

SPICE WORLD 2019

Be the Knight to Your
Active Directory Foes!

SPICEWORLD2019



Christopher Clai
Senior Cyber Security Engineer

SPICEWORLD2019

Best Practices to Harden Active Directory

SPICEWORLD2019

Document, Document, Document, Document

- Domain Configuration
- OU Design
- Group Usage
- Security Assignments
- Group Policy



From Microsoft's 25th anniversary in 2000

Develop - Structure and Process

- How do we handle....
 - Privileged Accounts? Standard Accounts? Service Accounts?
 - Computer Objects?
 - Permissions and Groups?
 - Account Management requests?
 - Disabling users?
- When do we review our AD configuration?

Backing Up Domain Controllers

- Perform a snapshot of the AD environment with **NTDSUTIL** before major changes.
- **Avoid snapshots with hypervisors** unless you want USN issues.
- Bare metal backup from Windows Server Backup is only supported restore methodology supported by Microsoft beyond NTDSUTIL snapshots.

Quick Tips for Hardening The Overall Environment

- Stop using the Administrator account! (RID 500)
- Disable SMBv1.
- Configure PDC to update time via NTP. All other systems via AD.
- Control DNS Communication.
- Enable *Restricted Admin Mode* on Remote Desktop Services for servers.
- Control Your IPv6 Environment as well as your IPv4.
- Enable PowerShell Logging!

Isolation and Network Segmentation

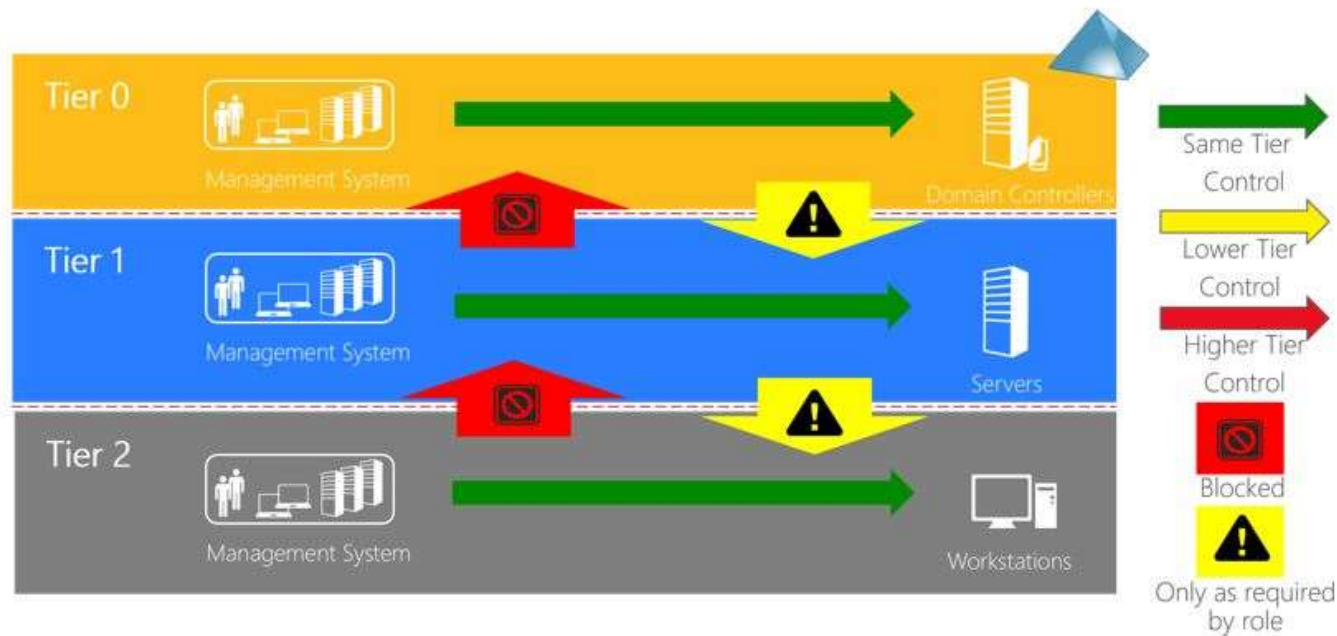
- Evaluate your network traffic flow.
- Isolate workstation to workstation communication unless necessary.
- Restrict administrative connections to servers to a privileged subnet.
- Block direct internet access from sensitive systems. (Like Active Directory)

Building an Administrative Environment

- Setup different Administrator accounts for each tier.
- Control access through GPO User Rights and networking segmentation.
 - Don't allow login or enumeration of privileged accounts to lower-tier systems and vice versa.



Build an Administrative Environment



Domain Controller Hardening

- Turn on the Windows Firewall.
 - Use your scopes!
- Remove non-AD related services.
- Forward Your Logs!
- Patch Frequently and consistently.
- Schedule regular audits of applications, system tasks, services.
- Disable Web Browsing.

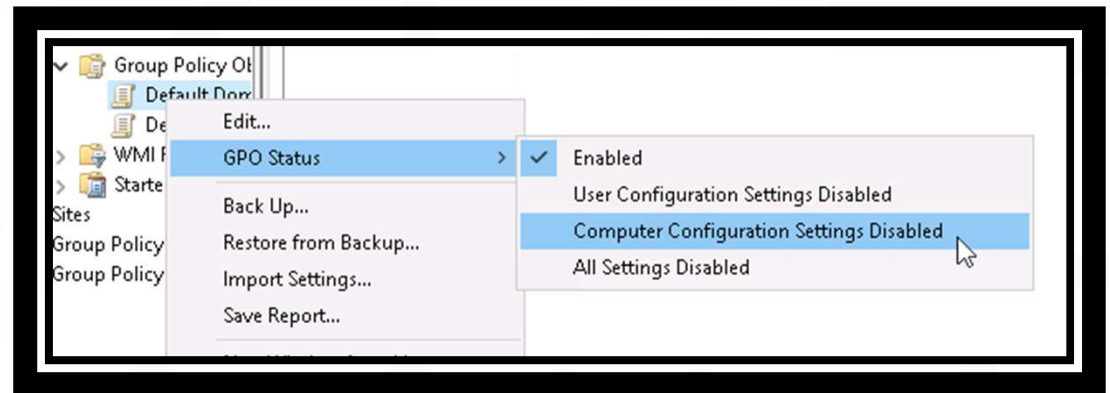


(Re)Structure Your OUs

- Structure to balance GPO application and administration.
- Use default OUs as honeypots with exception to Domain Controllers.
- Keep users, groups, and computer objects separate.
 - Separate your privileged accounts and groups too!
- Separate distribution and security groups.

Simplifying Your GPOs

- Use WMI and security filtering sparingly through effective OU design.
- Separate User and Computer settings and disable those parts of the policy if not in use to reduce the amount of settings a client system must evaluate.





Sample GPO Policy Flow Guideline

SPICEWORLD2019

#spiceworldATX

Modernize Your Authentication

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options

- LDAP Signing and Channel Binding enabled.
- Digitally sign communication.
- Never send unencrypted passwords to SMB servers.
- Require NTLM v2 at least. Block NTLM v1. Audit usage.
- Require SSL & 128-bit encryption for NTLM SSP where possible.

Elevating Your Passwords

- Change your Out of Band Passwords (DSRM & Domain Admin) regularly and stored non-digitally.
- Implement LAPS (Local Administrator Password Solution).
- Disable the storage of LM Hashes. (Via GPO)
- Change the KRBTGT Account Password Annually. Change once. Wait a day. Change again.

A man with a mustache, wearing a dark suit, white shirt, and patterned tie, is shown from the chest up. He has a surprised or incredulous expression on his face. The background is a blurred office setting with a window and some office equipment.

12345?

**THAT'S AMAZING!. I HAVE THE SAME
COMBINATION ON MY LUGGAGE!**

It's About Layers

- Document, Structure, Process. It matters.
- Rethink how you structure and design your AD environment.
- Retire Legacy Functionality, strengthen your configuration.
- Isolate and control network flow to sensitive systems.
- Tier your administration.
- Modernize your authentication.
- Sign your LDAP! *January 2020 is right around the corner.*

Managing, Monitoring, and Auditing Active Directory

SPICEWORLD2019

Managing Beyond The DC

- Use Remote Server Administrative Tools (RSAT)
- Learn & Use PowerShell

Import-Module ActiveDirectory

Enter-PSSession -ComputerName <SERVER>

Using Different Credentials?

\$mycred = Get-Credential

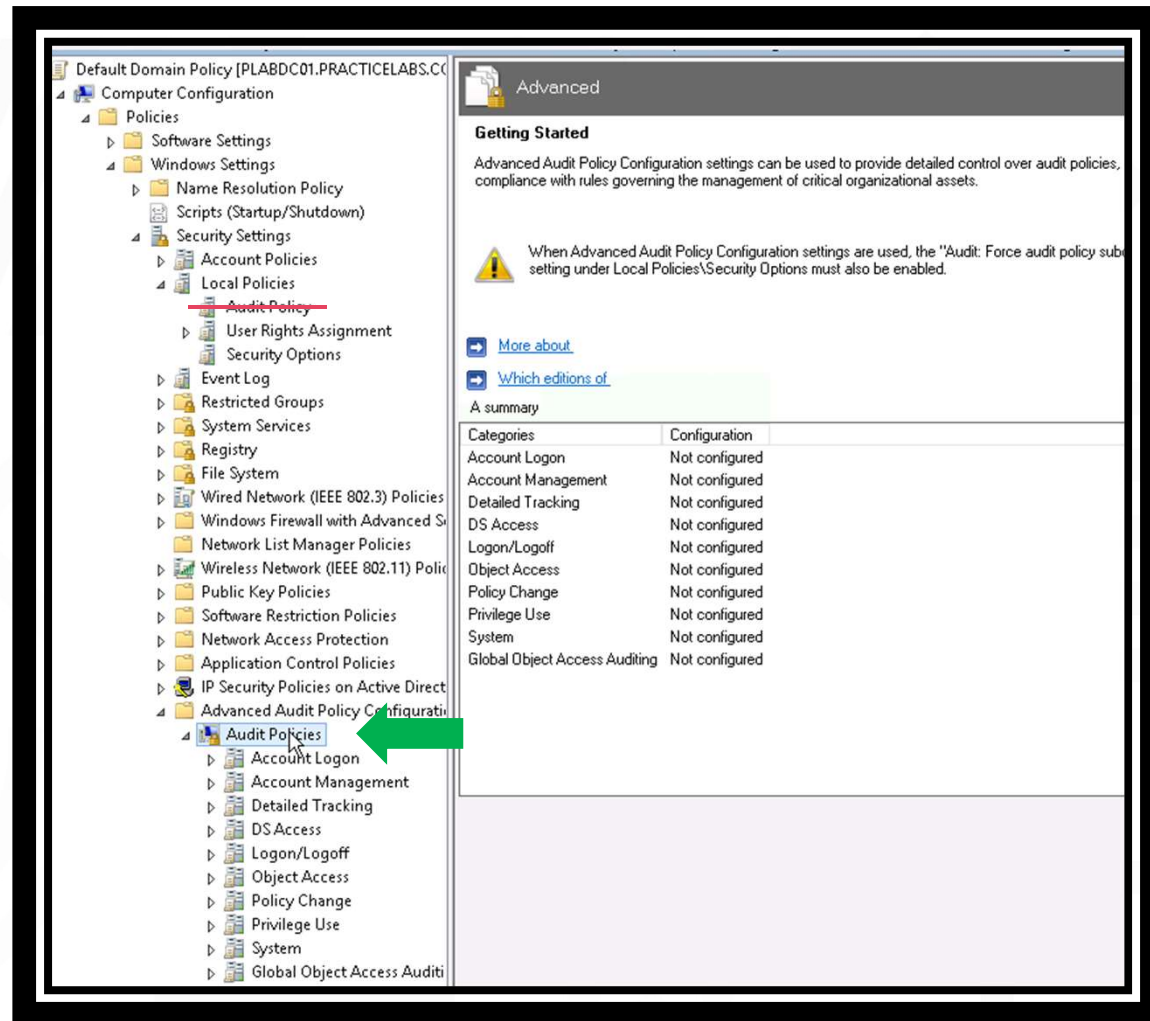
Enter-PSSession -ComputerName <SERVER> -Credential \$mycred

Setting Up Auditing

- Use Group Policy to define audit settings.
- Use Audit Categories for more granular control.

Audit: Force audit policy subcategory settings...

- Determine the acceptable amount of logging data.





Identifying Suspicious Activity

SPICEWORLD2019

♥ System Logs

System logs are your greatest source of information.

Protect log integrity by forwarding specific events or entire logs to another system.

- Security
- System
- Application and Services Logs
 - Directory Service
 - Windows PowerShell
 - Microsoft > Windows > App Locker
 - Microsoft > Windows > PowerShell
 - Microsoft > Windows > Windows Firewall w/ Advanced...

The screenshot shows the Windows Event Viewer application. The left pane displays the 'Event Viewer (Local)' tree with 'Security' selected under 'Windows Logs'. The right pane shows a list of security events, with 'Event 4634, Microsoft Windows security auditing.' selected. The 'Details' tab is active, showing the event description: 'An account was logged off.' and the following details:

Subject:	
Security ID:	S-1-5-90-3
Account Name:	DWM-3
Account Domain:	Window Manager
Logon ID:	0xAF09B

Logon Type: 2

This event is generated when a logon session is destroyed. It may be positively correlated with a Logon ID value. Logon IDs are only unique between reboots on the same computer.

At the bottom, a summary of the event is provided:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4634
Level:	Information
User:	N/A
OpCode:	Info
More Information:	Event Log Online Help

Additional details on the right side of the summary table:

Logged:	15/09/2019 17:59:58
Task Category:	Logoff
Keywords:	Audit Success
Computer:	PLABDC01.PRACTICELABS.C

The bottom right corner of the window displays the text '#spiceworldATX'.

GUI Searching Tips

- Find Audit Failure or Success Under *Keywords*.
- User search isn't always successful. Use: *Domain\Username*.
- When in doubt, use the *Find* feature.
- Create Custom Views for frequent searches.
- Use the Administrative Events custom view.

The screenshot shows the 'Filter Current Log' dialog box with the 'Filter' tab selected. The 'XML' tab is also visible. The 'Logged:' dropdown is set to 'Any time'. Under 'Event level:', the checkboxes for 'Critical', 'Warning', 'Verbose', 'Error', and 'Information' are all unchecked. The 'By log' radio button is selected, and the 'Event logs:' dropdown is set to 'System'. The 'By source' radio button is unselected, and the 'Event sources:' dropdown is empty. Below these, a text box contains '<All Event IDs>'. The 'Task category:' dropdown is empty. The 'Keywords:' dropdown is empty. The 'User:' dropdown is set to '<All Users>'. The 'Computer(s):' dropdown is set to '<All Computers>'. There is a 'Clear' button at the bottom right of the filter options. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

Filter Current Log

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

☒ By log Event logs: System

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

Searching Via PowerShell

Get-EventLog -List

Get-EventLog -LogName <Log>

-Newest #

-EntryType <Error, Warning, FailureAudit, SuccessAudit>

-UserName <User01, User*, or Domain01\User*>

-Message <*description*>

Export-CSV -Path <Path and CSV Detail>

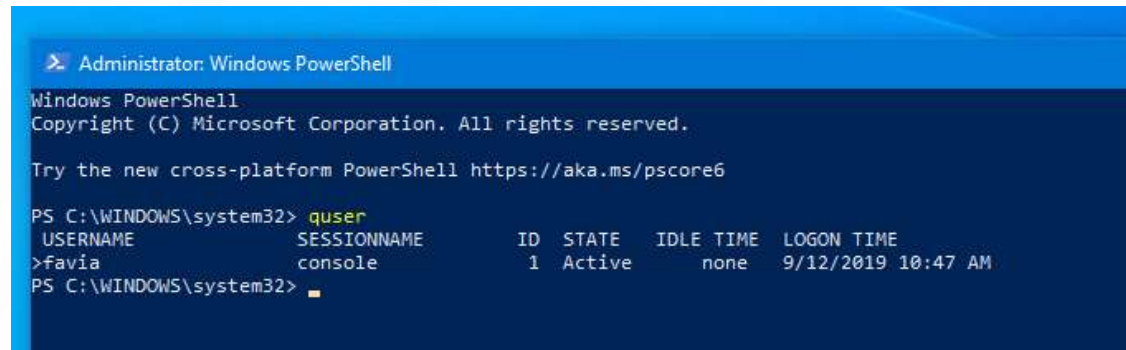
Get-EventLog -LogName Security | Where-Object {(\$_.eventid -eq 4732 -or
(\$_.eventid -eq 4733) -or (\$_eventid -eq 4746))} | Select
EventID, MachineName, EntryType, Message, InstanceID, TimeGenerated, Time
created, UserName | fl | Export-CSV C:\search.csv

Looking for Sessions

Stale sessions are a risk to your overall security posture.

Use PowerShell to locate sessions.

`quser /server <System Name>`



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

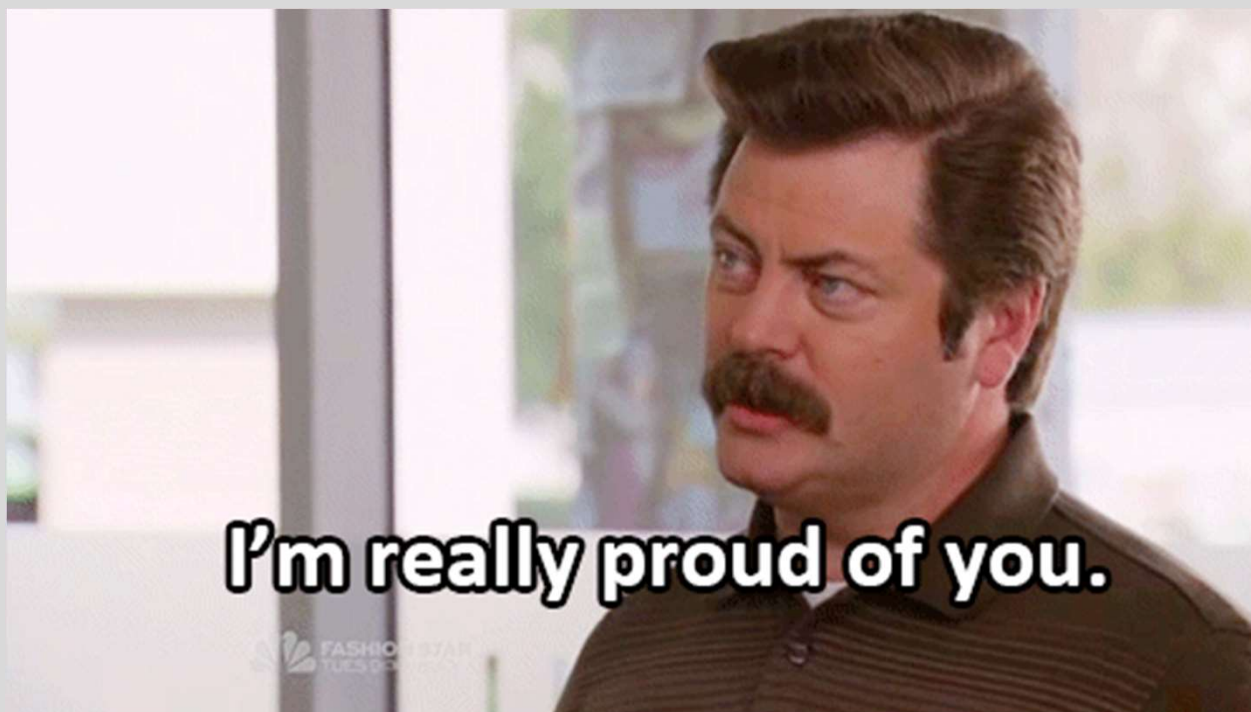
PS C:\WINDOWS\system32> quser
USERNAME          SESSIONNAME      ID  STATE  IDLE TIME  LOGON TIME
>favia            console         1   Active  none       9/12/2019 10:47 AM
PS C:\WINDOWS\system32>
```

Develop a Daily Routine

- New Accounts
- Modified Accounts
- Changes to Privileged Accounts & Groups
- Password Changes Outside Typical Times
- Logins to Special Accounts (Domain Admin)
- Group Policy Modifications

Staying Vigilant

- Get cozy with your system logs.
- Use PowerShell to search for specific events when suspect.
- Develop a daily routine to check for irregularities.
- Look for unexpected sessions on systems.
- Review and audit configuration annually, at least.



I'm really proud of you.

FASHION STAR
TUESDAY

www.syntaxbearror.io/spiceworld2019/

Password is **spicerex**

@chrisclai

chris.clai@ieee.org



SPICEWORLD2019



Thank you.

SPICEWORLD2019