Black Hat: Active Directory Delegation Dissected

Securing Centrify’s Active Directory Delegations

Robertson Pimentel, CISM, CISSP
Product Manager
Contents

• Why should you mature your Identity and Access Management practice?
• Centrify best practices for IAM
• Centrify platform
• Infrastructure Services (Server Suite and Privilege Service)
• Basics: Centrify Zones
• Active Directory Delegations
• Finding out
  • Who has delegated rights?
  • Who has used their delegated rights?
• 3 tips to secure your Centrify AD delegations
Why invest in Identity and Access Management?

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

80% of breaches involve privileged credential misuse.

Usage of stolen credentials as attack vector per threat agent motivation category (espionage, fun-ideology-grudge, financial/organized crime):

ESP: 27
FIG: 6
FIN: 598

50% less breaches
$5 MIL in cost savings
40% less on technology costs

© 2018 Centrify Corporation. All Rights Reserved.
CENTRIFY ZERO TRUST SECURITY:
UNIFIED NEXT-GEN ACCESS

SECURES ACCESS TO APPS FROM TRUSTED ENDPOINTS
SECURES ACCESS TO INFRASTRUCTURE

APPLICATION SERVICES
ENDPOINT SERVICES
INFRASTRUCTURE SERVICES
Infrastructure Services Consists

Privilege Elevation Service

- Active Directory Bridging: UNIX, Linux, OS X.
- Role-based Access Control: Windows, UNIX, Linux.
- Session Capture and Replay: Windows, UNIX, Linux.
- Optimized for Active Directory as the identity source.

Privilege Access Service

- Shared Account Password Management
- Secure Access (PSM, Jumpbox, etc.)
- Machine-to-Machine communications
- Optimized to leverage the Centrify Identity Platform.
- Identities Supported:
Centrify Zones

- Centrify Zones are Active Directory objects.
- Centrify Zones store UNIX identity information (unlike workstation/express mode).
- Centrify Zones support multiple schemas (SFU, RFC2307, Centrify).
- Zones allow the implementation of Access Control and Privilege Management rules across Windows, UNIX and Linux platforms.
- Zones contain also configuration information like Local users, NIS Maps, Multi-factor Authentication.
- Zones are administered with Active Directory tools and administrative tasks can be delegated to zones and child objects.
- Delegation is important in the context of Separation of Duties (SoD) or distributed administration.

There is no Centrify “server” the server is Active Directory.
Delegations in Centrify Infrastructure Service (formerly CSS)

- Centrify Access Manager [dc.centrify.vms]
- Zones
- Create Child Zone...
- Prepare UNIX Computer...
- Prepare Windows Computer...
- Delegate Zone Control...
- Change Master Domain Controller...

Active Directory

- RBAC (PAM) operations
  - Manage roles and rights
  - Modify computer roles
  - Create machine overrides and computer roles
  - Remove machine overrides and computer roles
  - Manage role assignments in zone, computer role...

- Override operations
  - Add users
  - Add groups
  - Add local users
  - Add local groups
  - Join computers to the zone
  - Remove zones
  - Remove users
  - Remove groups
  - Import users and groups to zone

- NIS map operations
  - Add or remove NIS map entries
  - Modify NIS map entries
  - Create NIS maps
  - Remove NIS maps
Leverage the Centrify Recommended OU Structure

- The Centrify Recommended OU structure eliminates the need for complex delegation.
- The OU Structure creates:
  - Authorization Managers: Can perform with RBAC functions.
  - Centrify Admins: Have full control over the OU structure.
  - Computer Managements: Can perform computer fulfillment operations.
  - Data Managers: Can perform UNIX identity (and NIS) operations.
- You can leverage your change control and JIT capabilities (see tips).
Who has delegated rights in Active Directory related to Centrify?

2017.3 and up: Effective Delegation Report (Report Services)

<table>
<thead>
<tr>
<th>AD User</th>
<th>Scope</th>
<th>Target</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:Administrator@centrify.vms">Administrator@centrify.vms</a></td>
<td>Windows Computer</td>
<td>win10.centrify.vms</td>
<td>[Windows Computer] Remove computer from zone</td>
</tr>
<tr>
<td></td>
<td>Computer Role</td>
<td>UNIX1 (Console Only)</td>
<td>[Computer Role] Manage role assignments</td>
</tr>
<tr>
<td></td>
<td>Computer Role</td>
<td>UNIX1 (Console Only)</td>
<td>[Computer Role] Modify computer role</td>
</tr>
<tr>
<td></td>
<td>Computer Role</td>
<td>UNIX1 (Console Only)</td>
<td>[Computer Role] Remove computer role</td>
</tr>
<tr>
<td></td>
<td>Computer Role</td>
<td>UNIX2 (Terminal)</td>
<td>[Computer Role] Manage role assignments</td>
</tr>
<tr>
<td></td>
<td>Computer Role</td>
<td>UNIX2 (Terminal)</td>
<td>[Computer Role] Modify computer role</td>
</tr>
<tr>
<td></td>
<td>Computer Role</td>
<td>UNIX2 (Terminal)</td>
<td>[Computer Role] Remove computer role</td>
</tr>
<tr>
<td><a href="mailto:bootcamp.admin@centrify.vms">bootcamp.admin@centrify.vms</a></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Add groups</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Add local groups</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Add local users</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Add users</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Allow computers to respond to NIS client requests</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Change zone properties</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Create NIS maps</td>
</tr>
<tr>
<td></td>
<td>Zone</td>
<td>AutoProw</td>
<td>[Zone] Join computers to the zone</td>
</tr>
</tbody>
</table>
Who has used their Centrify delegated rights?

- Centrify Auditing and Monitoring Service (DirectAudit): provides reports and captured sessions.
- Centrify App for Splunk™ provides Admin activity dashboard.
Design Tips to Protect Accounts with Centrify Delegation
Tip # 1 Protect your ZPA Service (fulfillment)

- Use the least privilege principle.
  - Don’t make the ZPA account a high-privileged account by granting “All Rights.”
    - It only needs “run as a service” in the target system.
    - It only needs add/remove/modify to the target objects provisioned (users/groups).
  - Leverage PAS to secure ZPA
    - Use System Discovery to identify systems running ZPA.
    - Rotate the service password based on policy.
    - Establish a maintenance window.
    - Monitor the service as needed.
Tip # 2: Practice Responsible Windows Administration

• Perform your Windows administration from a “secure workstation.”
  • Clean sourced. Current OS. Patched.
  • Does not allow internet or email access.
  • Ideally it’s “recycled” (e.g. rebuilt frequently).
  • Establish Identity Assurance (MFA, step-up).

• Do not grant permanent ownership (account) or membership (groups) that have delegated administration. Techniques:
  • Allow users to elevate to the groups that have these delegations using token manipulation (no hash!).
  • If shared account, ideally it’s a secure account (e.g. in your RED forest) and subject to aggressive password rotation.
  • Request Active Directory membership on demand.
  • Use Session Capture.
Tip # 3 – Monitor and Record (enrich Security operations)
LEADERSHIP: PIM, IDAAS, EMM

LEADER FORRESTER PIM WAVE

LEADER FORRESTER IDAAS WAVE

STRONG PERFORMER FORRESTER EMM WAVE

LEADER GARTNER IDAAS MQ

PC MAGAZINE EDITOR'S CHOICE

NETWORK WORLD CLEAR CHOICE WINNER
Thank You