P13 - Leveraging Active Directory to Secure and Audit Access to Non-Windows Systems

Presented by:
David McNeely, Sr. Director of Product Management
david.mcneely@centrify.com
Centrify Corporation
Trust Administrators but Verify Their Actions

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
Regulations Establish The Rules for IT

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

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
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
# Access Governance Starts with Centralization

Centralize Security Identity and Access Management within Active Directory

<table>
<thead>
<tr>
<th>Identity Consolidation</th>
<th>Privileged Access Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• De-duplicate identity infrastructure</td>
<td>• Associate privileges with individuals</td>
</tr>
<tr>
<td>• Get users to login as themselves / SSO</td>
<td>• Enforce “least access &amp; least privileges”</td>
</tr>
<tr>
<td>• Single security policy definition</td>
<td>• Audit privileged user activities</td>
</tr>
<tr>
<td>• Single point of administrative control</td>
<td>• Isolate systems &amp; encrypt data-in-motion</td>
</tr>
</tbody>
</table>

## Active Directory-based Security Infrastructure

- Users
- Groups
- Unix Profiles
- Security Policies
- User Roles

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
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
Solution is to Automate Security Enforcement

Leveraging Active Directory as the 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

Resulting in automated security for the Enterprise
Leverage Active Directory to Automate Security Enforcement

PROTECT SYSTEMS
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

Computer 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. SLIDE 10
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
Security Policies Auto-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
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
Leverage Active Directory to Automate Security Enforcement

AUTHORIZE PRIVILEGES
Active Directory Centralizes Account Management

- UNIX Account administration leverages centralized Active Directory processes and automation
- Account and authentication policies are enforced on all systems
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
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
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
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
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
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
Grant Privileged Commands to Roles

- Web Admins need root privileges to manage Apache Services
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/Department
- Users within a Role can be granted Rights to Computers serving a specific Role (DBA -> Oracle)
- 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 ~]$ dzinfo
Zone Status: DirectAuthorize is enabled
User: twilson
Forced into restricted environment: No

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Avail</th>
<th>Restricted Env</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Admin Role</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PAM Application</th>
<th>Avail</th>
<th>Source Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftpd</td>
<td>Yes</td>
<td>Web Admin Role</td>
</tr>
<tr>
<td>sshd</td>
<td>Yes</td>
<td>Web Admin Role</td>
</tr>
</tbody>
</table>

Privileged commands:

<table>
<thead>
<tr>
<th>Name</th>
<th>Avail Command</th>
<th>Source Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>vi</td>
<td>Yes</td>
<td>/etc/httpd/conf/* Web Admin Role</td>
</tr>
<tr>
<td>httpd</td>
<td>Yes</td>
<td>service http* Web Admin Role</td>
</tr>
<tr>
<td>start-stop-rest art</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
```

© 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

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

Security Log (/var/log/secure)

```plaintext
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
```
Leverage Active Directory to Automate Security Enforcement

AUDIT ACTIVITIES
System Logs and Events Provide 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?

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

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

I want to see all failed login attempts.

Are there any newly created local accounts on my server?

Who zone-enabled this user?
For Monitoring and Reporting of Logged Changes

- Employees
  - Added member(s) to this group about a minute ago by TANGO
  - Employees
    - AD Group: Employees
    - Group Scope: Global
    - Group Type: Distribution
    - Mail: employees@tango.se
  - Affected Members
    - tango.se/Users/Alpha
    - tango.se/Users/Bravo
    - tango.se/Users/Charlie

- twamley
  - Updated 5 minutes ago by TANGO/Administrator
  - tango.se/Program Data/Centrify/Zones/DMZ/Users/twamley
  - tango.se/Users/David Twamley
  - Centrify Zone: DMZ
    - UNIX User: twamley
    - UID: 10001
    - Shell: /bin/bash
    - Home: /home/twamley
    - GID: 10000
    - Enabled: True
    - When Created: 01:53:28 am, Tue 03/29/2011

© 2004-2011. CENTRIFY CORPORATION. ALL RIGHTS RESERVED.
High Definition Visibility Provided by Session Recording

- Establish User accountability
- Tracks all user access to systems
- Centrally search captured sessions
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
Centrify’s Vision
Control, Secure and Audit Access to Cross-Platform Systems and Applications

Centrify the Enterprise

Leverage infrastructure you already own – Active Directory – to:

Control
What users can access

Secure
User access and privileges

Audit
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
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
Why Customers Choose Centrify

*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

<table>
<thead>
<tr>
<th>Experience &amp; Expertise</th>
<th>The Best Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 3500+ enterprise customers</td>
<td>• Single architecture based on AD</td>
</tr>
<tr>
<td>• Largest dedicated team</td>
<td>• Comprehensive suite</td>
</tr>
<tr>
<td>• Unparalleled 24x7 support</td>
<td>• Proven success in deployments</td>
</tr>
<tr>
<td>• Record growth and profitable</td>
<td>• Non-intrusive</td>
</tr>
</tbody>
</table>

Industry Awards

![Industry Awards Images](image1.png)

Industry Certifications

![Industry Certifications Images](image2.png)
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