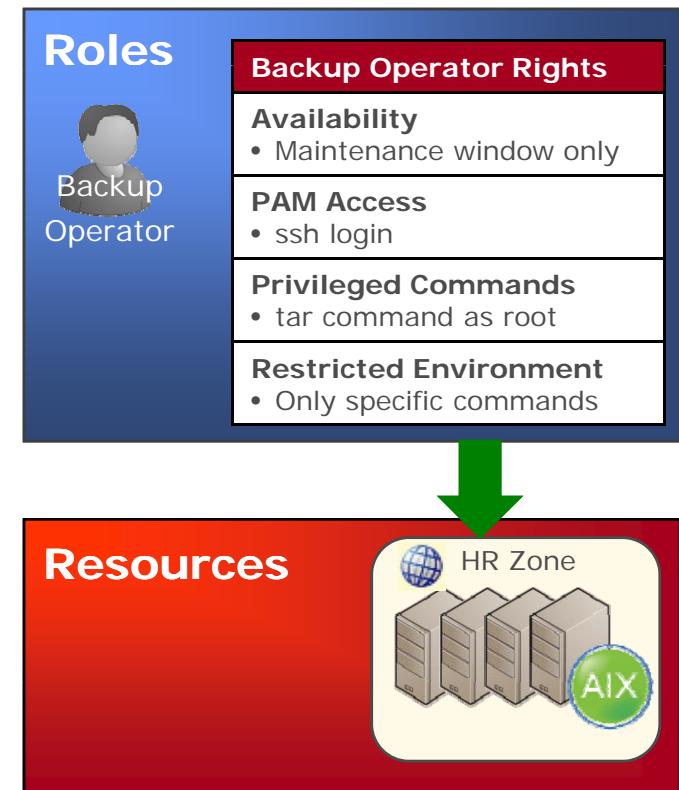
# Enforce Least Privilege with Role-based Policy

## 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

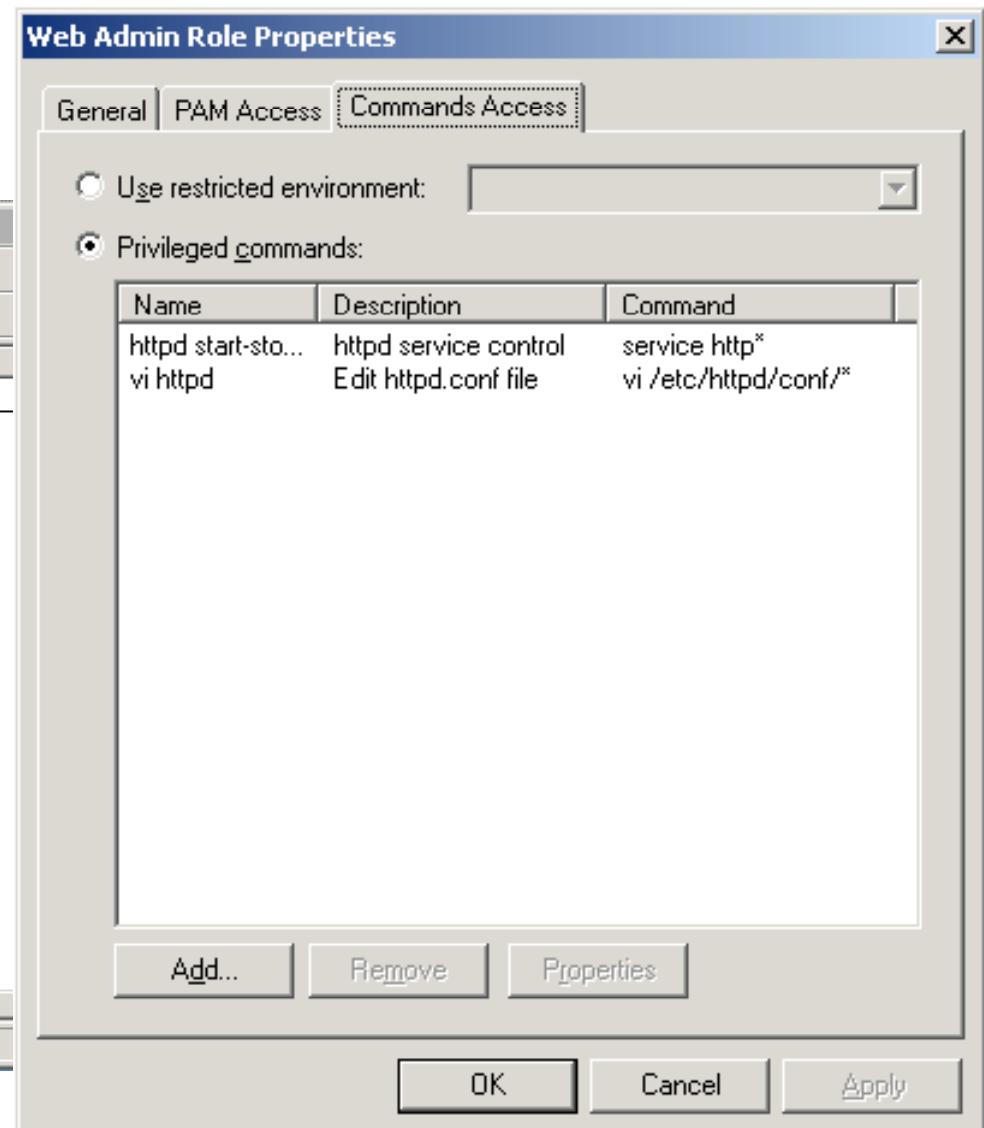
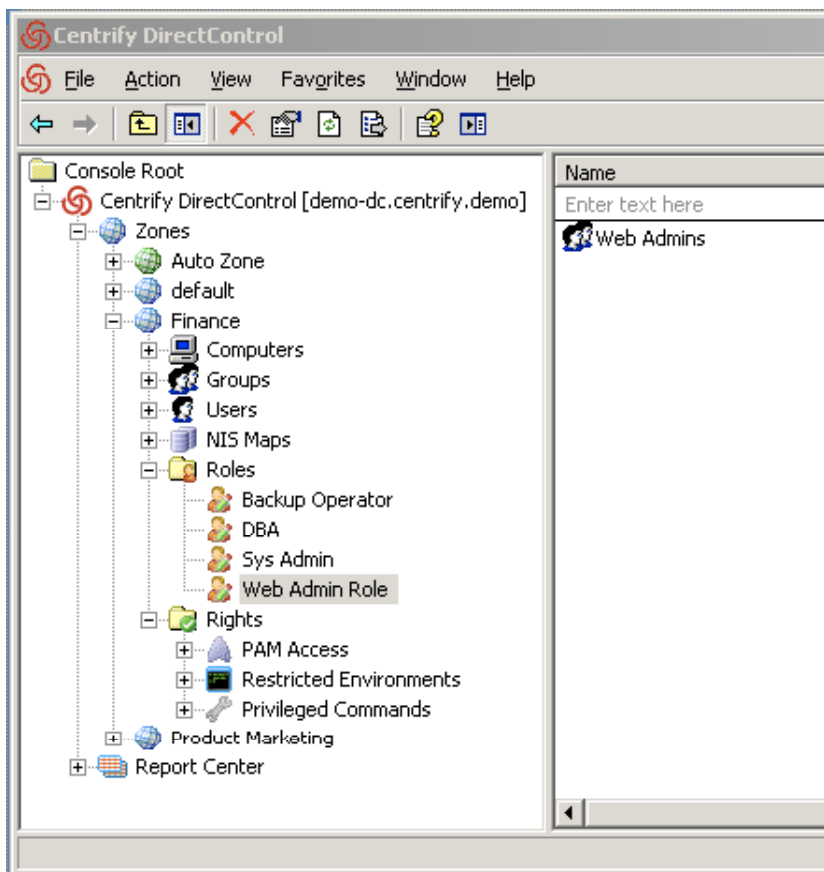
## Unix rights granted to Roles

- 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



# Grant Privileged Commands to Roles

- Web Admins need root privileges to manage Apache Services



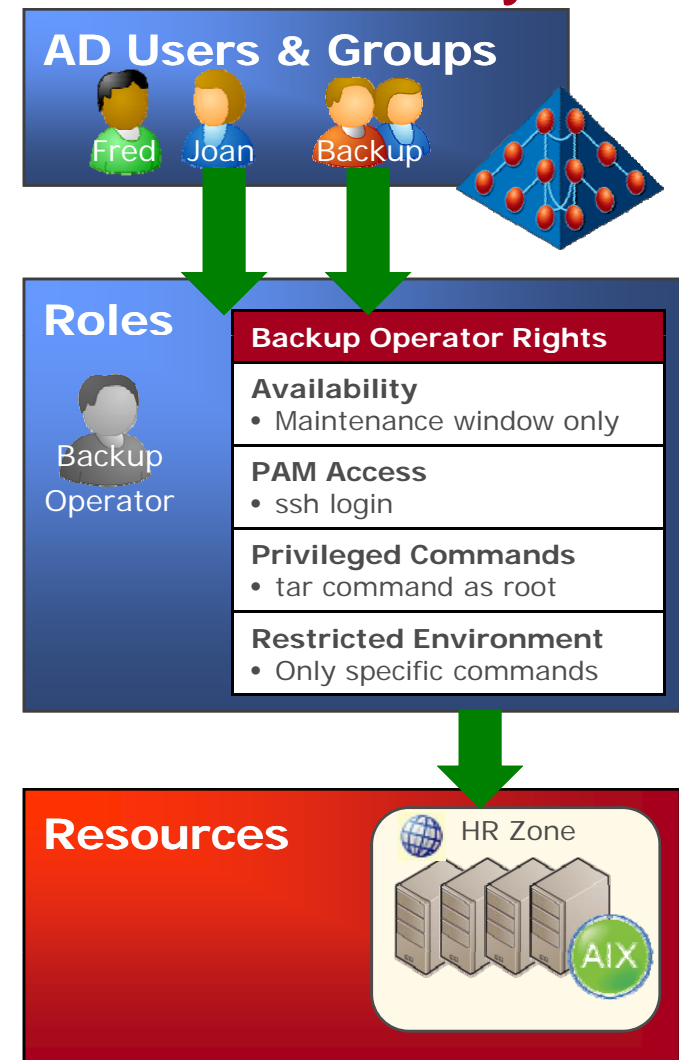
# Role Assignment in AD Ensures Accountability

## User 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



# 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 ~]$
```

## 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
```

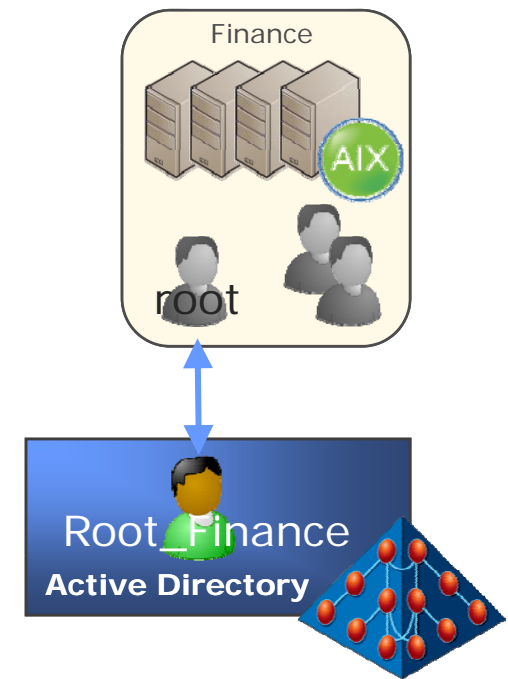
# Lock Down Privileged Accounts

Role-based Privilege Management (SUPM) for all users:

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

Lock the password for privileged and service accounts within Active Directory

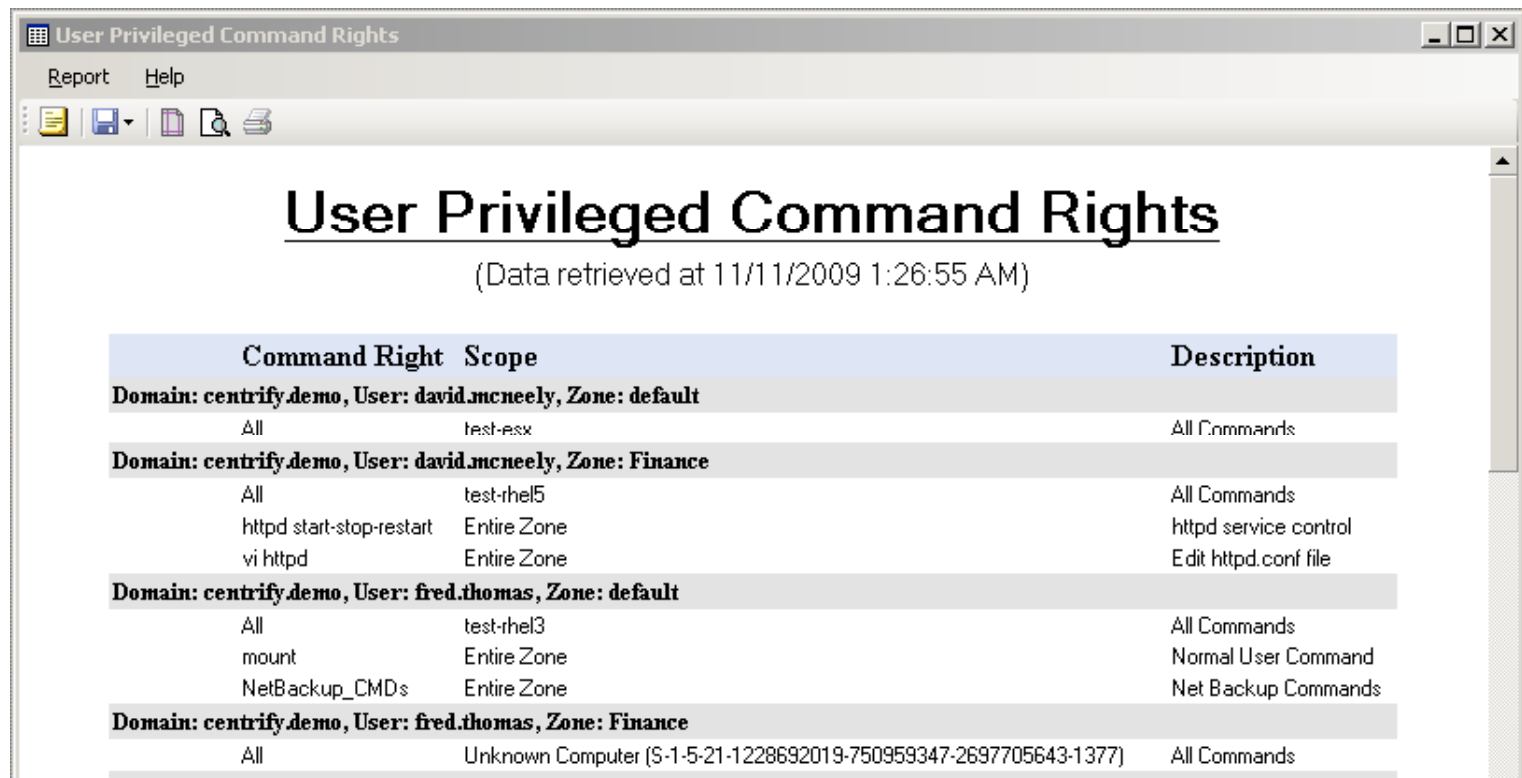
- Online login leverages AD password validation
  - Offline login uses a local cached account
  - Sync passwords for single user mode access
- 
- Or use SAPM tool to manage these accounts



# Accountability is Managed & Reported from AD

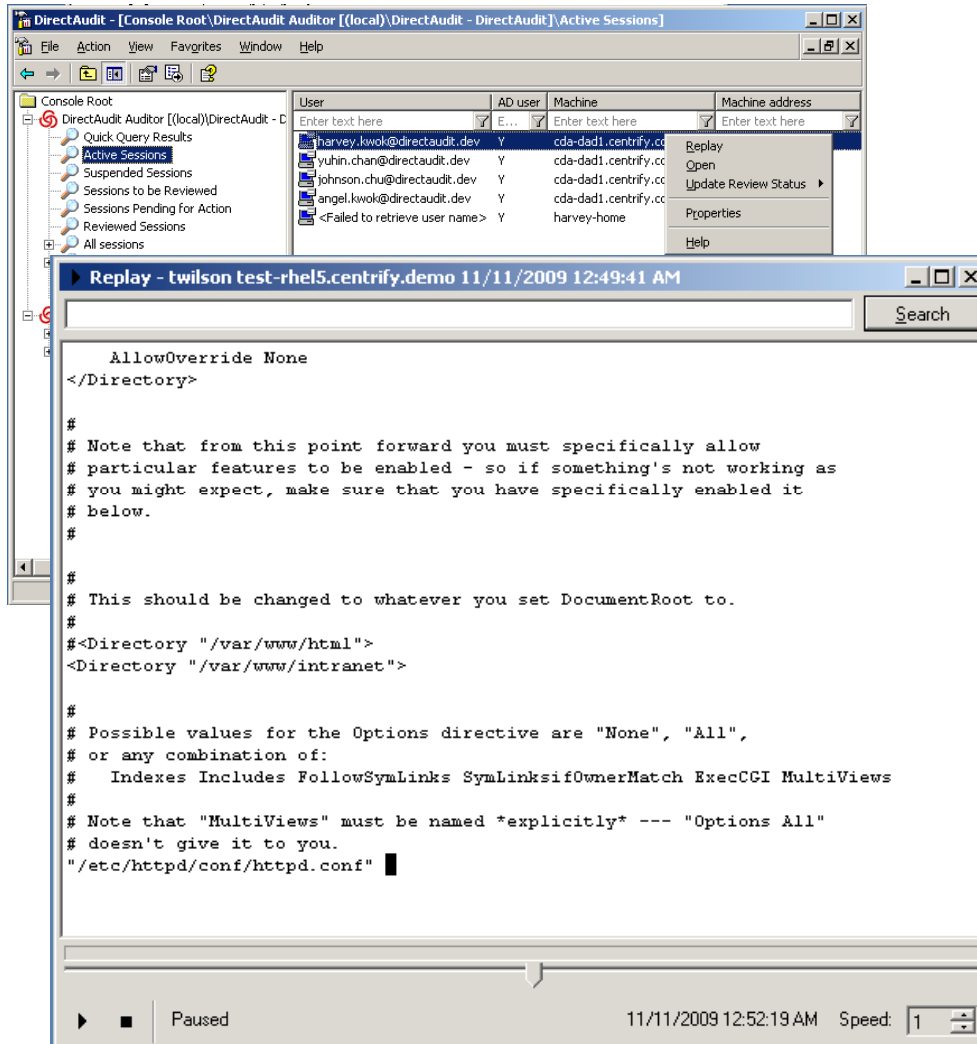
Authorization and Access Rights Reports are centrally created:

- 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

# Record Privileged User Activity to Satisfy Auditors



Unix system access is linked to users' unique AD account

Recording user access to systems

- Replay full user session activity
- 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

## Least Privilege Addresses Most Regulatory Requirements



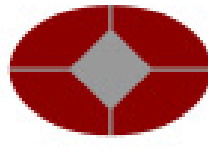
Sarbanes-Oxley Act  
Section 404



Federal Information Security Management Act



Health Insurance Portability and Accountability Act



Basel II. FFIEC Information Security Booklet



National Industrial Security Program Operating Manual

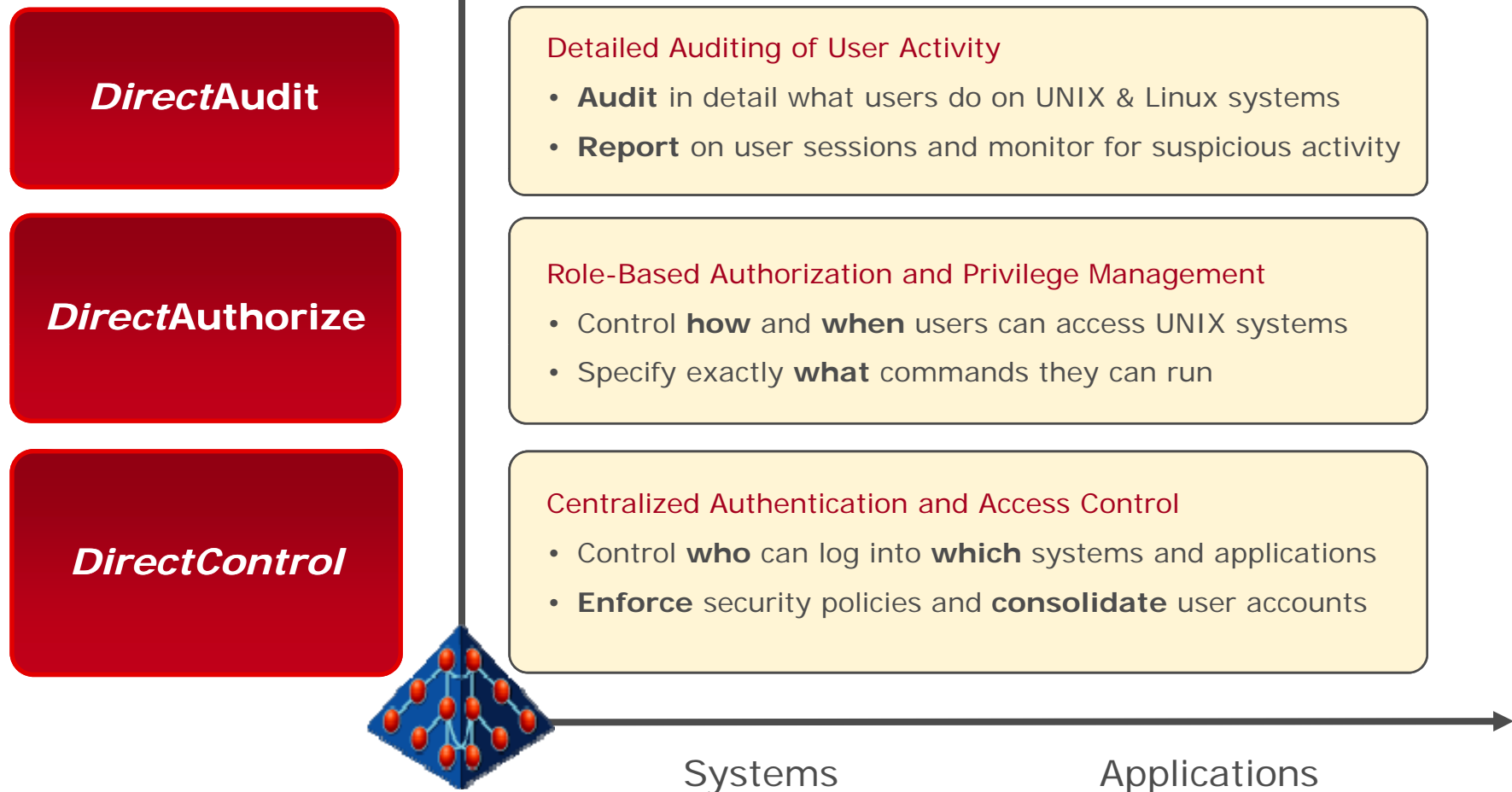


Payment Card Industry Data Security Standard

- ✓ System security policies are enforced
- ✓ Users can only access authorized systems
- ✓ Users granted specific privileges where required for their role
- ✓ Privileged accounts are locked down
- ✓ Separation of admin duties is enforced
- ✓ Privileged user activities are audited

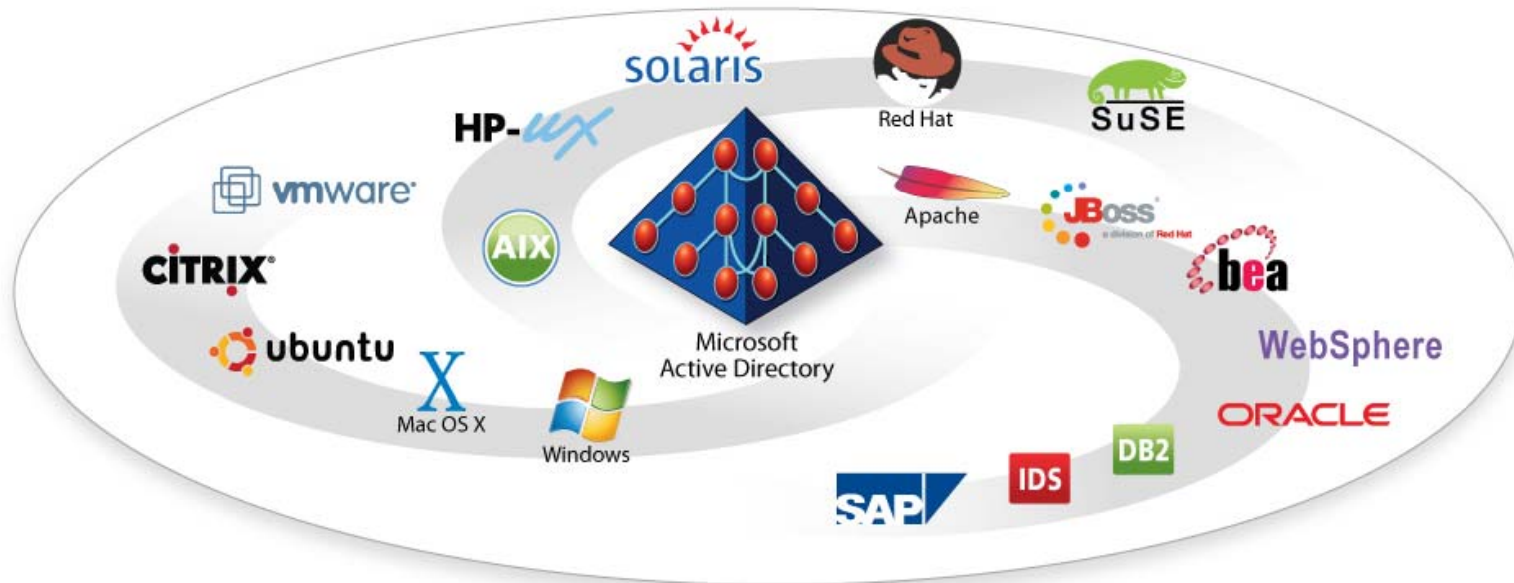
# Centrify Identity, Authorization and Audit Products

## IAM Optimization



# The Centrify Vision

Centralized Identity & Access Management Leveraging Active Directory



Centrify Suite improves IT efficiency, strengthens regulatory compliance initiatives, and centrally controls access and audits your heterogeneous computing environment.

