Trust but Verify

Leveraging Active Directory to Secure and Audit Access to On-premise and Cloud-based UNIX, Linux, and Mac Systems

David McNeely
Sr. Director of Product Management
Centrify Corporation
David.McNeely@Centrify.com
(408) 542-7518

Trust but Verify

In order to establish organization and protect our IT assets:

- Define Rules for the controlled environment
- Identify those who the Rules will apply to
- Authorize a set of Privileges to those to be trusted
- Monitor the use of those Privileges
- Take action on any misuse of those Privileges

These Rules can take many different everyday forms such as:

- Kids are allowed to use the internet – with software and parents monitoring
- We use freeways with speed limits – but Policemen and cameras monitor
- Passports grant access to other countries – Border patrol monitor activities

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Regulations Establish The Rules for IT

Information Assurance Security Controls are based on the same principles: rules, identity, authorization grants and monitoring

Federal Information Security Management Act

NIST Special Publication 800-53

Homeland Security Presidential Directive 12

Department of Defense Directive 8500.1

National Industrial Security Program Operating Manual

Federal Desktop Core Configuration

The Rules are well defined:

- Establish separation of duties
- Enforce system security policies
- Enforce network access policies
- Encrypt data-in-motion
- Enforce "least access"
- Require smartcard user login
- Lock down privileged accounts
- Grant privileges to individuals
- Audit privileged user activities

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

NIST 800-53 Provides Detailed Security Requirements

There are five identity and access management specific control families which we will look at more closely

- **Identity & Authentication (IA)**
  - Uniquely identify and authenticate users
  - Employ multifactor authentication
- **Access Control (AC)**
  - Restrict access to systems and to privileges
  - Enforce separation of duties and least-privilege rights management
- **Audit & Accountability (AU)**
  - Capture in sufficient detail to establish what occurred, the source, and the outcome
- **Configuration Management (CM)**
  - Develop/maintain a baseline configuration
  - Automate enforcement for access restrictions and audit the actions
- **Systems & Communications (SC)**
  - Boundary Protection
  - Transmission Integrity and Confidentiality
  - Cryptographic Key Establishment and Management including PKI Certificates

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Centrify's Proven Solution for Access Governance

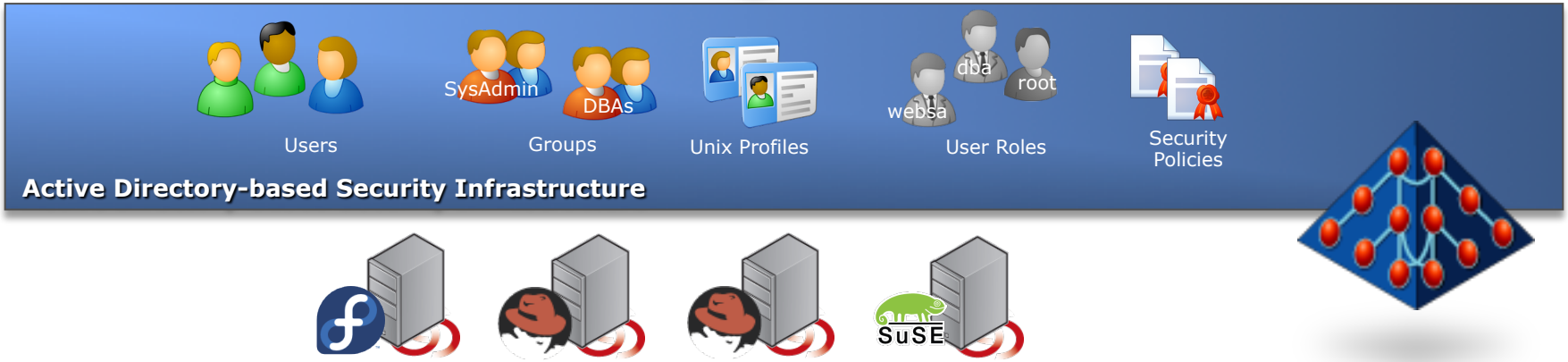
Centralizes Security Identity and Access Management within Active Directory

Identity Consolidation

- De-duplicate identity infrastructure
- Get users to login as themselves / SSO
- Single security policy definition
- Single point of administrative control

Privileged Access Management

- Associate privileges with individuals
- Enforce "least access & least privileges"
- Audit privileged user activities
- Isolate systems & encrypt data-in-motion



Protecting Systems. Authorizing Privileges. Auditing Activities.

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Centralized Management Presents Challenges

Centralization Goals

- Centralized UNIX Identities
- Establishing a global namespace
- Limited access granted where needed
- Locked down privileged accounts
- Privileges granted to individual users
- Audit privileged activities

Corresponding Challenges

- Legacy namespace is complex and different across many systems
- Individual system differences make centralization difficult
- Access rights are typically granted too broadly
- Granting privileges requires a simple way to create and manage the policies
- Integration with existing management processes

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Infrastructure as a Service Brings New Challenges

Adoption of IaaS is growing in the Enterprise

- Yankee Group says 24% are using IaaS, 60% are planning to use in 12 months
- Adoption trends are first in Development, then QA/Test, eventually to Production

Security remains the primary issue blocking Enterprise use

- Cloud Security Alliance identified 7 threats to cloud computing
- Gartner identified privileged user access as the #1 cloud computing risk

The Challenges to Enterprise use inexpensive public IaaS are very familiar

- Cloud server security is left to the customer
- Cloud server templates have common privileged accounts and passwords
- Cloud servers are typically deployed on public networks with dynamic IP addresses
- Access controls and activity auditing are left to the customer
- Applications hosted on these servers don’t enable end user single sign-on access

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Centrify Solution Automates Security Enforcement

Leverages Active Directory as Centralized Security Infrastructure

Protect Systems

- Group Policy enforces system security policies
- IPsec based network protection policies
- AD management of privileged accounts

Authorize Privileges

- AD-based unique identity
- Role-based access and privilege
- AD enforces separation of duties

Audit Activities

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

Automating Security for the Enterprise

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Leveraging Active Directory as Centralized Security Infrastructure

PROTECT SYSTEMS

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

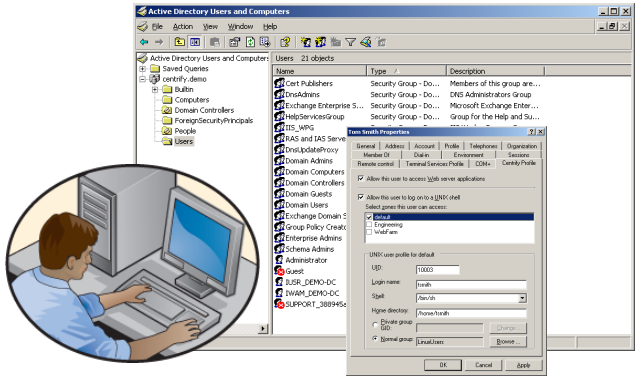
Active Directory-based Computer Identity

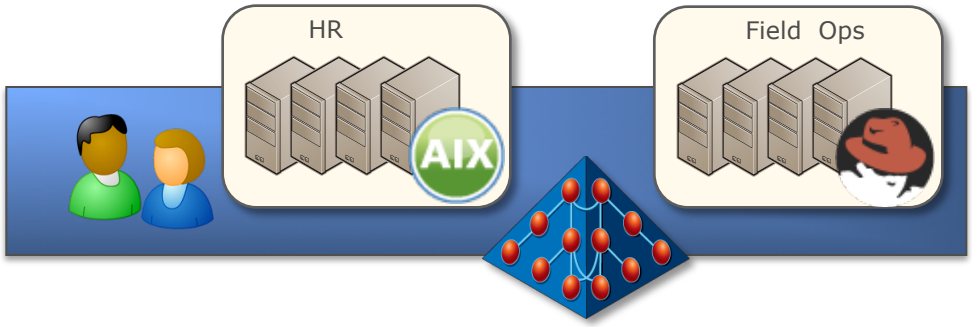
Active Directory services provide the foundation for Enterprise security

- 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

UNIX/Linux systems join Active Directory

- Establishing individual computer accounts for each system
- Automatically enrolling for PKI certificates and establishing Enterprise trust
- Enabling authorized Active Directory Users to login, online & offline
- Controlling user authentication for both interactive and network logins





© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Automated Security Configuration Management

Group Policy provides a platform to define standard baseline security settings to be enforced on all systems

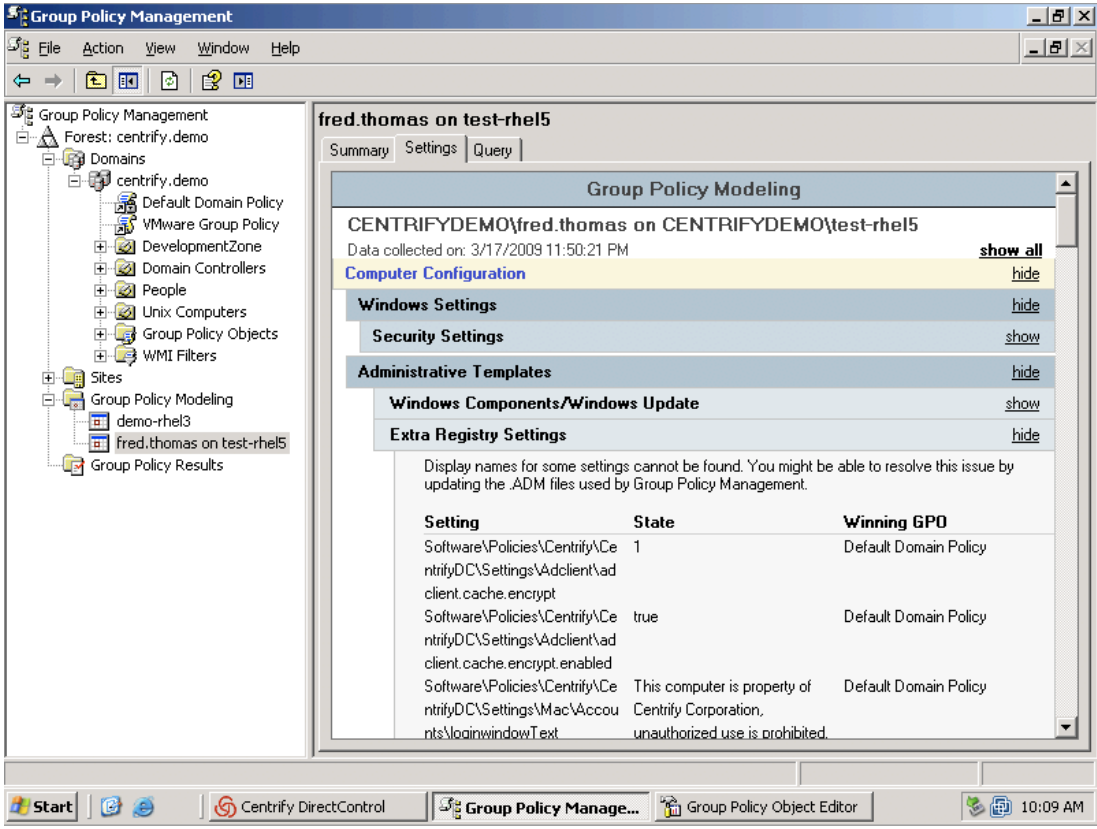
- DirectControl expands Group Policy usage to UNIX, Linux and Mac OS X systems

Mac Group Policies enable central system configuration

- Eliminating the need for OD & Workgroup Manager

Group Policy Management Console provides security baseline management

- Backup/Import Settings
- Modeling & Reporting on Policies

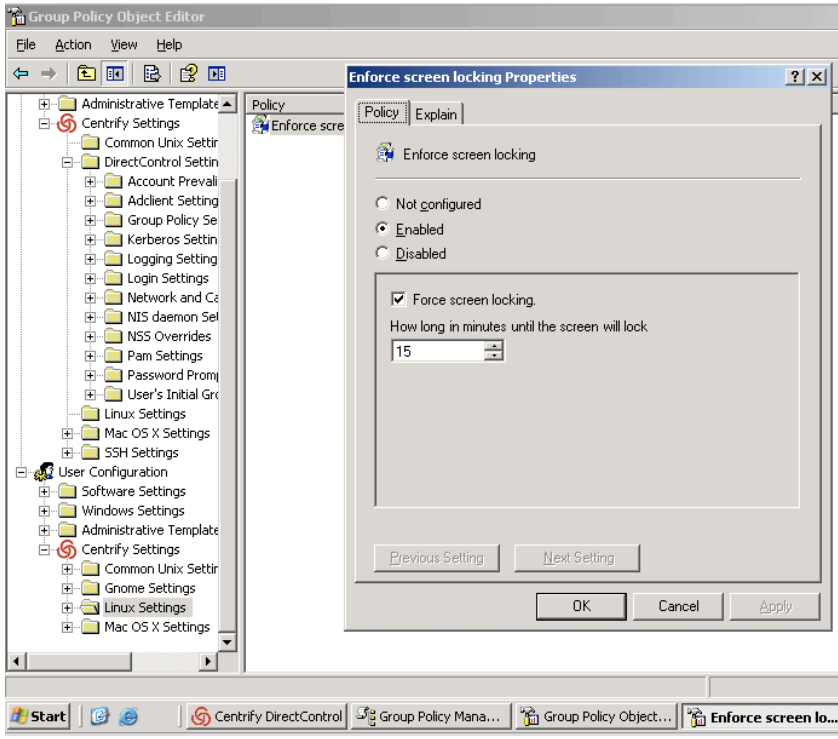


© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Security Policies Enforced by Group Policy

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

- Group Policy is automatically enforced at system join to Active Directory
- Group Policy routinely checks the system for compliance, updating as required
- User Group Policy is enforced at user login



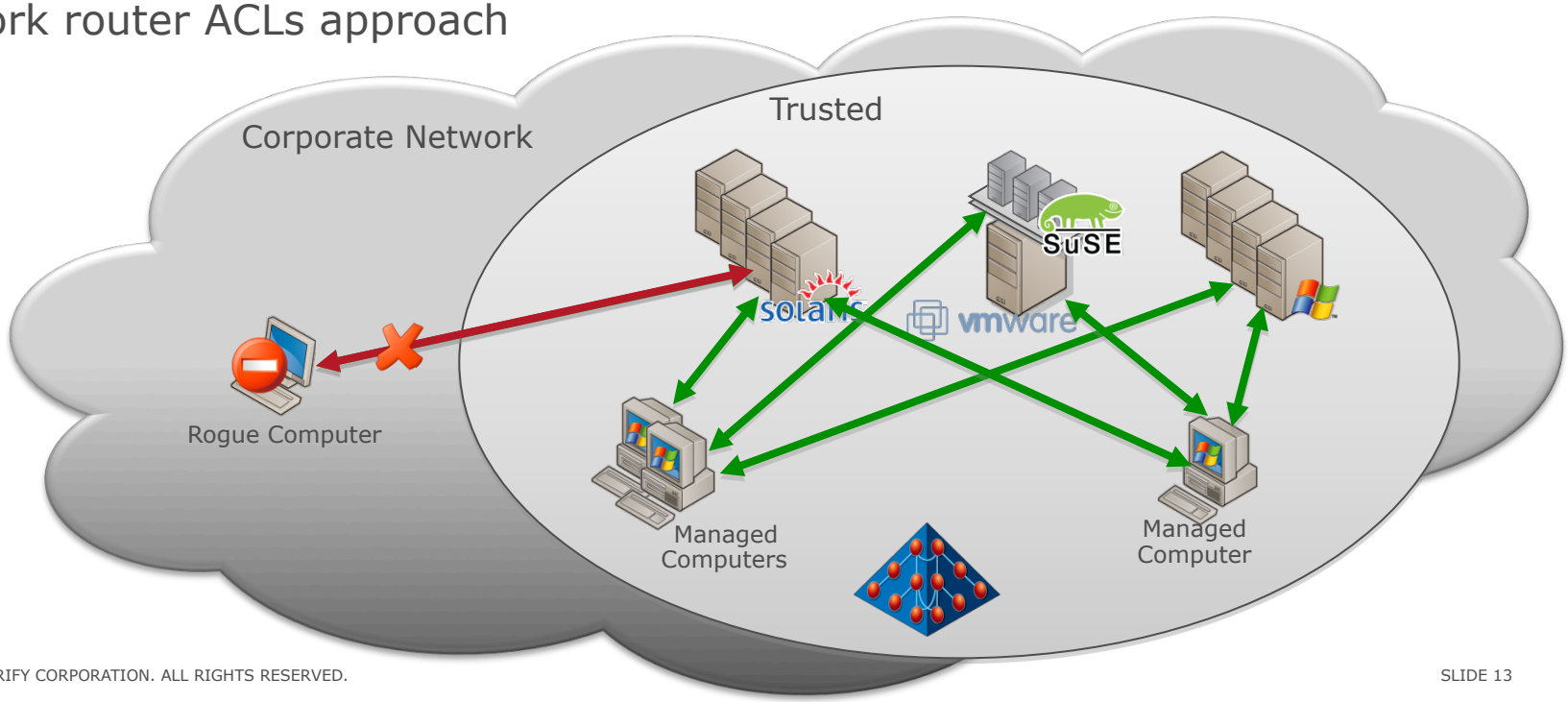
Group Policies enforce:

- System authentication configuration
- System Banner settings
- Screen Saver & Unlock policies
- SSH policies control remote access security
- Firewall policies control machine access
- Mac OS X specific policies control the system and user's environment

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Prevent Data Breaches from External Threats

- IPsec Transport Mode isolates the entire enterprise, preventing access by rogue or untrusted computers and users — reducing the attack surface
- Network-level access controls are much more important when:
  - Enterprise network boundaries become porous as they include wireless and grow exponentially
  - Users' work becomes more virtual, accessing corporate resources from mobile / remote locations
- Software- and policy-based approach lets you avoid an expensive VLAN and network router ACLs approach



© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

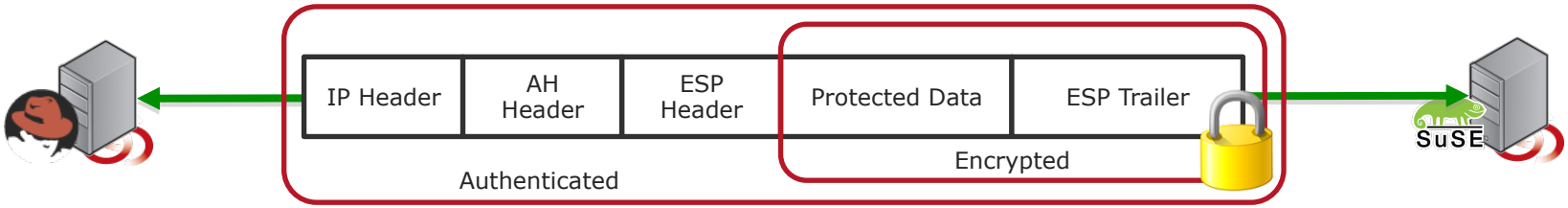
Isolate Sensitive Servers & Protect Data-in-Motion

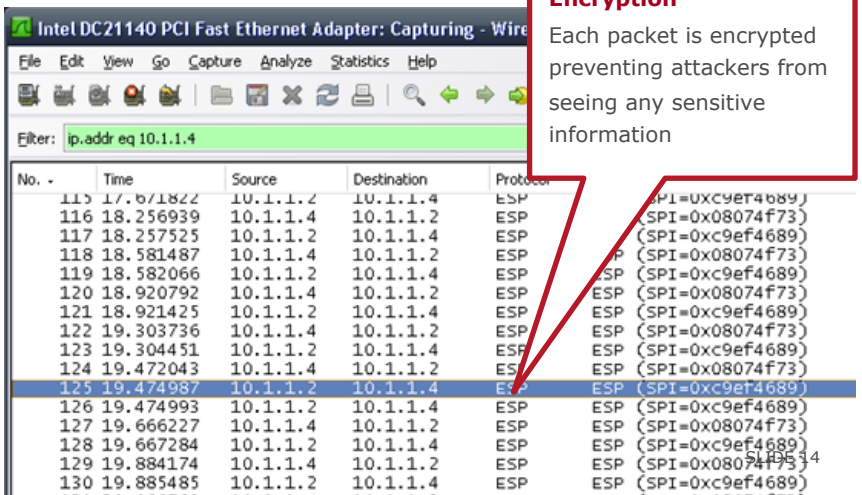
IPsec authentication policies logically isolate sensitive servers independent of physical network location

- Sensitive information systems are isolated based on PKI identities and AD group membership

IPsec encryption protects data-in-motion without modifying older applications

- Enforce peer-to-peer, network-layer encryption for applications that transport sensitive information





Encryption

Each packet is encrypted preventing attackers from seeing any sensitive information

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

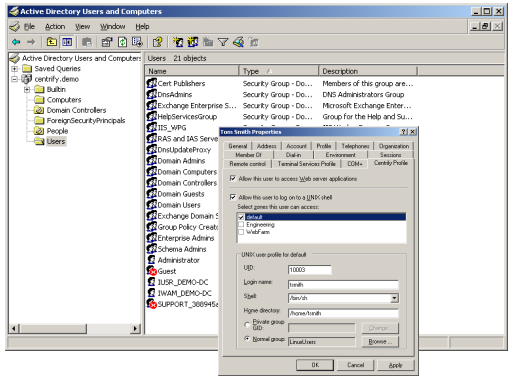
Leveraging Active Directory as Centralized Security Infrastructure

AUTHORIZE PRIVILEGES

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Active Directory Centralizes Account Management

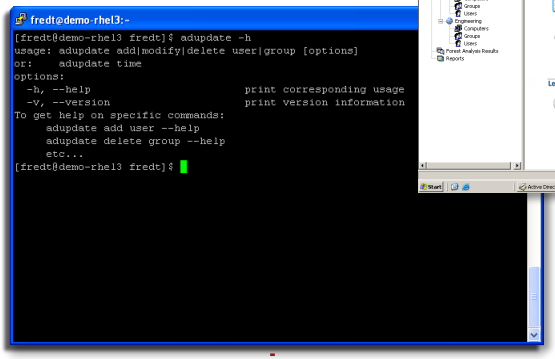
- UNIX Account administration leverages centralized Active Directory processes and automation
- Account and authentication policies are enforced on all systems



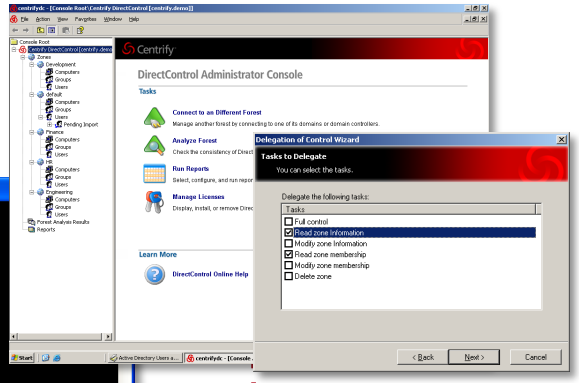
Active Directory Users and Computers

Existing Identity Management Solutions

Provisioning APIs/Tools



Unix Command Line Interface



MMC Admin Console

Active Directory-based Security Infrastructure

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Centralize The Most Complex UNIX Environments

Zones uniquely simplifies the integration and centralized management of complex UNIX identity and access permissions into Active Directory

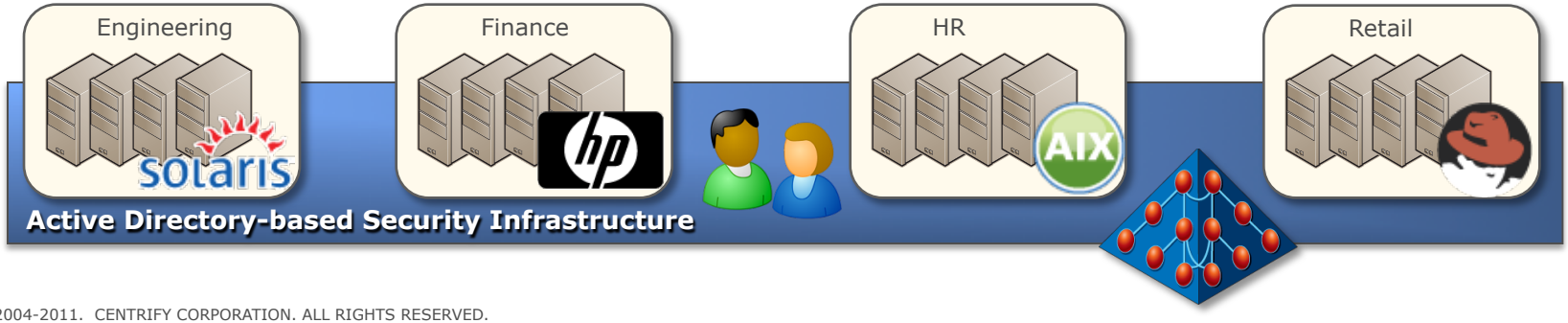
- Only solution designed from the ground up to support migration of multiple UNIX environments and namespaces into a common Directory
- Zones provides unique ability to manage UNIX identity, UNIX access rights and delegated administration

Centrify supports native AD delegation for separation of duties

- Zones create natural AD boundaries for delegated UNIX administration of a group of systems through AD access controls on UNIX Zone objects

Seamlessly integrate administration into existing IDM systems

- AD Group membership controls the provisioning of UNIX profiles granting access and privileges
- IDM systems simply manage AD Group Membership in order to control the environment



© 2004-2011. CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

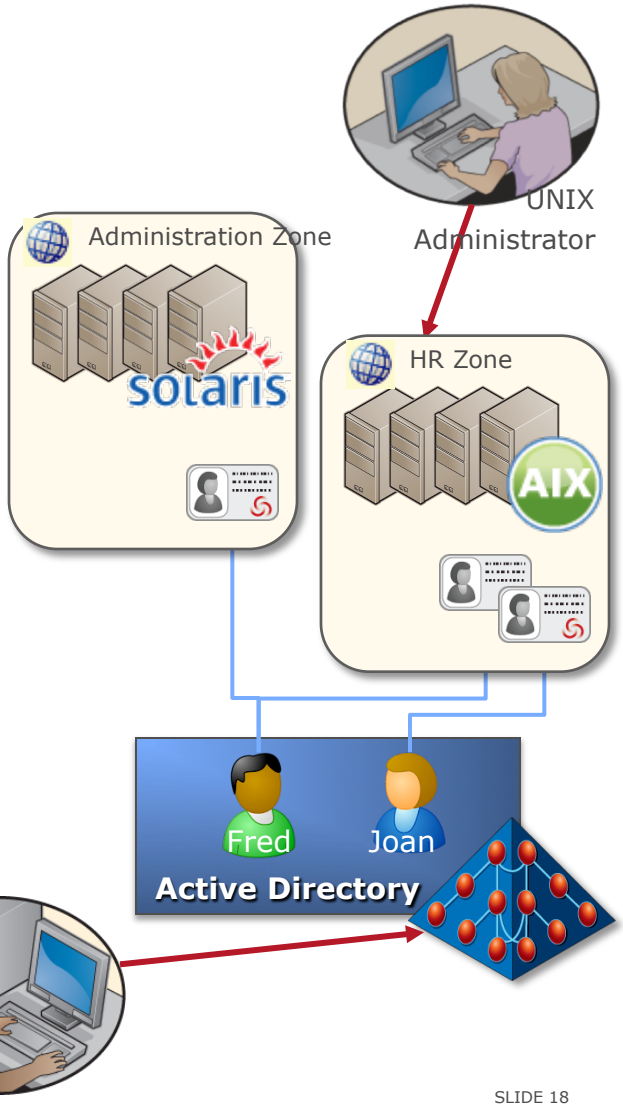
Ensure Separation of Administrative Duties

Separation of AD and Unix Admins

- User's Unix profile are stored independent of AD User object
- Unix Admins don't need rights to manage AD User objects, only Unix profiles

Separation of Unix Departmental Admins

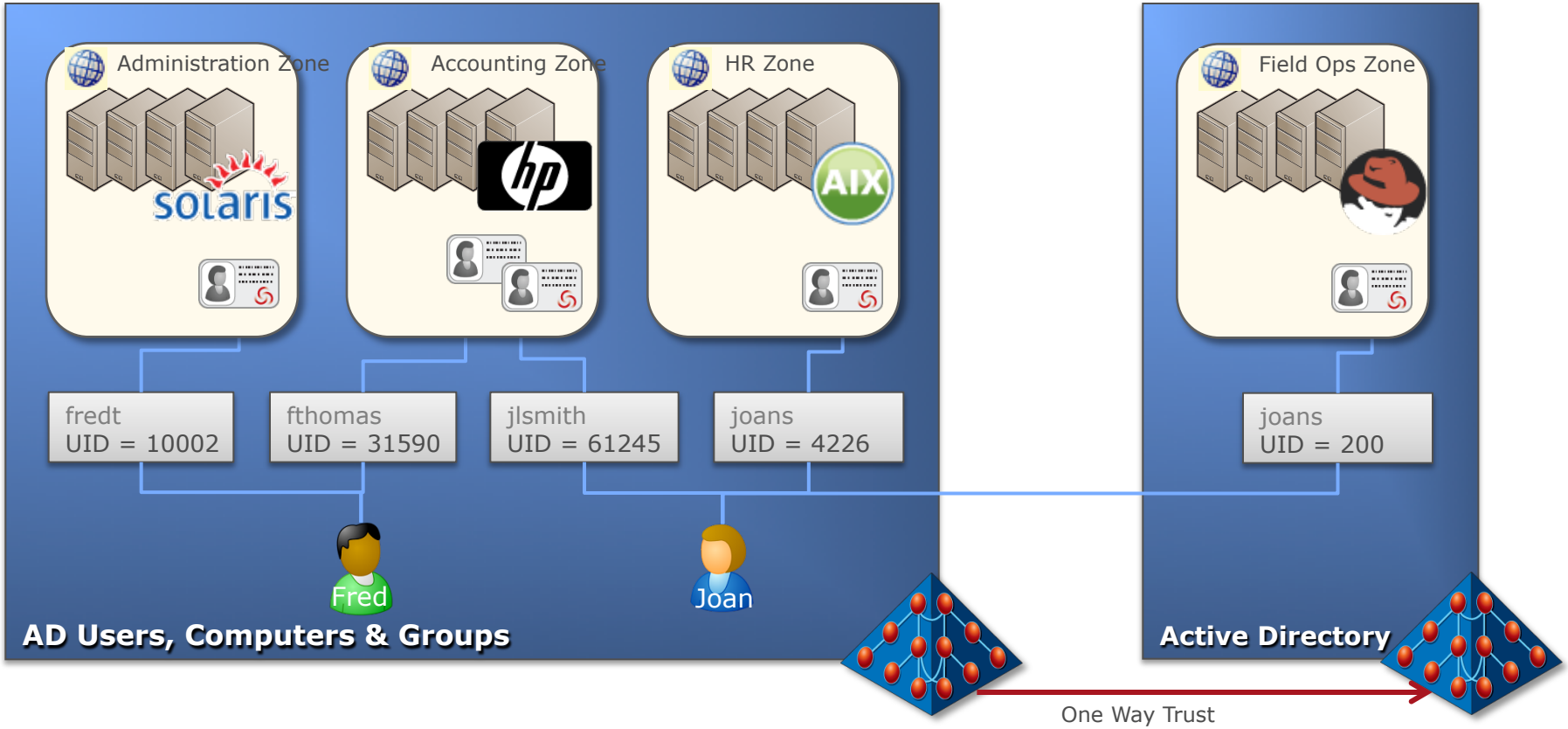
- Each Zone is delegated to the appropriate Unix Admin
- Unix Admins only need rights to manage Unix profiles within their own Zone



© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Least Access is Enforced Through Zones

- System Access is denied unless explicitly granted
- Access is granted to a Zone (a logical group of systems)
- Users' UNIX Profiles within a Zone are linked to the AD User



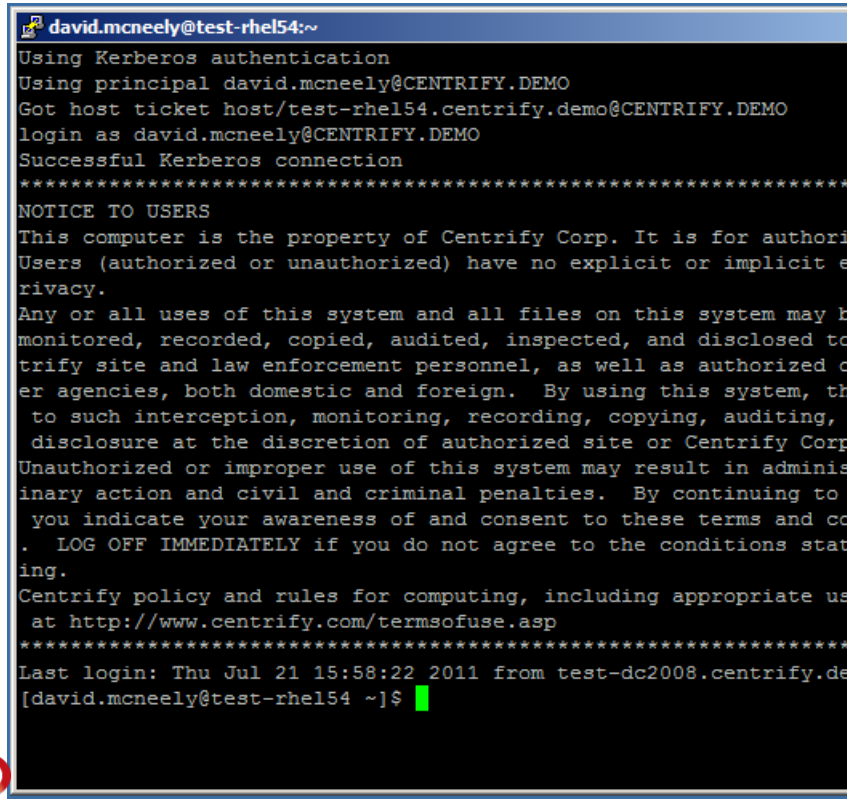
© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Active Directory-based User Login

Smartcard login policies are also enforced

- DirectControl for OS X supports CAC or PIV smartcard login to Active Directory granting Kerberos tickets for SSO to integrated services
- Users configured for Smartcard interactive login only are not allowed to login with a password, however Kerberos login after smartcard is allowed

Kerberos provides strong mutual authentication to Servers after desktop smartcard login



© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

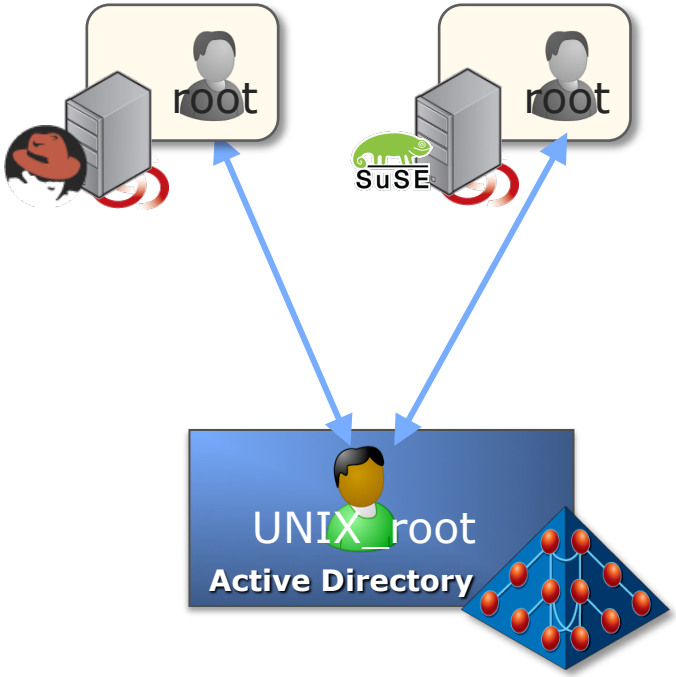
Lock Down Privileged Accounts

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



© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

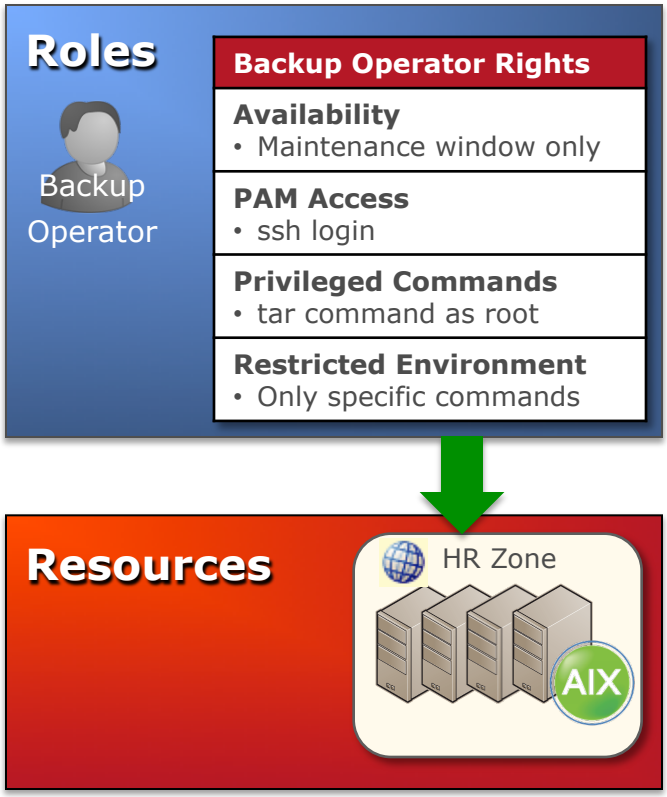
Associate Privileges with Named Individuals

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

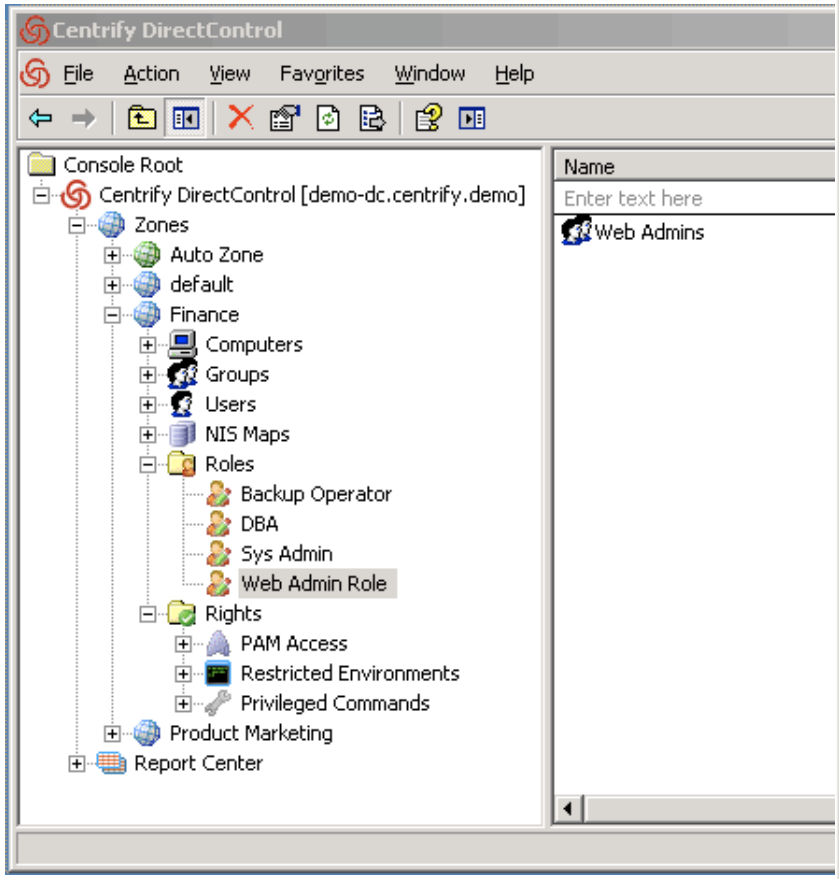
- Availability – controls *when* a Role can be used
- PAM Access – controls *how* users access UNIX system interfaces and applications
- Privilege Commands – grants elevated privileges where needed
- Restricted Shell - controls allowed commands in the user's environment

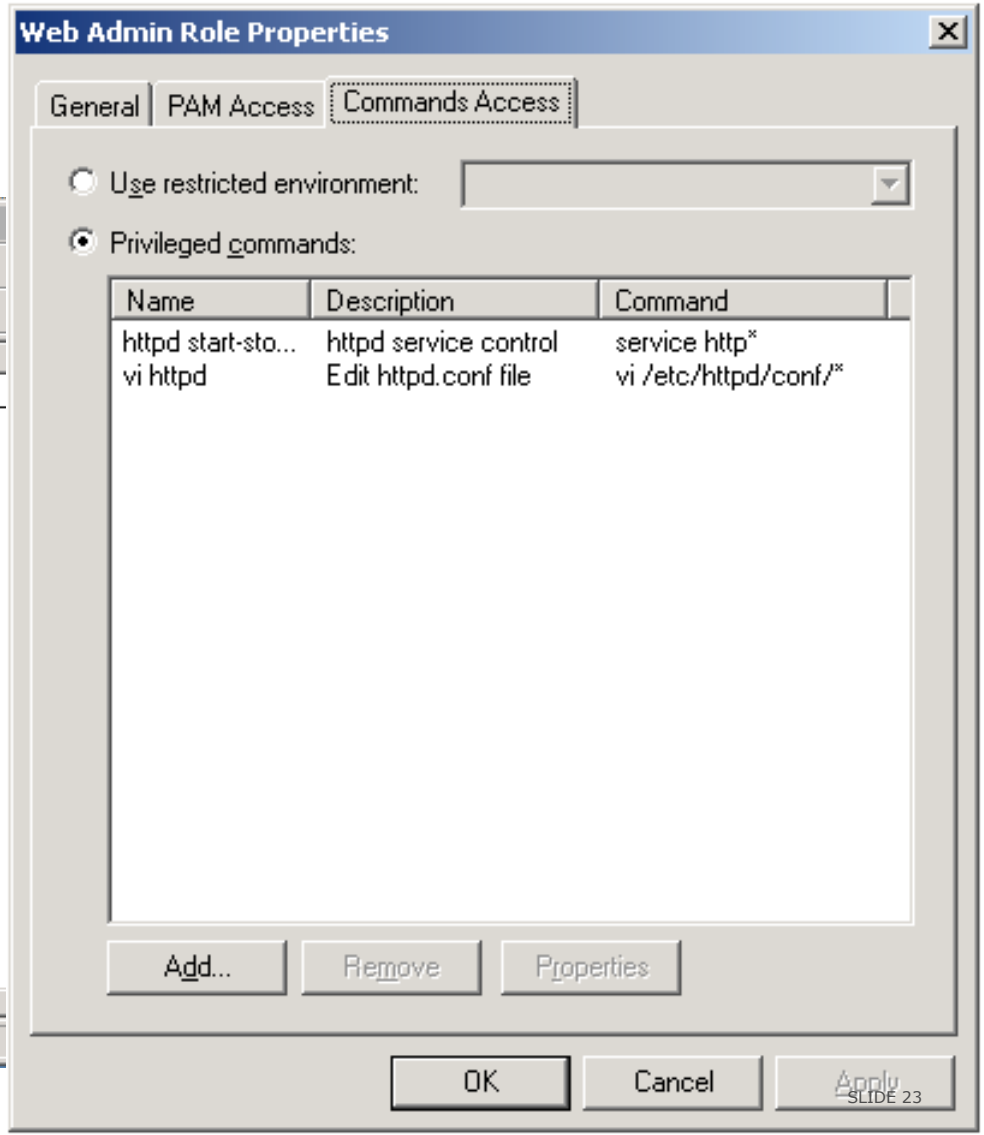


© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Grant Privileged Commands to Roles

- Web Admins need root privileges to manage Apache Services





© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

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

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

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)
```

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

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 ~]$
```

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

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
```

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Leveraging Active Directory as Centralized Security Infrastructure

AUDIT ACTIVITIES

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

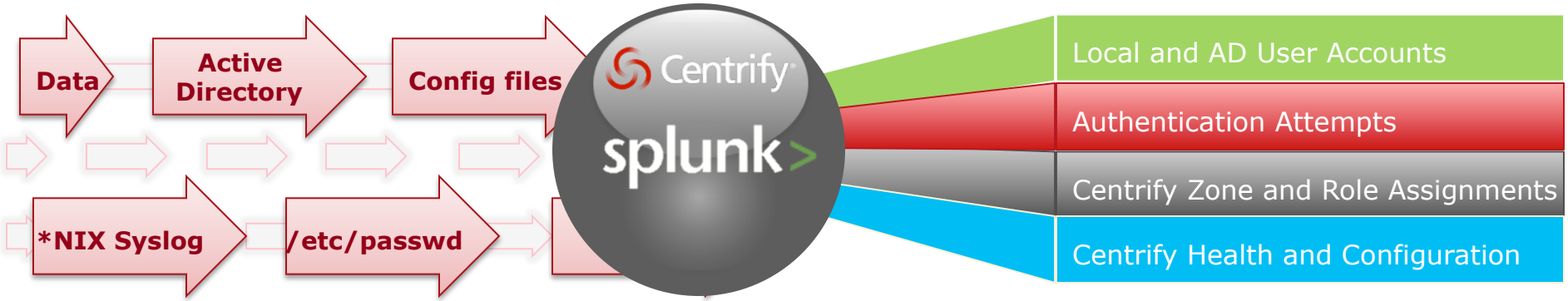
System Logs and Events Provide Limited Visibility

Show me accounts not used in last 90 days.

Are there any systems where Centrify is not connected?

How long was a user in a role?

- Syslog rollup brings in operational intelligence from other systems, apps, SIEM, security devices, etc.



I want to see all failed login attempts.

Are there any newly created local accounts on my server?

Who zone-enabled this user?

- Shows changes in AD, *nix login attempts, Windows login attempts, Centrify agent health, etc.

© 2004-2011. CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

For Monitoring and Reporting of Logged Changes

splunk > Centrify

Logged in as admin | App | Manager | Alerts | Jobs | Logout

Dashboards | Logs and Configs | Search | Support | Help | About

Centrify Insight Overview | Actions

All time

Getting Started

Add the data sources required for this app to provide meaningful functionality:

- Splunk Search Head — Install Splunk 4.2, install this app, enable the twitter input and forward the remaining boxes here.
- Windows Domain Controller(s) — Install the Windows Universal Fowarder. Collect Security Log and Active Directory. Must be run as an Active Directory domain user.
- Centrify managed *NIX boxes — Install Splunk 4.2, install this app, enable the appropriate inputs and forward to the Splunk Search Head.

To learn more about this app and Centrify:

- Read the Installation Guide
- Free Active Directory Tools for UNIX, Linux and Mac
- Centrify Express Community
- Splunk Answers for Centrify Insight
- Centrify Customer Support
- Centrify Support Tweets

NOTE: There are several scheduled searches we run on a regular basis in Splunk Enterprise. In Splunk Free you will need to manually run these searches once or twice a day. It is also useful to manually run these searches after changes like turning on addebug to collect centrifydc.log data.

- Reload centrifydc.log hosts
- Reload centrifydc.log modules
- Reload Active Directory Lookups

Centrify Insight Dashboards

Gain insight about users, groups and computers managed through Active Directory and the Centrify Suite. Requires the appropriate data sources to be configured. See the getting started section or the Centrify Insight documentation for more information.

Centrify Zone User

Active Directory U

Search Centrify Di

Recent Centrify Support Tweets

date	tweet
about a month ago	adinfo adds a capability to validate AD user and password against a given domain. E.g., adinfo -A -u ADUSERNAME
about a month ago	Centrify Suite 2011 now integrates more than 280 UNIX, Linux and Mac platforms with Microsoft Active Directory.
about a month ago	Centrify Suite 2011 now available for download. For more details, visit http://bit.ly/hLcvok (Requires login to Centrify S
about a month ago	@pwyliu : Did you mean SLES 11 SP1 ? If so 'yes'. Please check out our detailed list of supported platforms here: http
about a month ago	RT@CentrifyNews: Happy 6 year birthday #Centrify #DirectControl !! | http://bit.ly/bYTSc6 | V1.0 had support for only

twamley

Updated 5 minutes ago by TANGO\Administrator

tango.se/Program Data/Centrify/Zones/DMZ/Users/twamley — tango.se/Users/David Twamley

Centrify Zone	UNIX User	UID	Shell	Home	GID	Enabled	When Created
DMZ	david ⇒ twamley	10001	/bin/csh	/home/twamley	10000	True	01:53.28 am, Tue 03/29/2011

Show all 512 lines for 1 events DC — WIN-D64N2IVJ19B.tango.se Windows Event Codes — 5136

2

splunk > Centrify

Logged in as admin | App | Manager | Alerts | Jobs | Logout

Dashboards | Logs and Configs | Search | Support | Help | About

Search Active Directory and Zones | Actions

Object Type	Activity Type	Group Type	Search Text
Group	Altered Membership	Global Distribution	employees

Search

≥ 2 matching events | 43,097 scanned events Create alert Add to dashboard Save search

Employees

Added member(s) to this group about a minute ago by TANGO\IT

tango.se/Users/Employees

AD Group	Group Scope	Group Type	Mail	Affected Members
Employees	Global	Distribution	employees@tango.se	tango.se/Users/Alpha tango.se/Users/Bravo tango.se/Users/Charlie

Show all 264 lines for 8 events DC — WIN-D64N2IVJ19B.tango.se Windows Event Codes — 4750, 4751, 5136

1

Employees

Added member(s) to this group 3 days ago by TANGO\IT

tango.se/Users/Employees

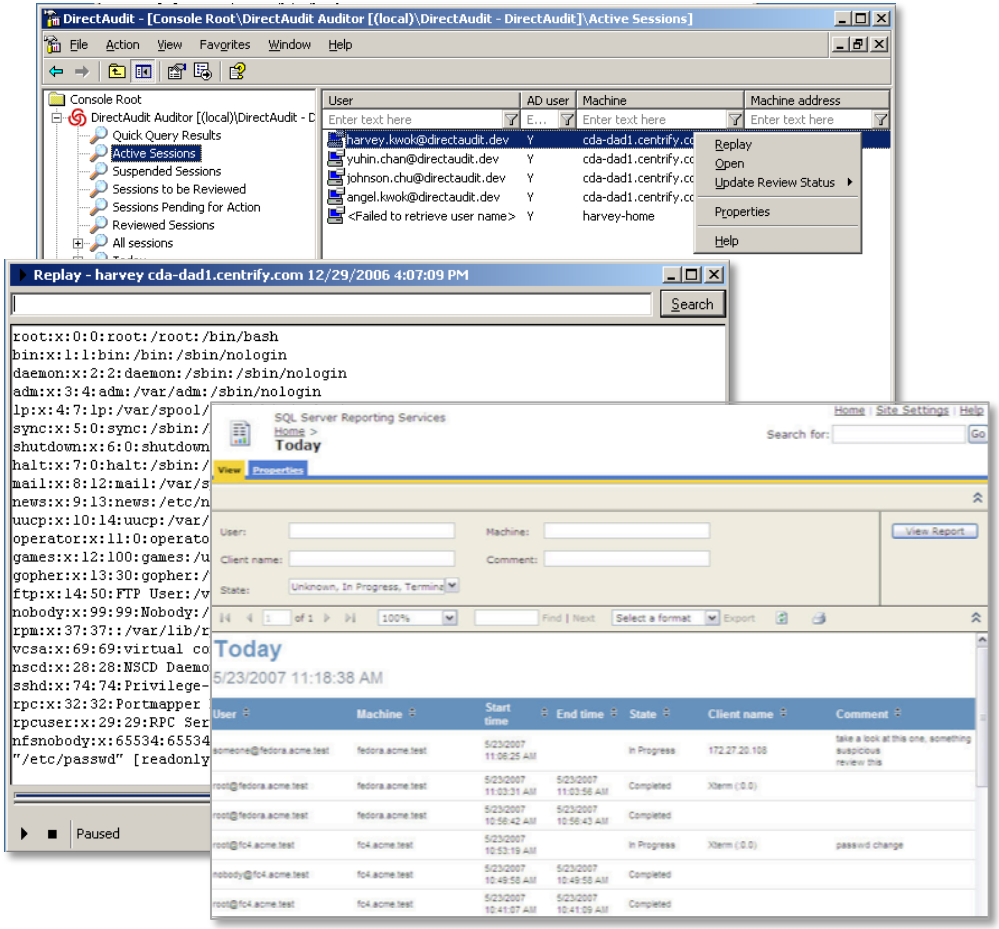
AD Group	Group Scope	Group Type	Mail	Affected Members
Employees	Global	Distribution	employees@tango.se	tango.se/Users/David Twamley

Show all 88 lines for 3 events DC — WIN-D64N2IVJ19B.tango.se Windows Event Codes — 4750, 4751

2

© 2004-2011. CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

High Definition Visibility Provided by Session Recording



UNIX system access & activity is linked to users' unique AD account

Tracks all user access to systems

- Provides full user session replay
- Shows what commands were executed
- Shows what changes they made to key files

Centrally search captured sessions for events, such as:

- All accesses to sensitive files
- Any execution of shutdown or kill
- All su and sudo executions

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

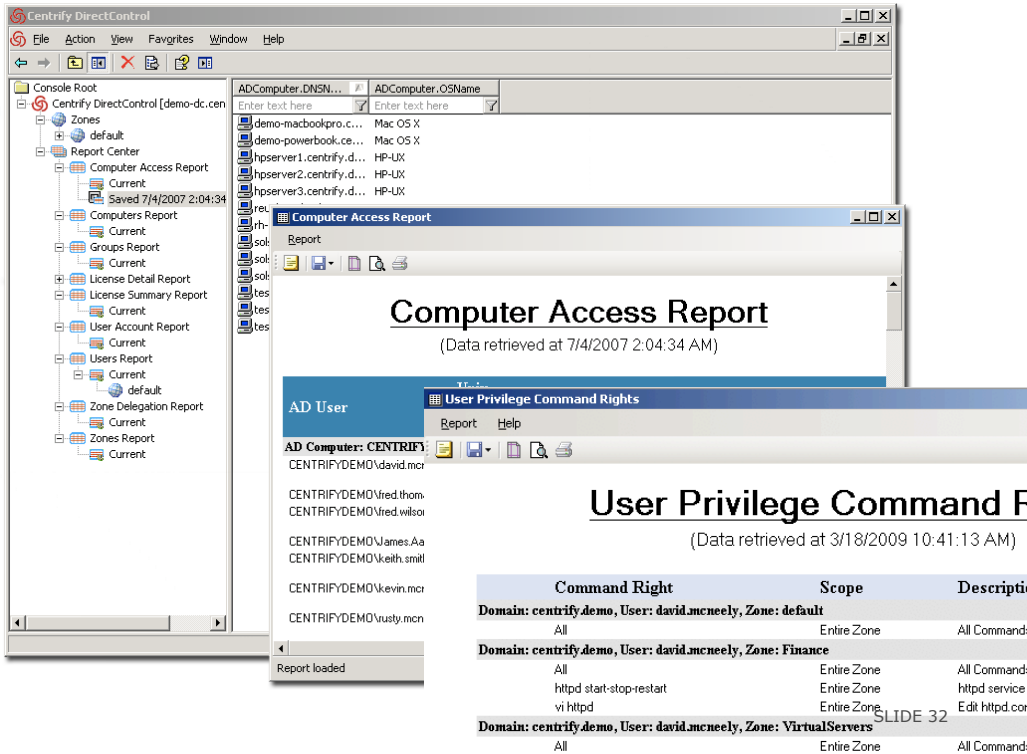
Reporting Simplified with Centralized Management

Authorization and Access Reports can be centrally created:

- Reporting on user account properties
- Detailing user role assignments and privilege command rights
- Showing user access rights to computers

Active Directory based reporting

- Reports are generated on live, editable AD information
- Administrators can take snapshots of a report



© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Addressing NIST 800-53 for UNIX

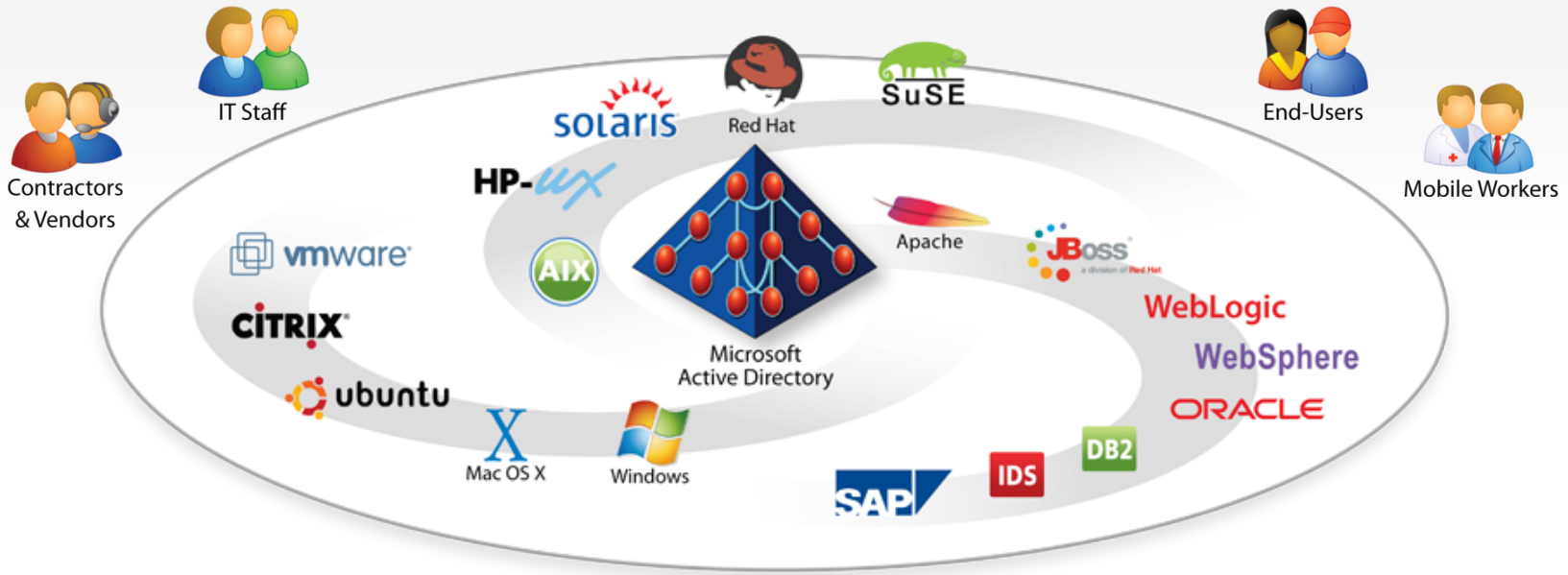
NIST SP 800-53 Requirement	Leverage Active Directory to:
Identity & Authentication (IA) • Uniquely identify and authenticate users • Employ multifactor authentication	• Link entitlements and actions to a centrally managed user identity in AD • Support smartcard authentication for Mac Workstations
Access Control (AC) • Restrict access to systems and to privileges • Enforce separation of duties and least-privilege rights management	• Enforce centralized policies for Role-based access and privilege rights • Enforce administrative separation of duties
Audit & Accountability (AU) • Capture in sufficient detail to establish what occurred, the source, and the outcome	• Capture all interactive sessions on audited systems, attributing the actions to the accountable person • Provide search and session replay
Configuration Management (CM) • Develop/maintain a baseline configuration • Automate enforcement for access restrictions and audit the actions	• Automatically enforce a baseline security policy • Continuously enforce/update the security policy
Systems & Communications (SC) • Boundary Protection • Transmission Integrity and Confidentiality • Cryptographic Key Establishment and Management including PKI Certificates	• Enforce domain and group-based isolation policies to protect sensitive assets • Encrypt data in motion between systems • Automate PKI management and validation on protected systems

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

The Centrify Vision

Control, Secure and Audit Access to Cross-Platform Systems and Applications

Centrify the Enterprise



Leverage infrastructure you already own – Active Directory – to:

Control	Secure	Audit
What users can access	User access and privileges	What the users did

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

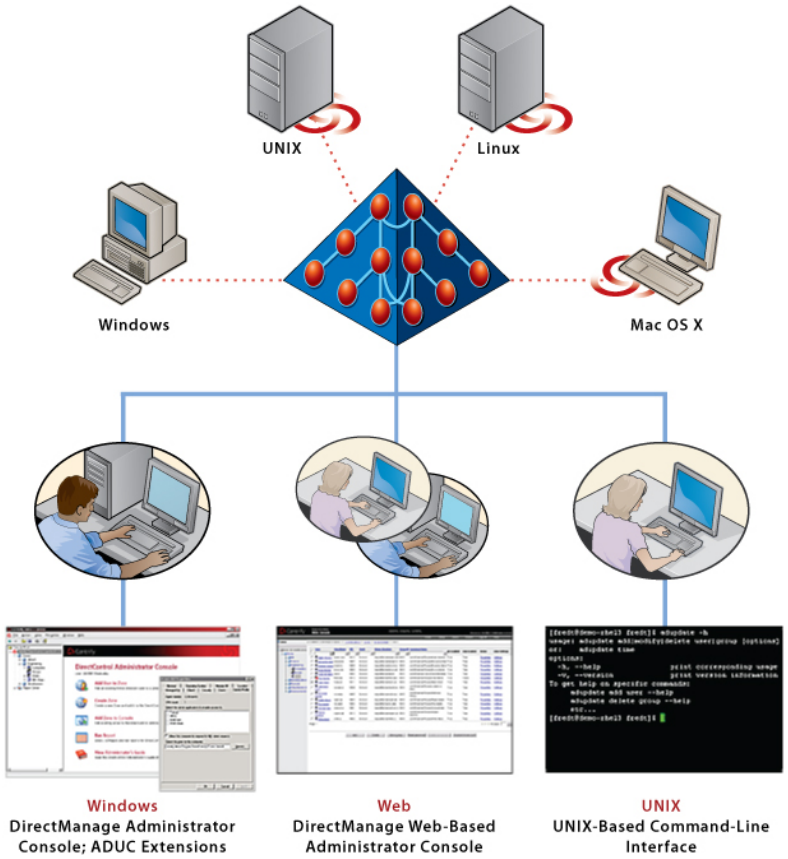
Reduce Costs Through Identity Consolidation

"Islands of identity" need to be managed and secured

- Locally managed etc/passwd file
- Legacy NIS or hand-built scripting
- High cost & inefficient to maintain

With Centrify:

- ✓ Consolidate disparate UNIX and Linux identity stores into AD
- ✓ Implement least-privilege security
- ✓ Centrally enforce security and configuration policies across UNIX, Linux and Mac systems
- ✓ Instantly terminate access to all systems and applications centrally



© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

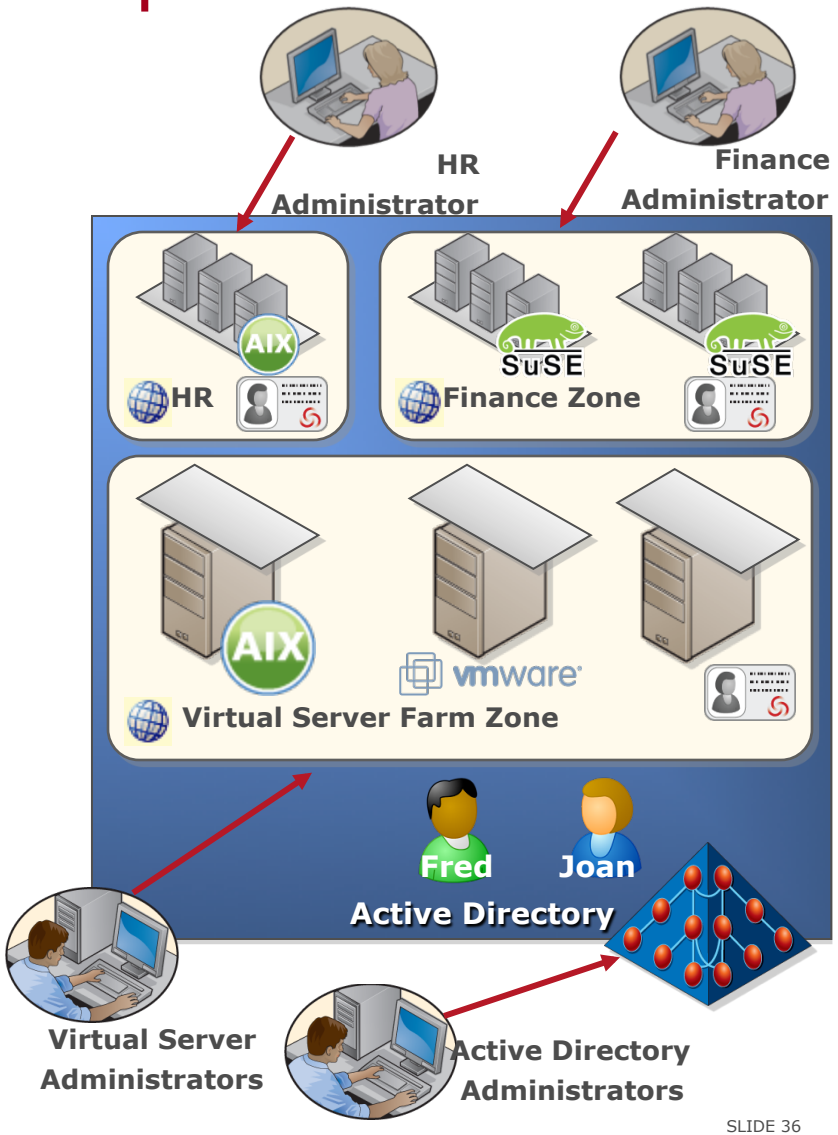
Mitigate Risks & Address Compliance

Evolving threat landscape and regulatory environment

- Shared "root" password compromises security & exposes intellectual property
- Anonymous access…
- Audits require reporting that ties access controls and activities to individuals

With Centrify:

- ✓ Associate privileges with individuals
- ✓ Lock down privileged accounts
- ✓ Enforce separation of duties
- ✓ Isolate sensitive systems
- ✓ Protect data-in-motion
- ✓ Audit all activity



© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Why Customers Choose Centrify

Gartner

Centrify is the "right vendor to choose" for Active Directory integration: Centrify's solution is "mature, technically strong, full featured, and possess(es) broad platform support." – 2009

"We recommended that clients strongly consider Centrify … its products can fit well within a multivendor IAM portfolio." – 2010

Experience & Expertise

- 3500+ enterprise customers
- Largest dedicated team
- Unparalleled 24x7 support
- Record growth and profitable

The Best Solution

- Single architecture based on AD
- Comprehensive suite
- Proven success in deployments
- Non-intrusive

Industry Awards

Industry Certifications

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED

Learn More and Evaluate Centrify Yourself

WEB SITE	**www.centrify.com**
FEDERAL SOLUTIONS	**www.centrify.com/federal**
TECHNICAL VIDEOS & MORE	**www.centrify.com/resources**
SUPPORTED PLATFORMS	**www.centrify.com/platforms**
REQUEST AN EVAL	**www.centrify.com/trial**
FREE SOFTWARE	**www.centrify.com/express**
CONTACT US	**www.centrify.com/contact**
PHONE	Worldwide: **+1 (408) 542-7500**
	Europe: **+44 (0) 1344 317950**

© 2004-2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED