Centrify®

ZERO TRUST SECURITY

Black Hat:
Active Directory
Delegation Dissected

Securing Centrify’s Active Directory Delegations

Robertson Pimentel, CISM, CISSP

Product Manager

Contents

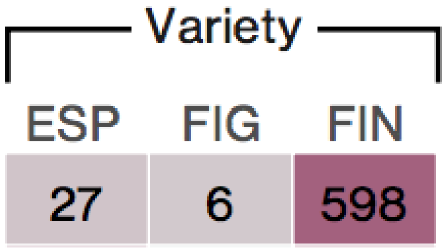
- Why should you mature your Identity and Access Management practice?
- Centrify best practices for IAM
- Centrify platform
- Infrastructure Services (Server Suite and Privilege Service)
- Basics: Centrify Zones
- Active Directory Delegations
- Finding out
  - Who has delegated rights?
  - Who has used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

Why invest in Identity and Access Management?

verizon

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

80%
of breaches involve privileged credential misuse



Variety		
ESP	FIG	FIN
27	6	598

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

IAM

FORRESTER

Stop The Breach: Reduce The Likelihood Of An Attack Through An IAM Maturity Model

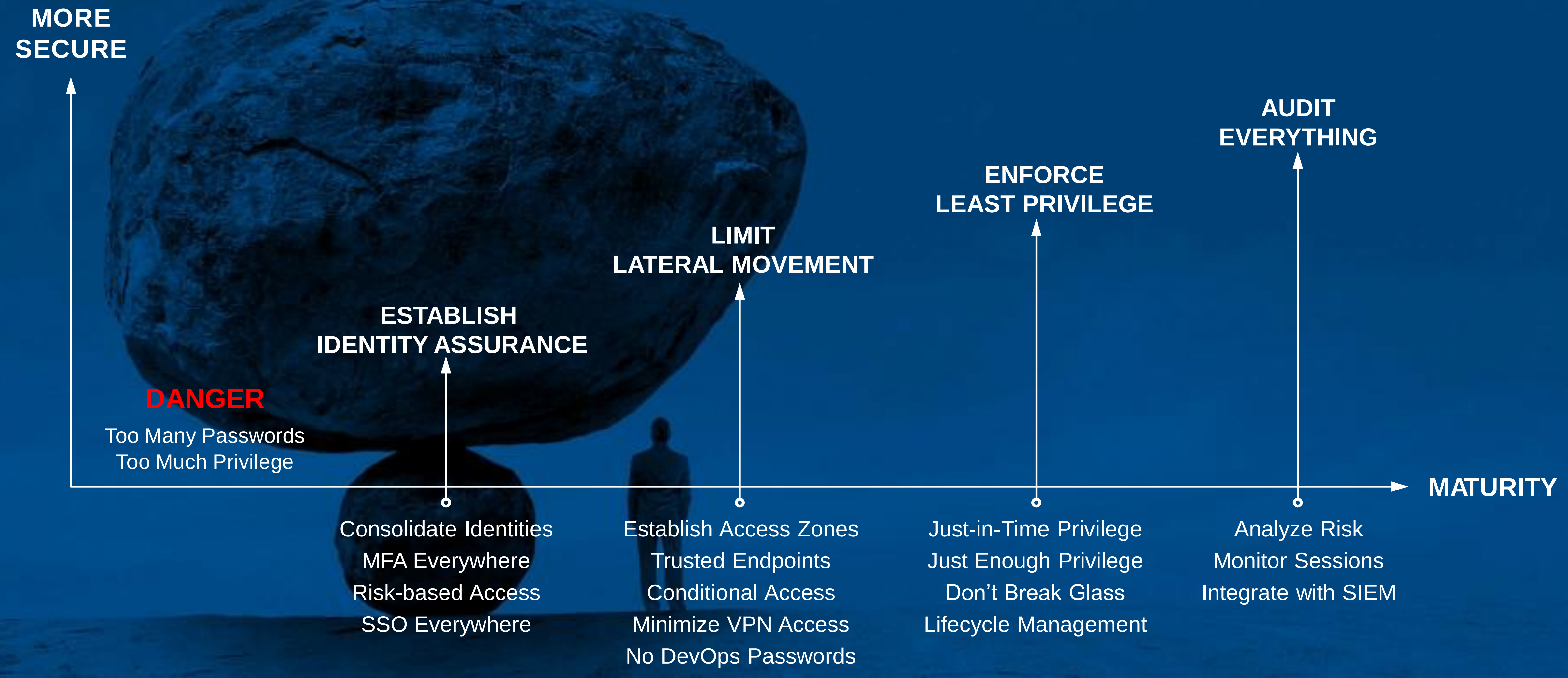
50% less breaches

$5 MIL in cost savings

40% less on technology costs

Centrify
ZERO TRUST SECURITY

BEST PRACTICES IAM MATURITY



MORE SECURE

MATURITY

DANGER

Too Many Passwords
Too Much Privilege

ESTABLISH IDENTITY ASSURANCE

Consolidate Identities
MFA Everywhere
Risk-based Access
SSO Everywhere

LIMIT LATERAL MOVEMENT

Establish Access Zones
Trusted Endpoints
Conditional Access
Minimize VPN Access
No DevOps Passwords

ENFORCE LEAST PRIVILEGE

Just-in-Time Privilege
Just Enough Privilege
Don’t Break Glass
Lifecycle Management

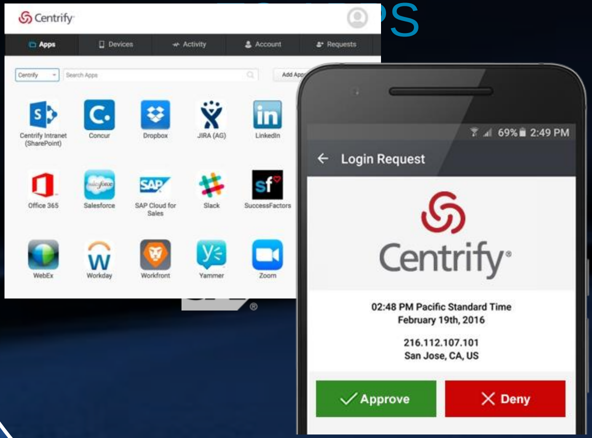
AUDIT EVERYTHING

Analyze Risk
Monitor Sessions
Integrate with SIEM

CENTRIFY ZERO TRUST SECURITY:

UNIFIED NEXT-GEN ACCESS

SECURES ACCESS



69% 2:49 PM

Login Request

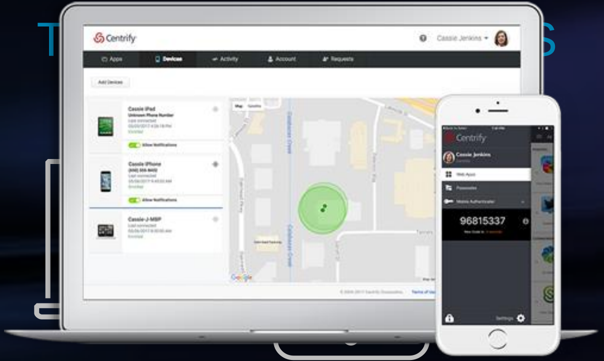
Centrify

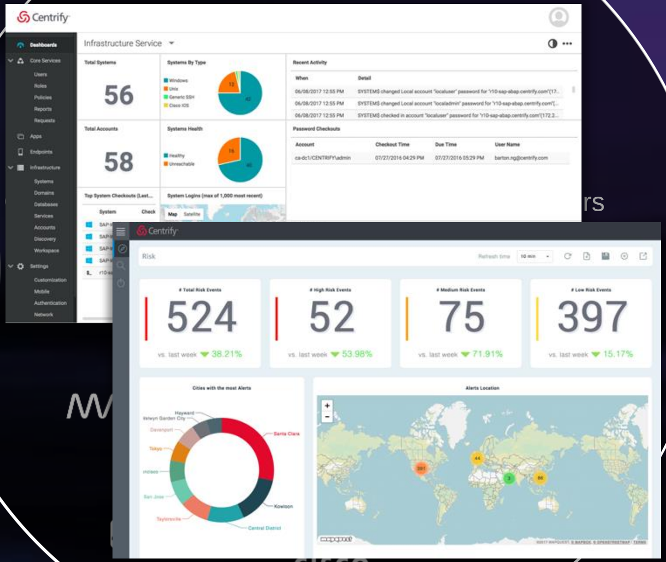
02:48 PM Pacific Standard Time
February 19th, 2016

216.112.107.101
San Jose, CA, US

Approve Deny

FROM





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.

Active Directory

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:

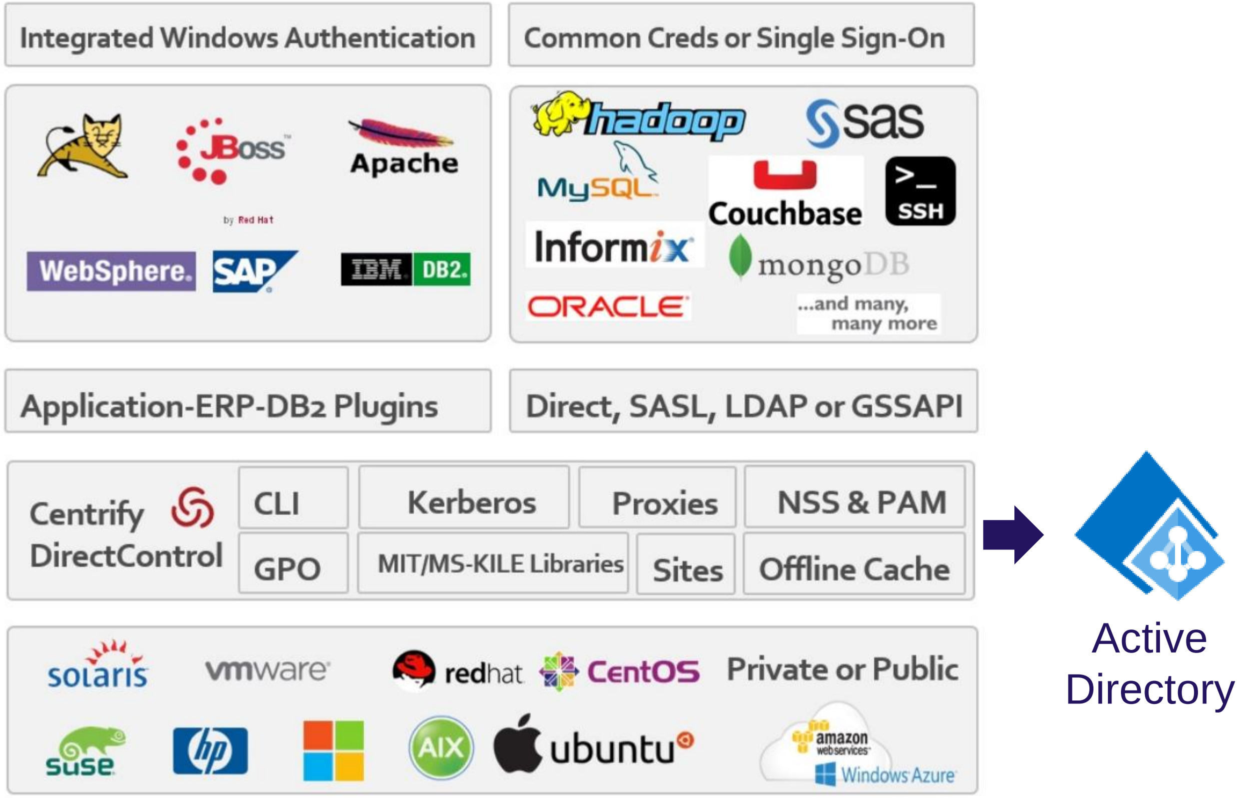
Active Directory

LDAP

Centrify

Google My Business

Centrify Zones



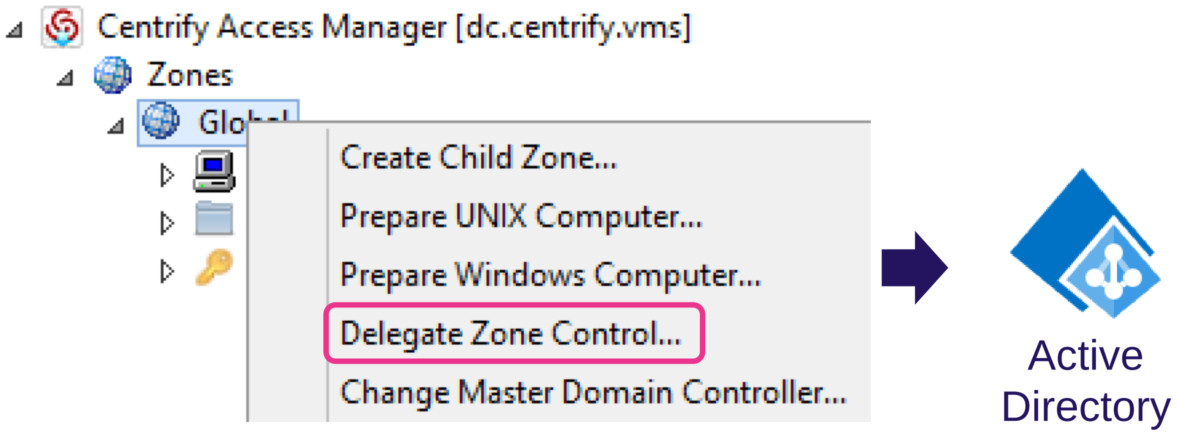
There is no Centrify "server" the server is Active Directory.

Zones 101

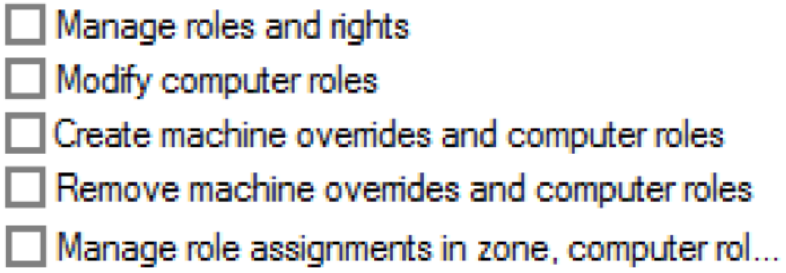
- Centrify Zones are Active Directory objects.
- Centrify Zones store UNIX identity. information (unlike workstation/express mode).
- Centrify Zones support multiple schemas (SFU, RFC2307, Centrify).
- Zones allow the implementation of Access Control and Privilege Management rules across Windows, UNIX 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.

Centrify
ZERO TRUST SECURITY

Delegations in Centrify Infrastructure Service (formerly CSS)

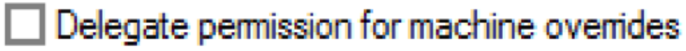

Centrify Access Manager [dc.centrify.vms]
Zones
Glo
Create Child Zone...
Prepare UNIX Computer...
Prepare Windows Computer...
Delegate Zone Control...
Change Master Domain Controller...
Active Directory

RBAC (PAM) operations



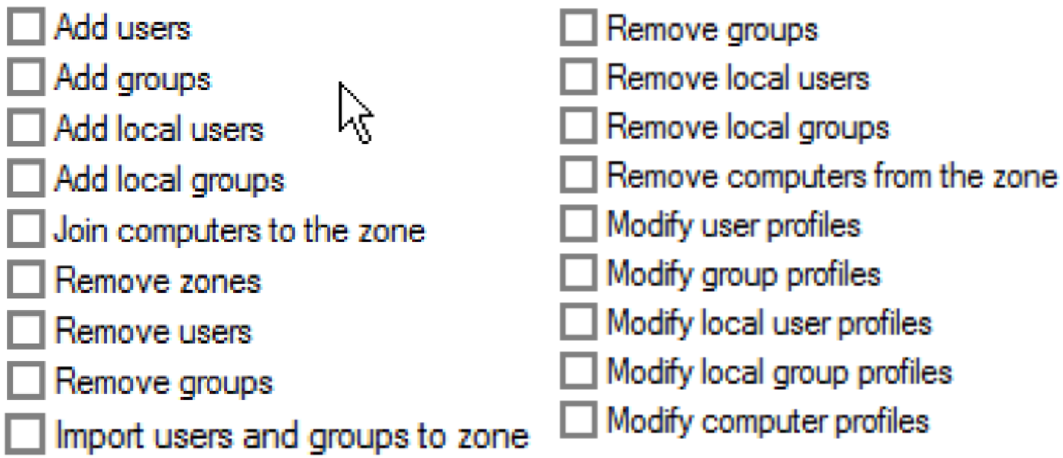
- □ Manage roles and rights
- □ Modify computer roles
- □ Create machine overrides and computer roles
- □ Remove machine overrides and computer roles
- □ Manage role assignments in zone, computer rol...

special (delegation) operations



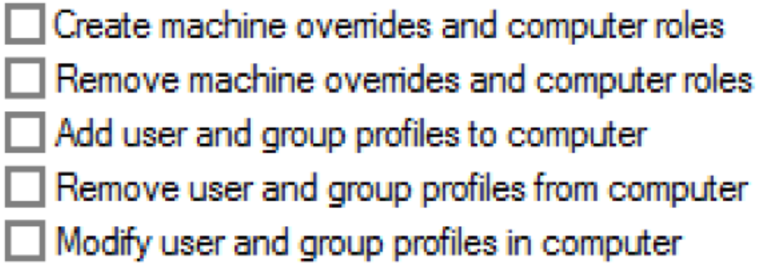
- □ Delegate permission for machine overrides

fulfillment operations (typically ZPA)



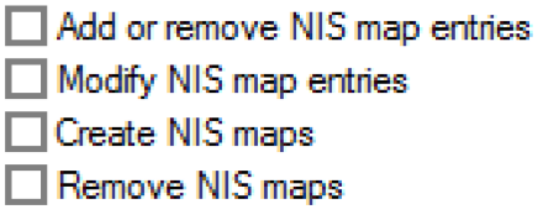
- □ Add users
- □ Add groups
- □ Add local users
- □ Add local groups
- □ Join computers to the zone
- □ Remove zones
- □ Remove users
- □ Remove groups
- □ Import users and groups to zone
- □ Remove groups
- □ Remove local users
- □ Remove local groups
- □ Remove computers from the zone
- □ Modify user profiles
- □ Modify group profiles
- □ Modify local user profiles
- □ Modify local group profiles
- □ Modify computer profiles

override operations



- □ Create machine overrides and computer roles
- □ Remove machine overrides and computer roles
- □ Add user and group profiles to computer
- □ Remove user and group profiles from computer
- □ Modify user and group profiles in computer

NIS map operations

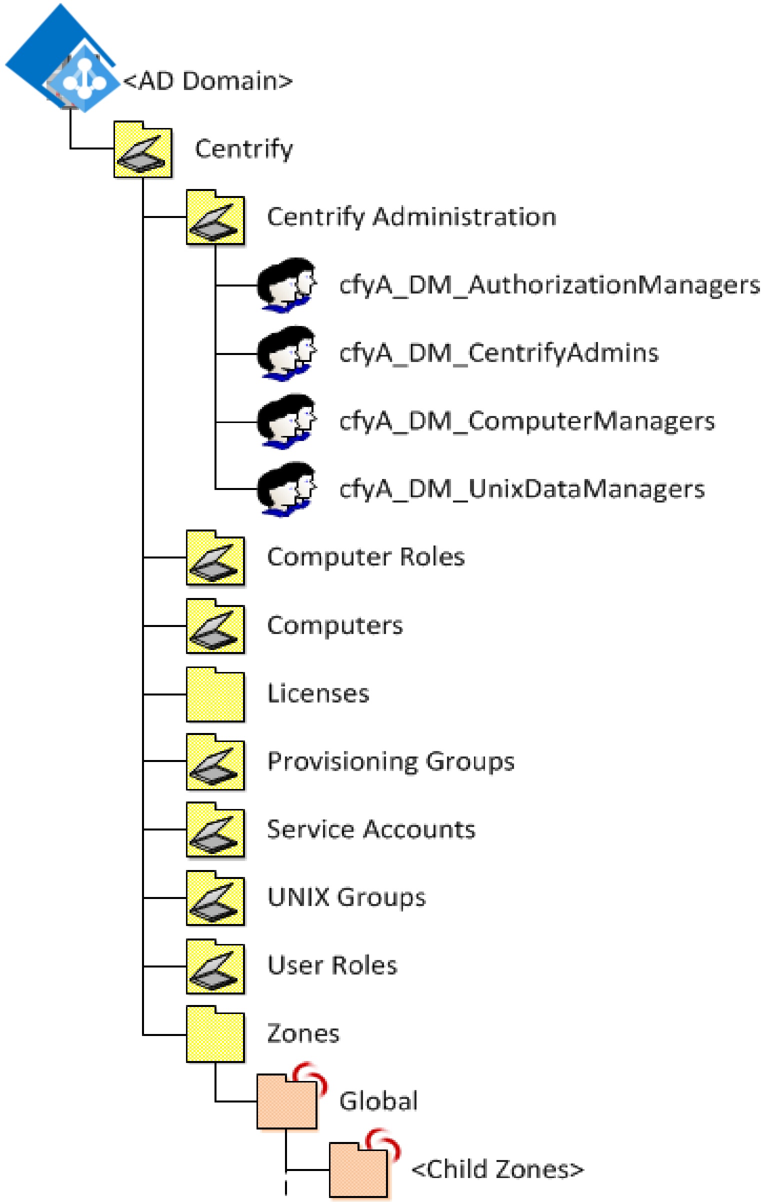


- □ Add or remove NIS map entries
- □ Modify NIS map entries
- □ Create NIS maps
- □ Remove NIS maps

Centrify
ZERO TRUST SECURITY

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).

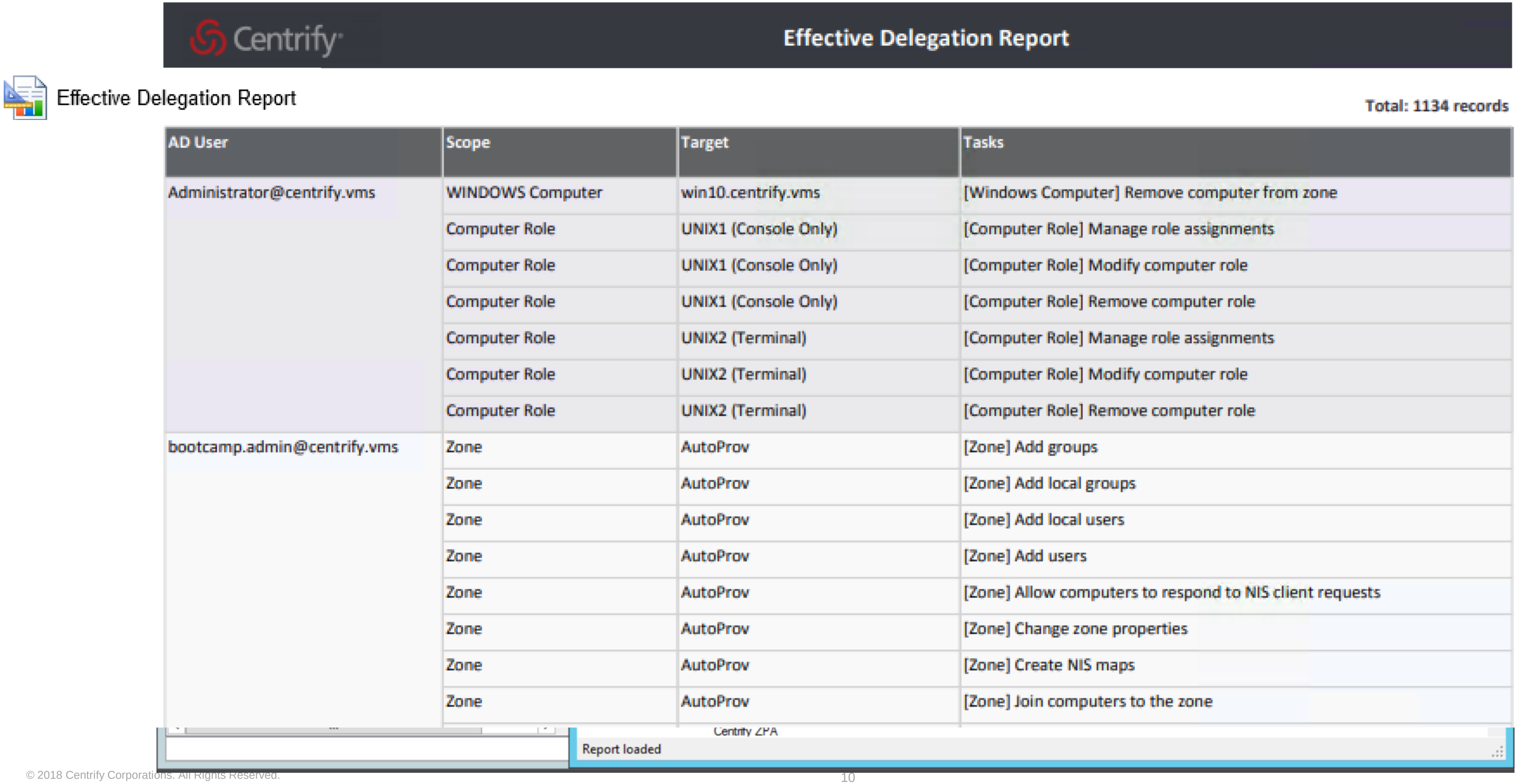


- <AD Domain>
  - Centrify
    - Centrify Administration
      - cfyA_DM_AuthorizationManagers
      - cfyA_DM_CentrifyAdmins
      - cfyA_DM_ComputerManagers
      - cfyA_DM_UnixDataManagers
    - Computer Roles
    - Computers
    - Licenses
    - Provisioning Groups
    - Service Accounts
    - UNIX Groups
    - User Roles
    - Zones
      - Global
        - <Child Zones>

Who has delegated rights in Active Directory related to Centrify?

2017.3 and up: Effective Delegation Report (Report Services)

Pre-2018: Zone Delegation Report



Effective Delegation Report

Effective Delegation Report

Total: 1134 records

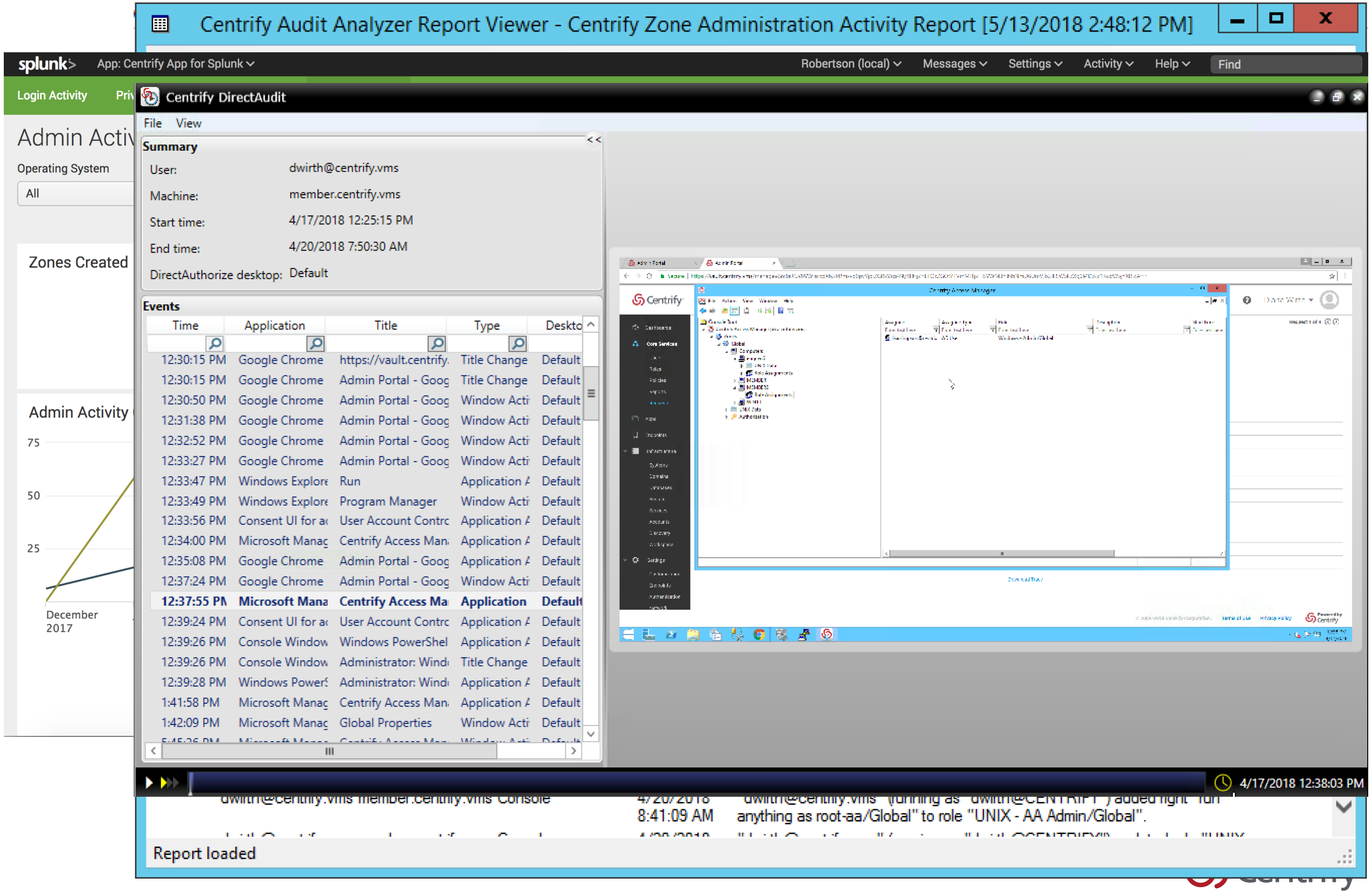
AD User	Scope	Target	Tasks
Administrator@centrify.vms	WINDOWS Computer	win10.centrify.vms	[Windows Computer] Remove computer from zone
	Computer Role	UNIX1 (Console Only)	[Computer Role] Manage role assignments
	Computer Role	UNIX1 (Console Only)	[Computer Role] Modify computer role
	Computer Role	UNIX1 (Console Only)	[Computer Role] Remove computer role
	Computer Role	UNIX2 (Terminal)	[Computer Role] Manage role assignments
	Computer Role	UNIX2 (Terminal)	[Computer Role] Modify computer role
	Computer Role	UNIX2 (Terminal)	[Computer Role] Remove computer role
bootcamp.admin@centrify.vms	Zone	AutoProv	[Zone] Add groups
	Zone	AutoProv	[Zone] Add local groups
	Zone	AutoProv	[Zone] Add local users
	Zone	AutoProv	[Zone] Add users
	Zone	AutoProv	[Zone] Allow computers to respond to NIS client requests
	Zone	AutoProv	[Zone] Change zone properties
	Zone	AutoProv	[Zone] Create NIS maps
	Zone	AutoProv	[Zone] Join computers to the zone

Report loaded

Who has used their Centrify delegated rights?

Centrify

- Centrify Auditing and Monitoring Service (DirectAudit): provides reports and captured sessions.
- Centrify App for Splunk™ provides Admin activity dashboard.



Summary

User: dwirth@centrify.vms

Machine: member.centrify.vms

Start time: 4/17/2018 12:25:15 PM

End time: 4/20/2018 7:50:30 AM

DirectAuthorize desktop: Default

Events

Time	Application	Title	Type	Deskto
12:30:15 PM	Google Chrome	https://vault.centrify.	Title Change	Default
12:30:15 PM	Google Chrome	Admin Portal - Goog	Title Change	Default
12:30:50 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:31:38 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:32:52 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:33:27 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:33:47 PM	Windows Explore	Run	Application A	Default
12:33:49 PM	Windows Explore	Program Manager	Window Acti	Default
12:33:56 PM	Consent UI for ac	User Account Contrc	Application A	Default
12:34:00 PM	Microsoft Manag	Centrify Access Man.	Application A	Default
12:35:08 PM	Google Chrome	Admin Portal - Goog	Application A	Default
12:37:24 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:37:55 PM	**Microsoft Mana**	**Centrify Access Ma**	**Application**	**Default**
12:39:24 PM	Consent UI for ac	User Account Contrc	Application A	Default
12:39:26 PM	Console Window	Windows PowerShel	Application A	Default
12:39:26 PM	Console Window	Administrator: Wind	Title Change	Default
12:39:28 PM	Windows PowerS	Administrator: Wind	Application A	Default
1:41:58 PM	Microsoft Manag	Centrify Access Man.	Application A	Default
1:42:09 PM	Microsoft Manag	Global Properties	Window Acti	Default

4/17/2018 12:38:03 PM

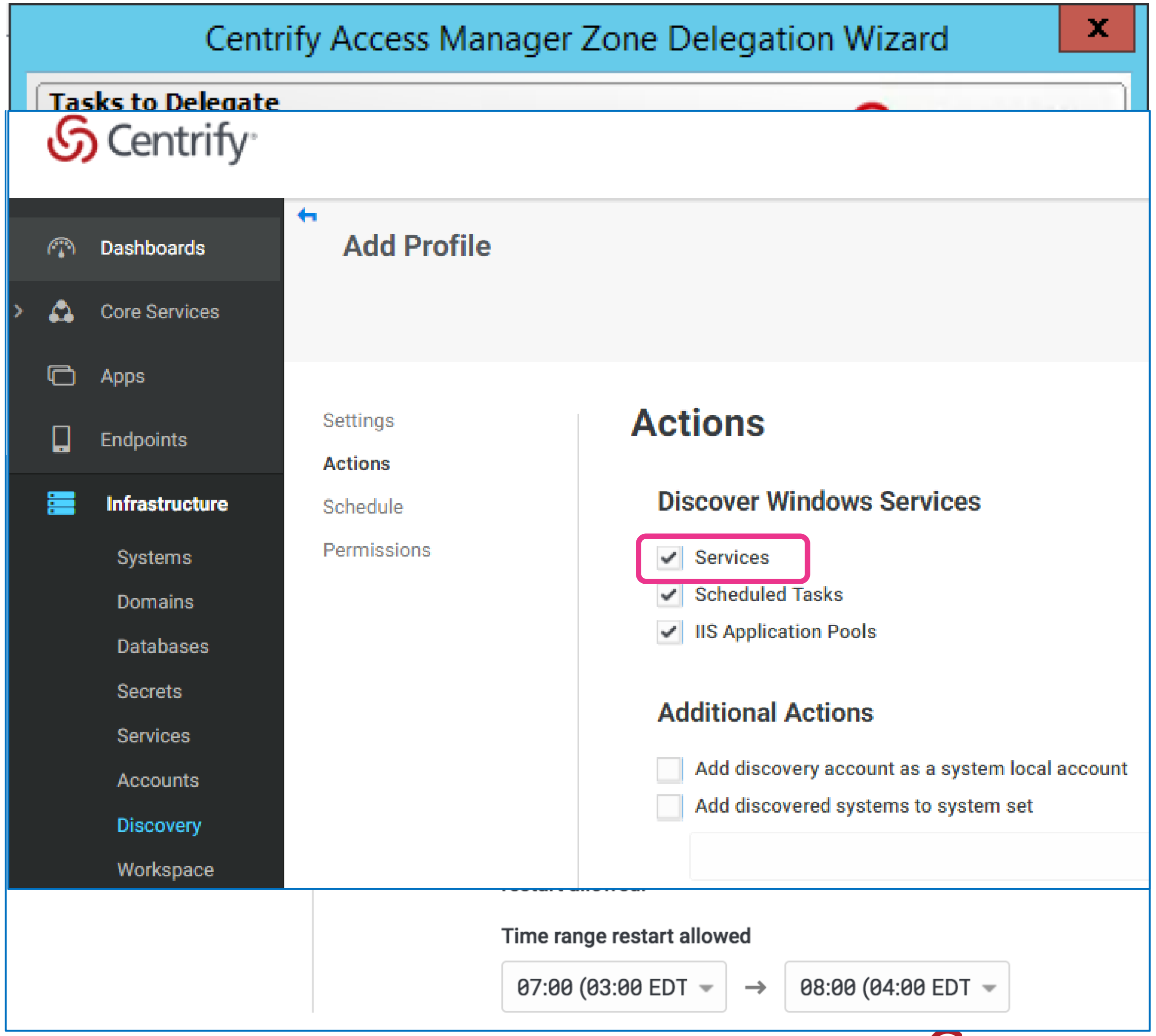
dwirth@centrify.vms member.centrify.vms Console 4/20/2018 8:41:09 AM dwirth@centrify.vms (running as dwirth@CENTRIFY) added right "run anything as root-aa/Global" to role "UNIX - AA Admin/Global".

Report loaded

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.



Centrify Access Manager Zone Delegation Wizard

Tasks to Delegate

Add Profile

Actions

Discover Windows Services

☑ Services

☑ Scheduled Tasks

☑ IIS Application Pools

Additional Actions

□ Add discovery account as a system local account

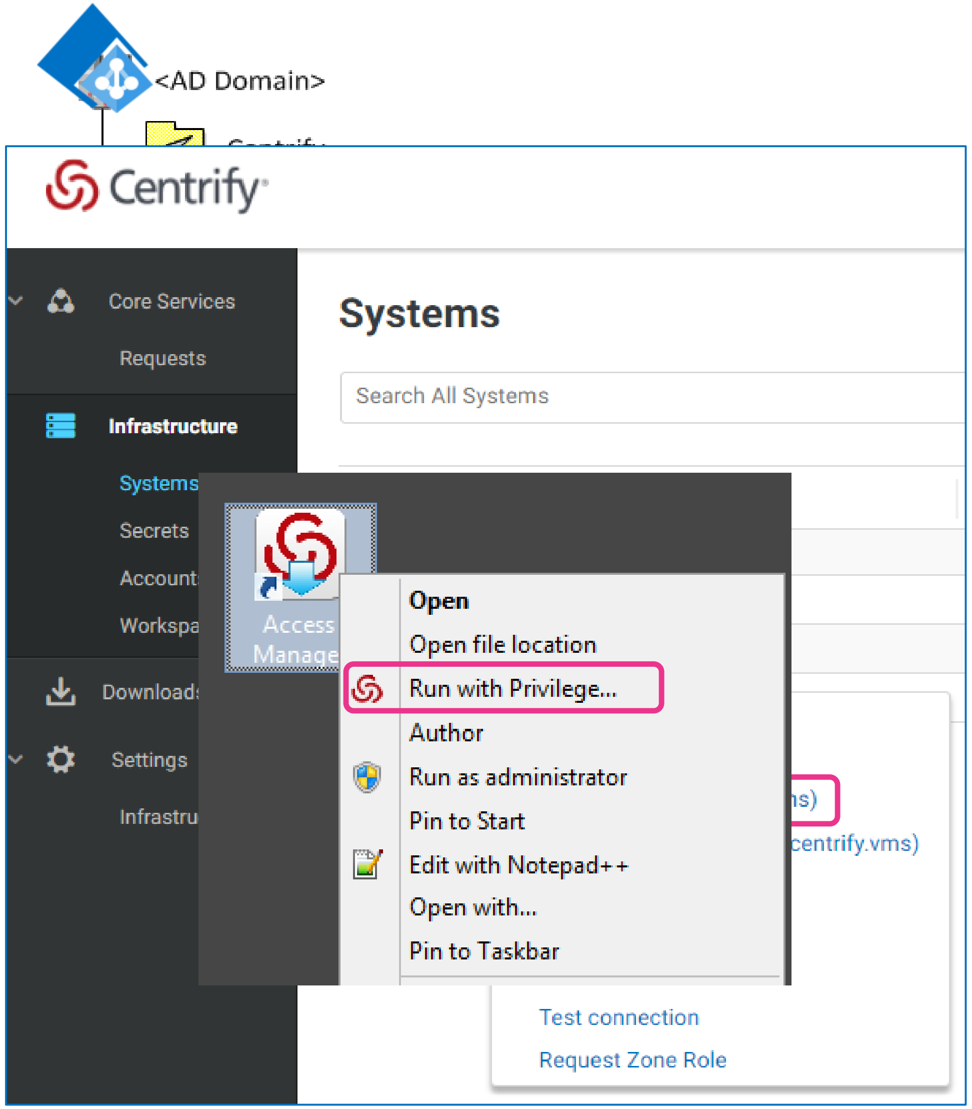
□ Add discovered systems to system set

Time range restart allowed

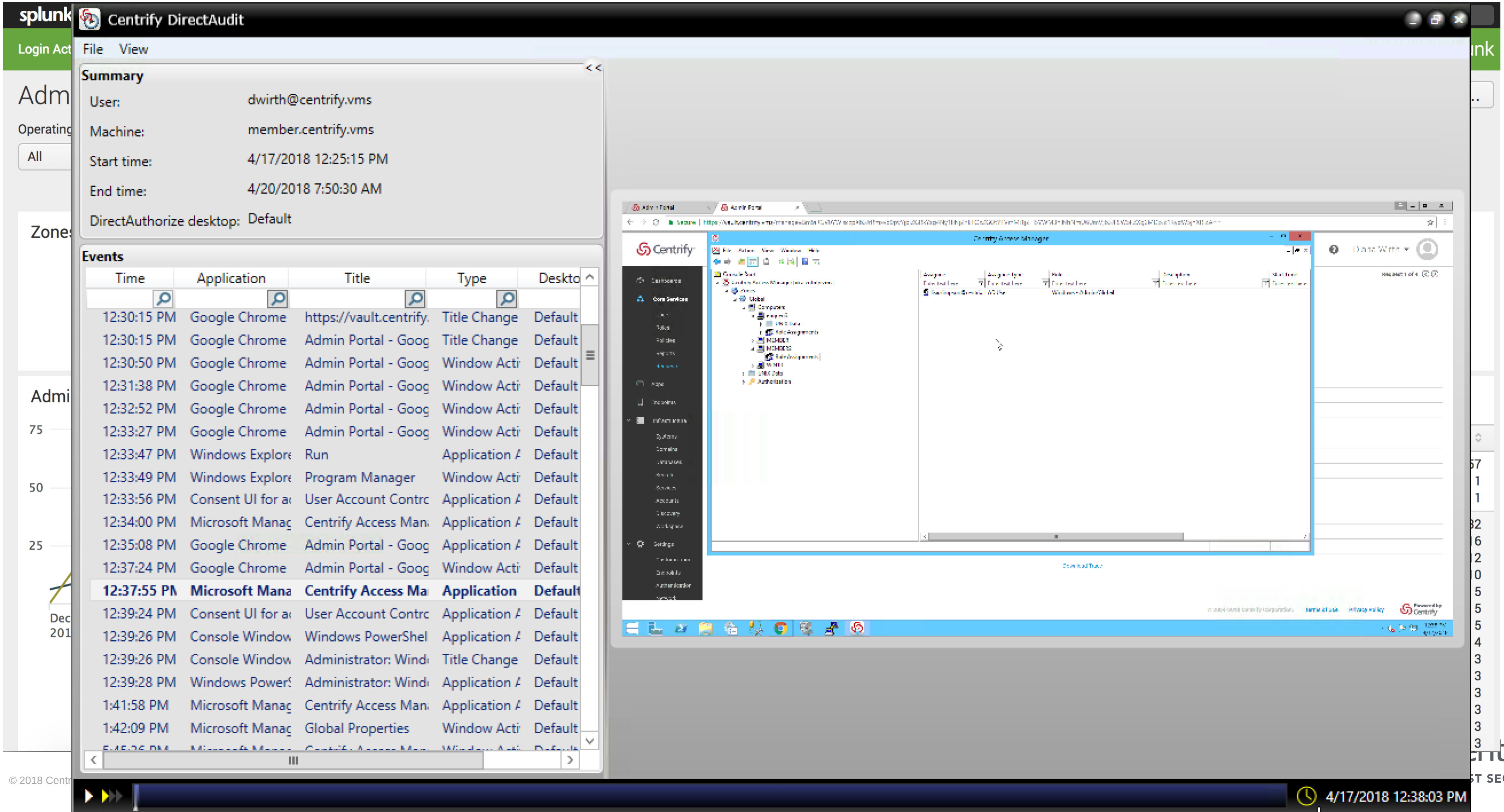
07:00 (03:00 EDT → 08:00 (04:00 EDT

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)



Summary

User: dwirth@centrify.vms

Machine: member.centrify.vms

Start time: 4/17/2018 12:25:15 PM

End time: 4/20/2018 7:50:30 AM

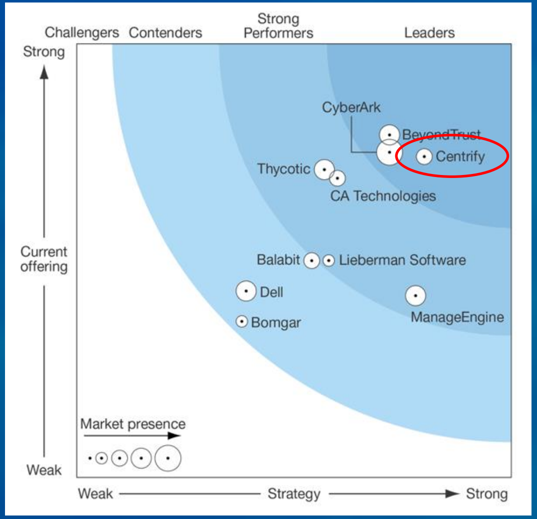
DirectAuthorize desktop: Default

Events

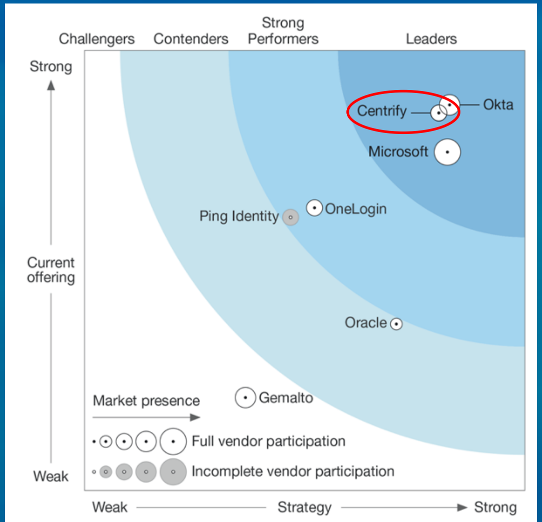
Time	Application	Title	Type	Deskto
12:30:15 PM	Google Chrome	https://vault.centrify.	Title Change	Default
12:30:15 PM	Google Chrome	Admin Portal - Goog	Title Change	Default
12:30:50 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:31:38 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:32:52 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:33:27 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:33:47 PM	Windows Explore	Run	Application A	Default
12:33:49 PM	Windows Explore	Program Manager	Window Acti	Default
12:33:56 PM	Consent UI for a	User Account Contro	Application A	Default
12:34:00 PM	Microsoft Manag	Centrify Access Man	Application A	Default
12:35:08 PM	Google Chrome	Admin Portal - Goog	Application A	Default
12:37:24 PM	Google Chrome	Admin Portal - Goog	Window Acti	Default
12:37:55 PM	**Microsoft Mana**	**Centrify Access Ma**	**Application**	**Default**
12:39:24 PM	Consent UI for a	User Account Contro	Application A	Default
12:39:26 PM	Console Window	Windows PowerShel	Application A	Default
12:39:26 PM	Console Window	Administrator: Windo	Title Change	Default
12:39:28 PM	Windows Powers	Administrator: Windo	Application A	Default
1:41:58 PM	Microsoft Manag	Centrify Access Man	Application A	Default
1:42:09 PM	Microsoft Manag	Global Properties	Window Acti	Default

LEADERSHIP: PIM, IDAAS, EMM

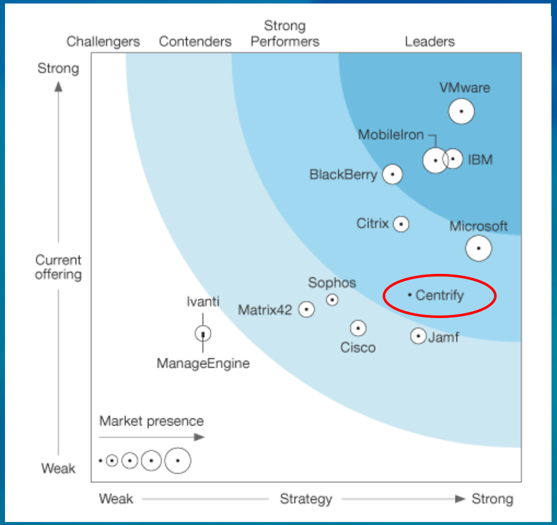
LEADER FORRESTER PIM WAVE



LEADER FORRESTER IDAAS WAVE

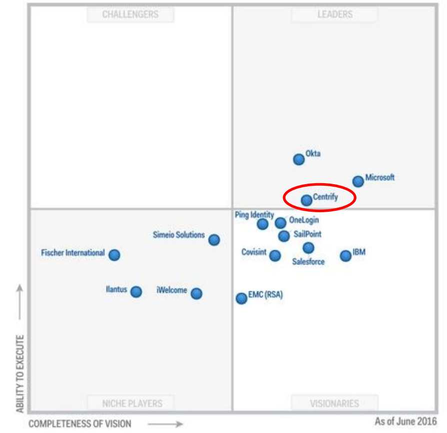


STRONG PERFORMER FORRESTER EMM WAVE



LEADER GARTNER IDAAS MQ

Figure 1. Magic Quadrant for Identity and Access Management as a Service, Worldwide



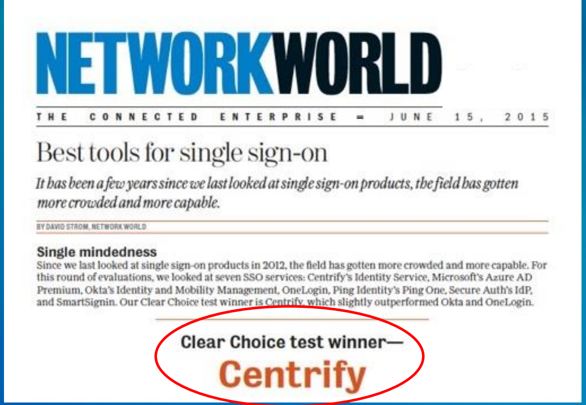
Source: Gartner (June 2016)

PC MAGAZINE EDITOR'S CHOICE

PC
PCMAG.COM
EDITORS' CHOICE

Best Identity Management Solution of 2017

NETWORK WORLD CLEAR CHOICE WINNER



NETWORKWORLD

THE CONNECTED ENTERPRISE = JUNE 15, 2015

Best tools for single sign-on

It has been a few years since we last looked at single sign-on products, the field has gotten more crowded and more capable.

BY DAVID STROM, NETWORK WORLD

Single mindedness

Since we last looked at single sign-on products in 2012, the field has gotten more crowded and more capable. For this round of evaluations, we looked at seven SSO services: Centrify's Identity Service, Microsoft's Azure AD Premium, Okta's Identity and Mobility Management, OneLogin, Ping Identity's Ping One, Secure Auth's IdP, and SmartSignin. Our Clear Choice test winner is Centrify, which slightly outperformed Okta and OneLogin.

Clear Choice test winner—
Centrify

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect the judgement at the time and are subject to change.

Gartner "Magic Quadrant for Identity and Access Management as a Service" by Gregg Kreizman, June 2016. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Thank You

Centrify®

ZERO TRUST SECURITY