



Be the Knight to Your Active Directory Foes!

Resource Handout and Supplemental Guide

Attended the Panel at SpiceWorld 2019?

Please rate the session and give any constructive feedback on what I can do to provide a better experience.

To rate the panel, please do the following:

1. Open the **SpiceWorld** app on your phone.
2. Click on **Schedule**.
3. **Locate the session** you are attending and click / press on it.
4. Scroll toward the bottom to the survey section and press on the link to **take the session survey** to complete it.

Thank you in advance and hope to see you next year!

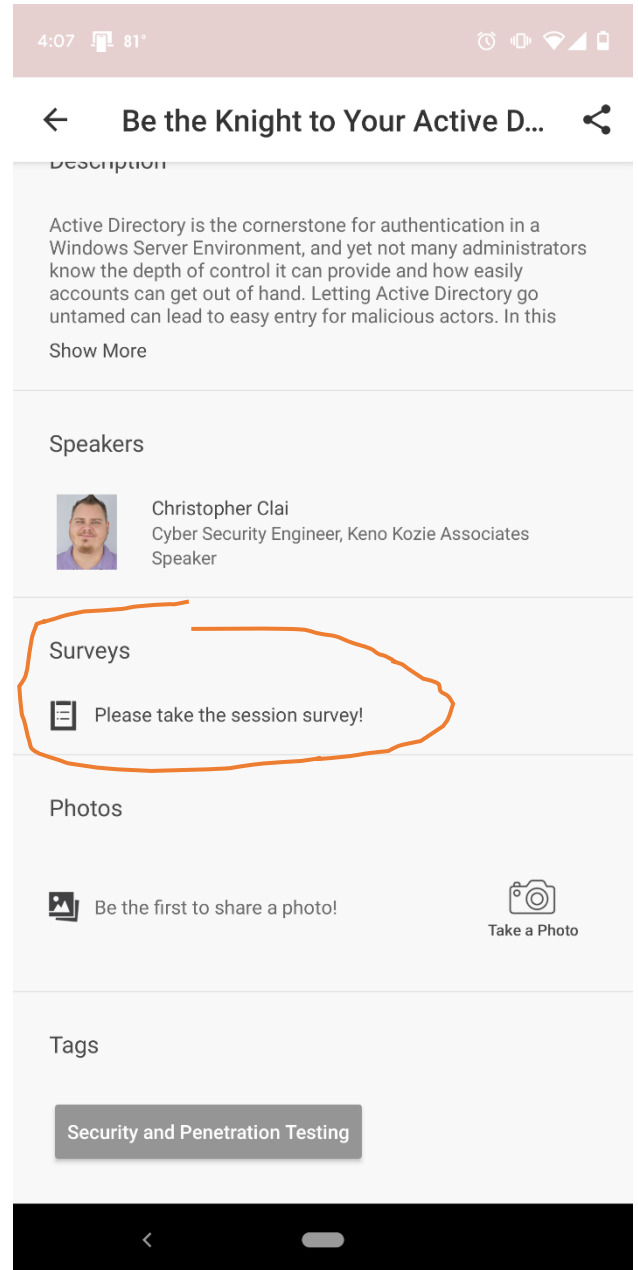


Table of Contents

Best Practices to Harden Active Directory

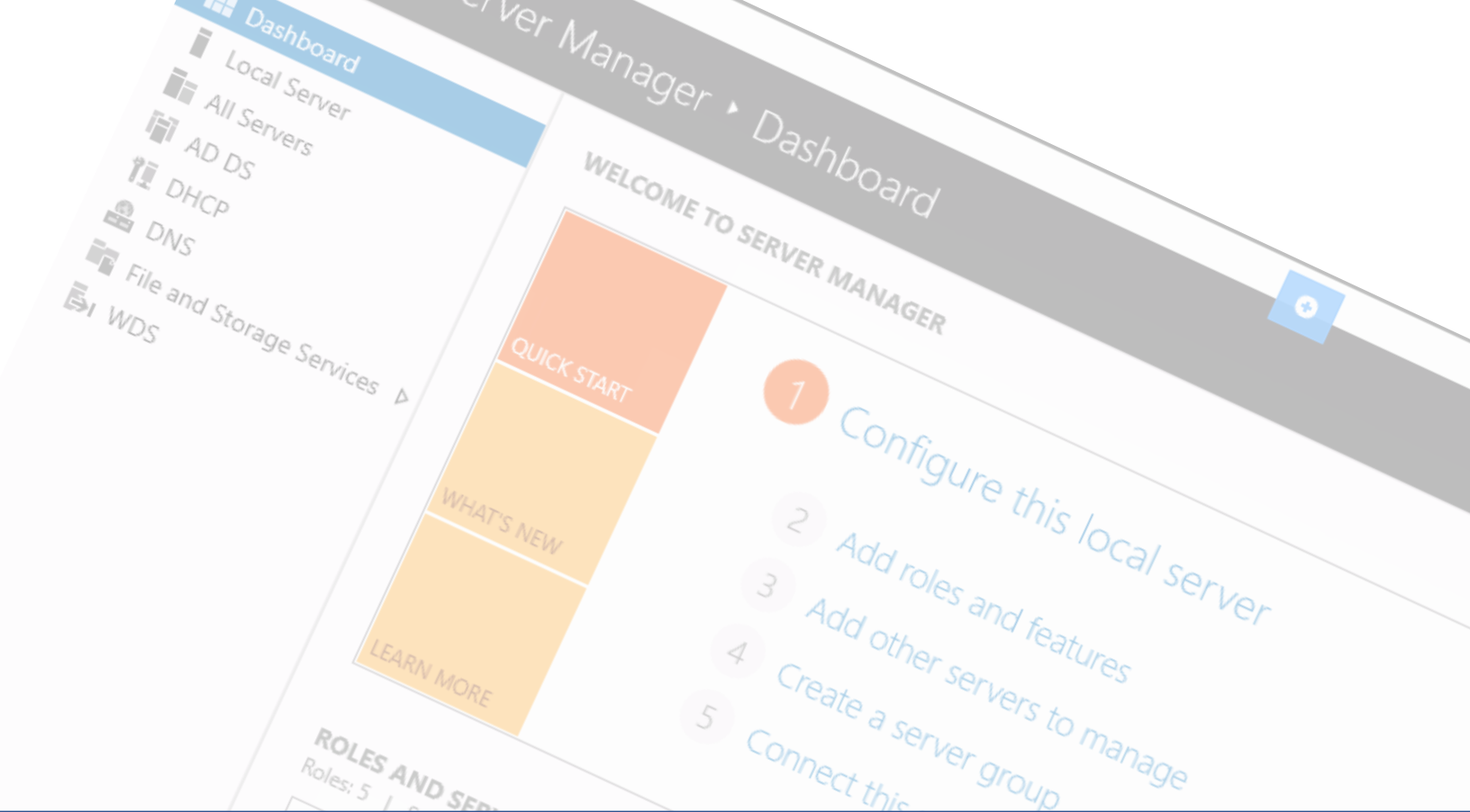
Document, Document, Document, Document.....	4
Developing Structure and Process.....	5
Backing Up Domain Controllers.....	6
Quick Tips for Hardening the Overall Environment.....	9
Isolating Systems Using Windows Firewall and Network Segmentation.....	14
Building an Administrative Environment.....	15
Defining Administrative Account Rights.....	16
Privileged Access Workstations (PAWs)	17
Domain Controller Hardening.....	18
(Re) Structuring Your OUs.....	19
Simplifying Your GPOs.....	21
Sample GPO Policy Flow Configuration.....	22
Modernize Your Authentication.....	23
Elevating Your Passwords.....	26

Managing, Monitoring, and Auditing Active Directory

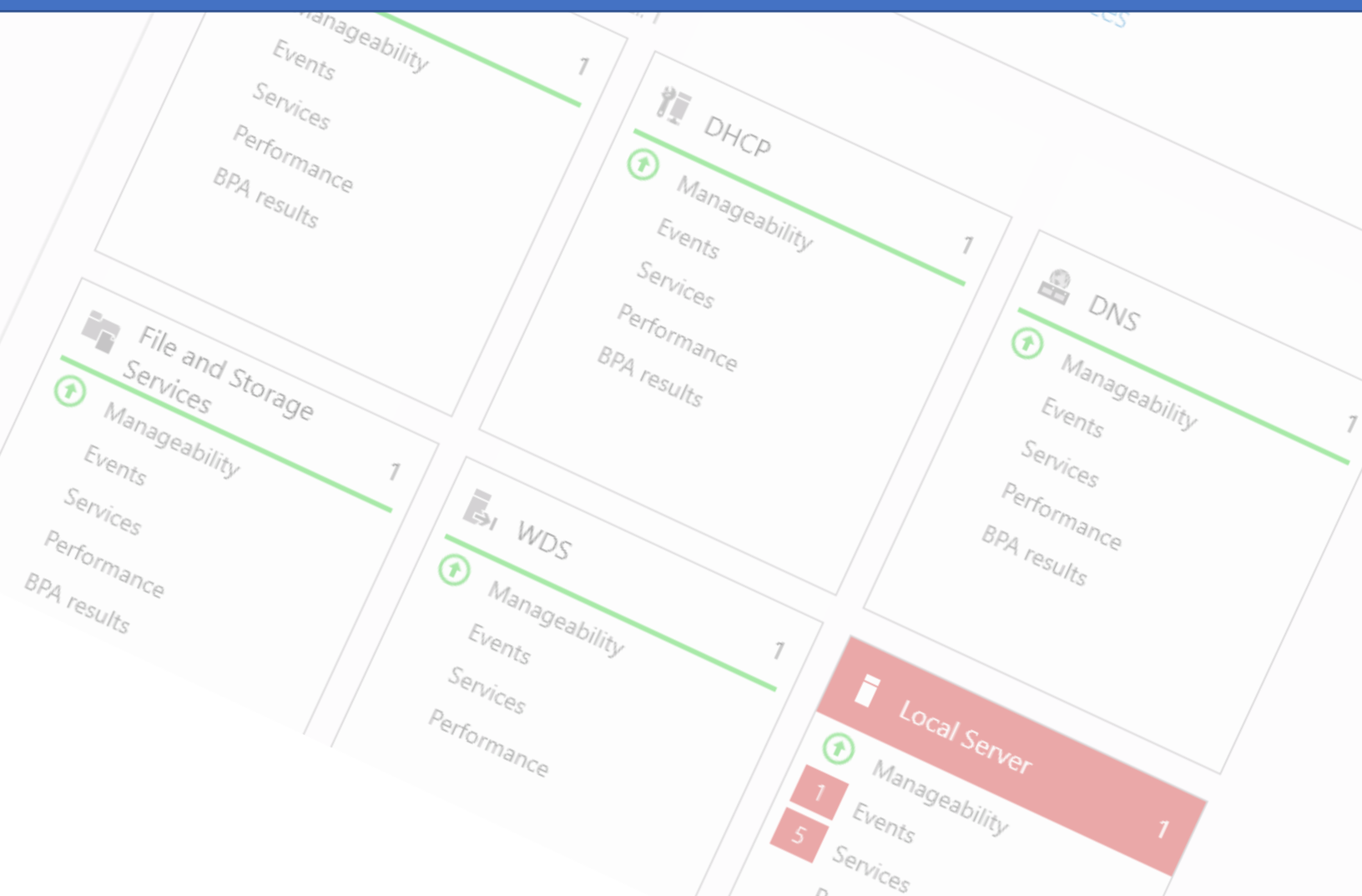
Managing Beyond the DC.....	29
Setting Up Auditing.....	30
Understanding Audit Guidance.....	31
Audit Category: Account Logon.....	32
Audit Category: Account Management.....	33
Audit Category: Detailed Tracking.....	34
Audit Category: DS Access.....	35
Audit Category: Logon and Logoff.....	36
Audit Category: Policy Change.....	37
Audit Category: System.....	38
Audit Categories: Global Object Access Auditing, Object Access, and Privilege Use.....	39

Identifying Suspicious Activities

♥ System Logs.....	41
Log Management Tips.....	42
GUI Searching Tips for Event Viewer.....	43
Searching via PowerShell.....	44
Look for Sessions.....	45
Develop a Daily Routine.....	46
Additional Resources.....	47



Best Practices to Harden Active Directory



Document, Document, Document, Document

One of the single biggest issues I've found in my career is the amount of System Administrators who seem to forget to document. There are various reasons given for this from fear of losing the job if they share the knowledge to overload or even apathy.

In an age where compliance and standards are becoming the definition and processes like ITIL or COBIT are being adopted, you can no longer ignore documentation. Taking the time and resources to document the way things are setup, how they are connected, and how they are managed will make it easier for you and your team down the road and helps when disaster strikes.

When it comes to Active Directory, here are things I often look for:

- Domain configuration
- OU design and usage details
- Group usage (Security, Distribution, Privileged)
- Group Policy
- Security Assignments / Permissions

If you haven't started on your documentation journey, the above list may be a good start for defining what you need to produce.

When in doubt, document it out.

Developing Structure and Process

Once you begin documenting the way things are configured, you may find a burning need to develop structure which simplifies administration, but also makes documentation easier.

If you don't have a structure around your Active Directory environment, then it's time to think about how you structure and organize your OUs and GPOs. These should be structured in a way that balances the simplification of administration with the simplification of GPO application. This is a careful tasking because excessive GPOs can lead to settings issues, and overly complicated administration can lead to poor management and things getting by with nobody recognizing.

When it comes to processes, they require structure and documentation in order to be efficient. So once you have those down, it's time to consider how we handle AD operations in the environment.

To help guide you on that process, here are some questions that I often use on engagements.

- How permissions are issued?
- How are accounts are provisioned and deprovisioned?
- How are service accounts managed?
- How is AD managed?
- How AD is backed up or made redundant?
- How do you manage computer objects?
- How do you handle group management?
- Is there any delegation process within the environment?

Getting the foundations of documentation, structure, and process can be initially time consuming, and you may bounce between them until you find a harmonious balance that works best for your environment.

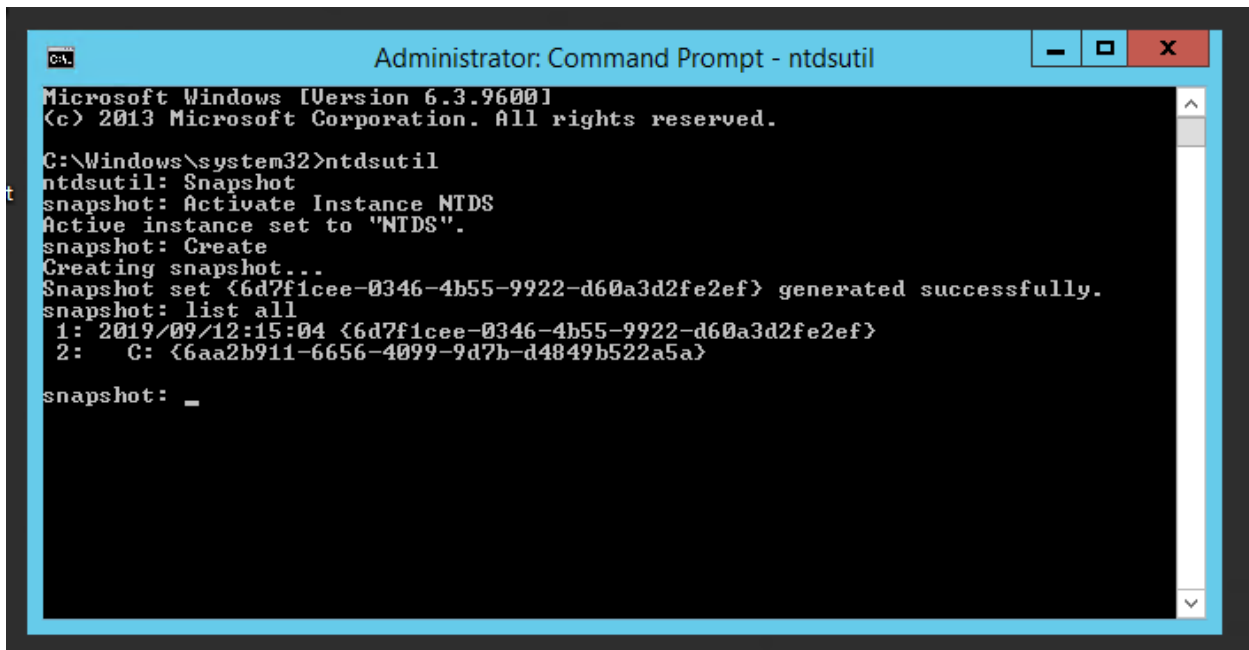
Backing Up Domain Controllers

Using NTDSUTIL to Snapshot Your AD State

NTDSUTIL is a command-line tool that can be used to perform database maintenance of Active Directory Domain Services and Active Directory Lightweight Directory Services.

To create a snapshot with NTDSUTIL

- Run a command prompt in Administrative Mode
- Run the following commands:
 - Ntdsutil
 - Snapshot
 - Activate Instance NTDS
 - Create
- Ctrl + C to close the ntdsutil or type exit and hit enter. You may have to type exit a 2nd time after.



```
Administrator: Command Prompt - ntdsutil
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

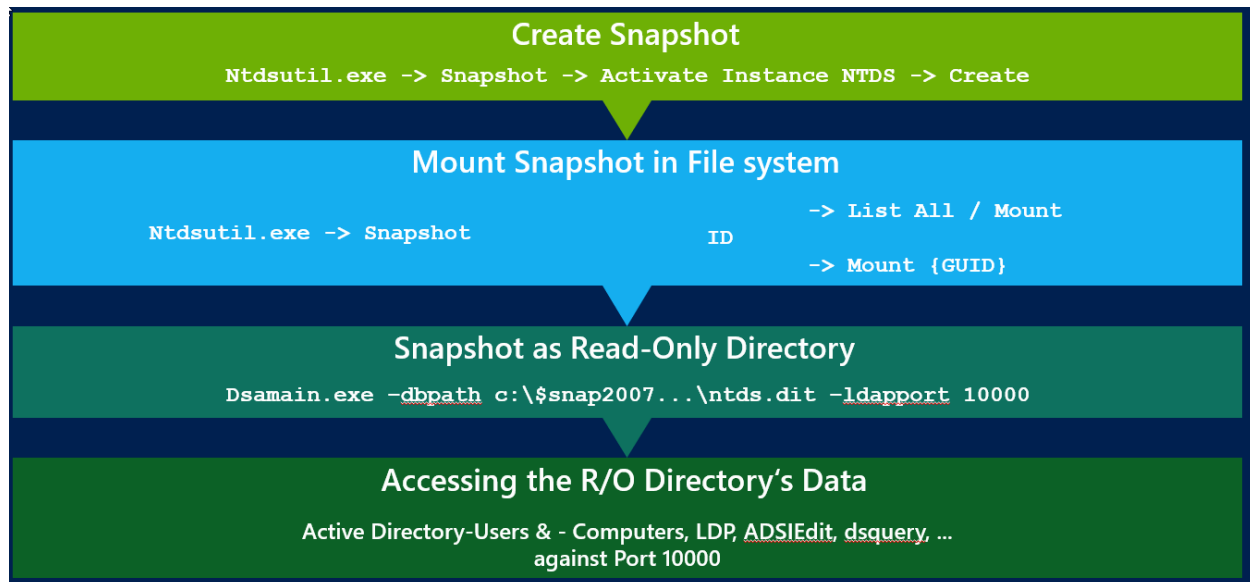
C:\Windows\system32>ntdsutil
ntdsutil: Snapshot
snapshot: Activate Instance NTDS
Active instance set to "NTDS".
snapshot: Create
Creating snapshot...
Snapshot set {6d7f1cee-0346-4b55-9922-d60a3d2fe2ef} generated successfully.
snapshot: list all
1: 2019/09/12:15:04 {6d7f1cee-0346-4b55-9922-d60a3d2fe2ef}
2: C: {6aa2b911-6656-4099-9d7b-d4849b522a5a}

snapshot: _
```

To Review Current Snapshots

- Run a command prompt in Administrative Mode
- Run the following commands:
 - Ntdsutil
 - Snapshot
 - List all
- Ctrl + C to close the ntdsutil or type exit and hit enter. You may have to type exit a 2nd time after.

Mounting and administering a snapshot is a lot more extensive, but these basic two commands are useful to take a snap and make sure it is listed after completion. It's ideal to do this before making major changes.



NTDSUTIL offers some minimal recovery options that may be harder to restore account attributes and group memberships. However, there is a PowerShell solution to assist with that which you can find here: <https://blogs.technet.microsoft.com/ashleymcglone/2014/04/24/oh-snap-active-directory-attribute-recovery-with-powershell/>

In addition to backup functionality, there are other functions available through the NTDSUTIL. For more information about NTDSUTIL, please read: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753343\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc753343(v=ws.11))

Avoiding Snapshots with Hypervisors

Snapshots taken with hypervisors can result in what is known as a USN rollback. This can lead to replication failure and an inconsistent Active Directory which will produce no errors and will not easily appear in general diagnostic functions. You'll notice issues when some DC's don't recognize new AD objects or password changes.

Starting with Windows Server 2012, domain controllers recognize when they are being rolled back, and the DC can take recovery actions when supported System State Restore is done and reinitializes replication agreements between other domain controllers. This requires Hyper-V 3.0, support for the "VM Generation Identifier" (GenID), and you are running Windows Server 2012 or newer.

More details about USN Rollback and methods for resolution and proper rollback options is available here: <https://support.microsoft.com/en-us/help/875495/how-to-detect-and-recover-from-a-usn-rollback-in-windows-server-dc>

Bare Metal Backups with Windows Server Backup or Azure Online Backup

Microsoft is particular when it comes to what backup method they will assist in restores with. To reduce the potential of support issues, it's recommended that you perform bare metal backups using the **Windows Server Backup** or **Azure Online Backup** tools.

If you use another backup product, it's ideal to first perform a bare metal windows server backup on a separate drive, and then back that up.

Quick Tips for Hardening the Overall Environment

There are a series of actions you can take to harden your overall environment that helps protect your Domain Controllers as part of it. They are often easy to get going and can be a great first step toward greater improvements to your security posture.

Stop Using the Default Administrator Account (RID 500)

RID 500 refers to a portion of the Security Identifier (SID) that is assigned to the default domain administrator account. The SID of the account will often be **S-1-5-21-domain-500**.

This account should be your emergency account should you need to utilize it. Change the password at least annually, if not more frequently, make it strong, and keep it stored offline. Access to the password should be limited. I recommend storing it alongside your DSRM password.

When you stop using the account, you can begin using the account as a honeypot and track its behavior more aggressively to spot signs of potential compromise.

Need to determine which Active Directory account is the RID 500 one?

1. Logon to a DC or any domain joined computer with Support Tools or **RSAT** installed.
2. Open **LDP.EXE** from the Start Menu
3. Click the **Connection menu** and **select Connect**
(you can leave this window blank and it will connect to the closest DC)
4. Click **OK**
5. Click the **Connection menu** again and **select Bind**
(you can leave this window blank and it will use the current user's credentials)
6. Click **OK**
7. Click the **View menu** and **select Tree**.
8. Select the Domain from the list and click **OK**.
9. Expand the nodes to see the OUs. Navigate around until you find any user account (could be yours, it doesn't matter)
10. Press **CTRL+N** to clear the screen
11. Double clicking any existing user account looking for the ObjectSID attribute in the right hand pane. It should look like objectSID=S-1-5-21-xxxxxx-xxxxxx-xxxxxxx-xxx. Write down that SID.
12. Now right click the DC=**domainname**,DC=**domain** node from the left pane, and select **Search**.
13. Make sure Base DN is DC=**domainname**,DC=**domain** and scope is set to Subtree.
14. Change the filter to: **(objectSID=S-1-5-21-xxxxxx-xxxxxx-xxxxxxx-500)**
15. Click **Run**, and should see the user's name and location in the background (right pane). You are looking for the **distinguishedName** attribute. That's it.

Disable SMB1

SMB1 is a depreciated protocol that is over 30 years old. The original protocol is subject to denial of service, remote code execution, and man-in-the-middle attacks. It is also a path used by malware to quickly propagate.

SMB1 may still be used by NAS devices and certain printers of manufacturers who love to use old technology, but it should not be used in a modern network today. As long as SMB1 is enabled, it remains a quick path to exploitation.

For full details on how to disable and remove SMB1, read the following Microsoft KB:

<https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server>

Read more about SMB1 and more on why you need to seriously stop using it:

<https://techcommunity.microsoft.com/t5/Storage-at-Microsoft/Stop-using-SMB1/ba-p/425858>

Configure Your PDC to Update Time via NTP, All Others via AD

Time manipulation is a method for adversaries attempt to gain authentication approval, and to cover the tracks of their activities beyond clearing or corrupting logs. By controlling how time can be manipulated in your environment, you reduce the risk of systems going out of sync.

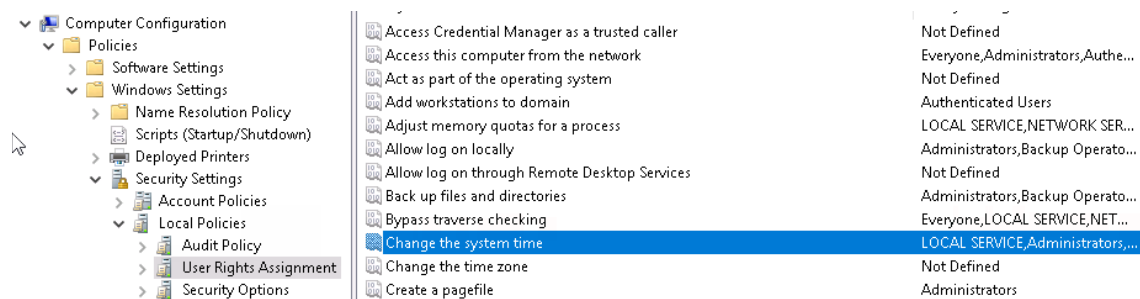
You will also want to limit time control changes to certain Administrative groups via the GPO. You can do this by navigating to *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment*.

Define the setting for *Change the System Time*.

A recommended setting is allow system time to be changed by Domain Administrators on the Domain Controllers and GPOs that target non-DCs should not have any account listed, but the setting should be defined to prevent an override locally.

Configuring NTP on Windows Using GPOs:

<http://www.sysadminlab.net/windows/configuring-ntp-on-windows-using-gpo>



Control DNS Communication in Your Environment

The advent of DNS-over-HTTPS promises to be more secure for users but comes at a cost to modern system administration and provides certain vendors with considerable information about your user's activities. DNS-over-HTTPS bypasses traditional DNS controls which can lead to hackers being able to transparently resolve and communicate to Command and Control servers.

To control this type of behavior, the following steps are recommended:

- Block all DNS communication outbound except from approved servers.
- Force DNS settings to come from your network DHCP environment or statically assigned.
- Use ADMX files issues by the major browser vendors to block and deny DNS-to-HTTPS features.
 - Google Chrome: <https://support.google.com/chrome/a/answer/187202?hl=en>
 - Mozilla Firefox: <https://github.com/mozilla/policy-templates/releases>
 - Microsoft Edge: <https://www.microsoft.com/en-US/download/details.aspx?id=53430>

Expect in the future that blocklists will be coming out intended to block other DNS-over-HTTPS services as they come online.

Enable Restricted Admin Mode on Remote Desktop Services for Servers

RestrictedAdmin mode prevents the transmission of reusable credentials to the remote system to which you connect using remote desktop. This prevents credentials from being harvested during the initial connection process if the remote server has been compromised.

When RestrictedAdmin mode is enabled, your account must be a member of the local Administrators group on the destination system. If your users do not use RDP to connect to their workstations, then you can enable this on workstations as well.

To Enable Destination Systems to Receive Incoming Remote Desktop Connections Using RestrictedAdmin mode, make the following registry changes:

1. Open Registry Editor: click **Start**, click **Run**, type **regedit**, and then click OK.
2. In Registry Editor, create the following registry key:
 - HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa**
 - Name: **DisableRestrictedAdmin**
 - Type: **REG_DWORD**
 - Value: 0
3. This setting takes effect immediately; no reboot is required.

To disable RestrictedAdmin mode, set the value of **DisableRestrictedAdmin** to 1.

To use Remote Desktop in RestrictedAdmin Mode

Open a command prompt and enter the following: *Mstsc.exe /V:Server01:3390 /RestrictedAdmin*

To Require all Outbound Remote Desktop requests to use RestrictedAdmin mode:

Be sure to push the registry change noted above prior to making this setting in group policy, or you'll be unable to RDP to the desired system(s).

1. Open Group Policy Management Console: click **Start**, click **Run**, type **gpmc.msc**, and then click **OK**.
2. Select the group policy which best applies to the systems from which you will initiate Remote Desktop connections.
3. Edit the Group Policy and navigate to the following node:

Computer Configuration\Policies\Administrative Templates\System\Credentials Delegation

4. Configure the value of "Restrict delegation of credentials to remote servers" to **Enabled**.
5. This setting will take effect when Group Policy refreshes. To immediately refresh group policy, open an elevated command prompt and enter the following text:

Control Your IPv6 Environment as well as your IPv4

IPv6 is turned on by default in newer OS's. While the intent was positive, intending to keep your computers from being unable to communicate with IPv6 only systems, it has unintended consequences. When an environment does not have an IPv6 issuer, systems turn to the link-local methodology to develop connectivity between devices within a network segment.

This has resulted in several risks, but the three major ones are:

- **Lack of IPv6 Security Training and Education.** The lack of understanding results in security holes that are unknown to the team managing the network.
- **Security Device Bypassing via Unfiltered IPv6 and tunneled traffic.** There are currently 16 different tunnel and transition methods, not including upper layer tunnels for SSH, IPv5-IPSec, SSL/TLS, and even DNS. Local network equipment may forward IPv6 packets to edge devices before transitioning to IPv4 with traditional network monitoring tools and security structures not acting upon the traffic. This leads to an easy route for attackers with little to no insight for your team. Traditional segmentation methods have been shown to be bypassed by IPv6 tunneling.
- **Lack of IPv6 Support with ISPs and vendors.** Not having a native IPv6 connection from your provider results in a tunnel style configuration. A tunnel connected to your interface further increases security complexity and provides an opening for man-in-the-middle and denial-of-service attacks.

Additional risks continue to be found as research is continued into the subject of the risks of uncontrolled IPv6 in an environment.

Disable IPv6 communication from workstations and servers unless explicitly noted by the vendor until you have native IPv6, DHCP issuance, and security controls that adequately monitor, shape, or control IPv6 flow within your network environment. (There is some evidence that disabling IPv6 affects Exchange Systems).

A proper deployment is essential to avoiding risks that IPv6 can cause due to default configuration.

Additional reading on the subject:

http://ipv6forum.com/dl/white/IPv6_security_models_and_implications_28072010.pdf

<https://sba-research.org/wp-content/uploads/publications/Johanna%20IPv6.pdf>

<https://blogs.cisco.com/security/icmp-and-security-in-ipv6>

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=907211

<http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IPv6-Security-Audit-Assurance-Program.aspx>

<https://www.darkreading.com/attacks-breaches/ipv6-and-the-growing-ddos-danger/a/d-id/1322942>

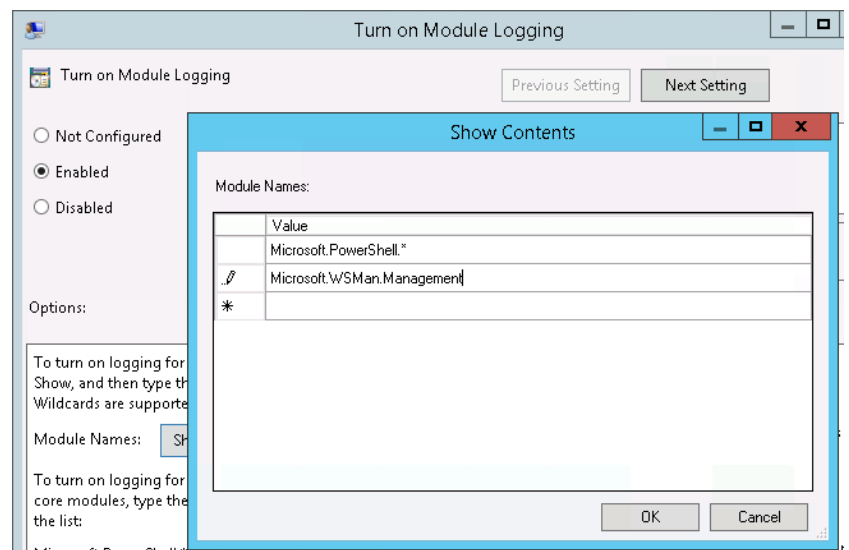
<https://www.networkworld.com/article/2171504/biggest-risks-in-ipv6-security-today.html>

Enable PowerShell Logging

If you are not already, you want to log PowerShell activity to be able to review and capture commands and scripts ran in your environment. The results of this logging are found in the Event Viewer under *Application and Services Log > Microsoft > Windows > PowerShell > Operational*.

To configure PowerShell logging, perform the following:

1. Open Group Policy Editor and navigate to:
Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell
2. Select the setting for **Turn on Module Logging**.
3. Configure as shown below:
 - a. Select **Enabled**
 - b. Define the Module Names by click on *Show...* :
Microsoft.PowerShell.*
Microsoft.WSMan.Management



Isolating Systems Using Windows Firewall and Network Segmentation

You can severely restrict unauthorized use of your environment and lateral movement by creating isolation zones in your environment. These can start simple and become more comprehensive as time goes on.

Start by determining some basics. Here are some questions I like to start off with to define a basic plan.

1. Do my workstations need to communicate directly with each other?
2. What servers do my workstations need to communicate directly to?
3. What subnet(s) am I performing administrative tasks from?
4. Do any sensitive servers require direct access to the internet?
5. Does my BYOD network need any access to servers or just direct internet access?

These questions can begin developing the foundation for your network segmentation and isolation planning.

For example, if your workstations do not need to communicate directly with each other, then block communication between them through Windows Firewall and limit communication to a specific server subnet and the internet.

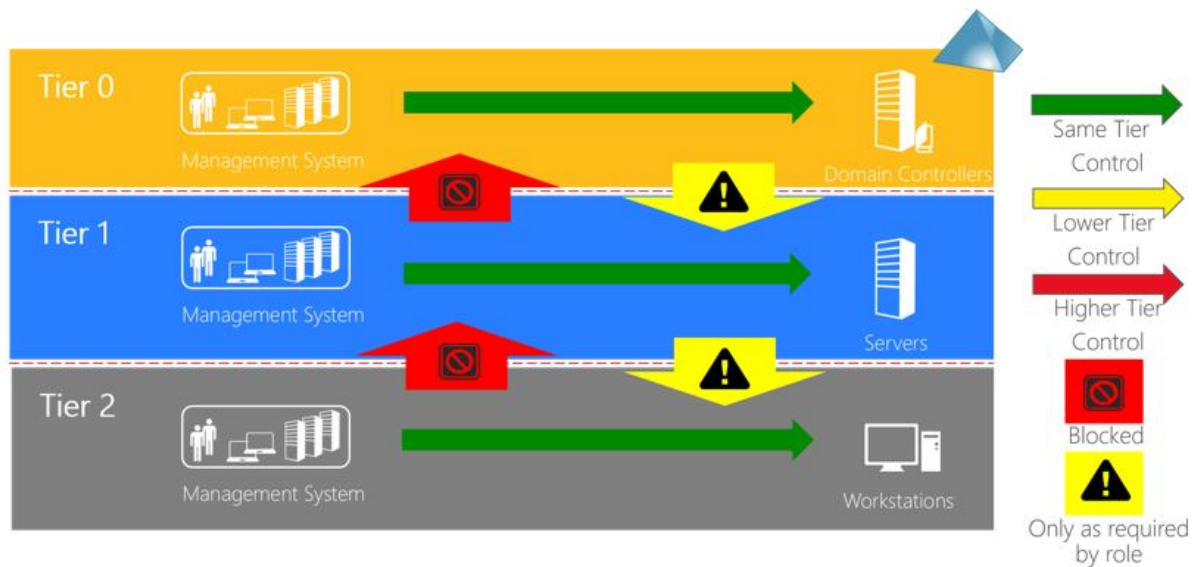
You can do the same with your servers by limiting what workstations can communicate with them and restricting what subnet can touch administrative ports such as WMI, RPC, and RDP.

These modifications will help slow down someone attempting to gain access in your environment and provide a better opportunity for you to react and stop an active attack.

Building an Administrative Environment

Building an administrative environment is part of a broader effort to further limit the damage potential and lateral movement of attackers who gain credentials into your environment.

The model introduced by Microsoft focused on three tiers as shown below:



Administrators are generally limited to the tier in which they are issued. This can be controlled via Group Policy and firewall rules.

In the above model, Tier 0 is where the most sensitive accounts would be located, which manage the domain controllers. Administrators in lower tiers are unable to administer or login to the domain controllers directly, but there is a potential based on role to communicate from Tier 0 to lower tiers.

If you can avoid the downward movement, I would recommend doing so to limit the potential of those credentials being gained to begin with.

This means that if an Administrator manages all three tiers, they should have a different logon for each tier, and use a different workstation to manage each tier. These administrative workstations can be shared. Further guidance regarding privileged access workstations (PAWs) are further in this document.

This model can be gradually employed over time, increasing in complexity to ease a transition in an active environment. It can also be beneficial to employ other network security practices such as network segmentation and stricter control on communications between system tiers beyond just the administrative control.

For more information regarding the concept of the Secure Privilege Model, please view the following information: <https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material>

Defining Administrative Account Rights

Part of building an administrative environment includes creating different levels of Administrators in order to maintain the different systems. Here are some things to consider in making sure you follow principles of least privilege to limit the permissions of each account type.

Configuring Tier 0 Administrators

Only your **Tier 0 Administrators**, the ones who manage your Domain Controllers, should be granted membership as a Domain Administrator.

All Other Administrators

For all other administrators, you should have group policies that define their permission for computers in particular groups.

If you need your other administrators to join systems to the domain, you will need to provide them that permission in a group policy by going to *Computer Configuration > Policies > Windows Settings > Security Options > Local Policies > User Rights Assignment* and defining the **Add workstations to domain** setting.

To define a particular group as local administrators to systems, you'll want to change it in group policy by going to *Computer Configuration > Preferences > Control Panel Settings > Local Users and Groups* and defining the Local Administrator group to include the group of Administrators you want to assign to administer those series of systems. Choose the action of **update**. Avoid replace as this will delete any other records in the group on local systems, unless you are sure you want to do this.

If you need lower tier Administrators to perform specific tasks in AD that are not editable through User Rights Assignment you will want to delegate permissions. To do this:

1. Open **Active Directory Users and Computers**.
2. Right click the target OU that you want to grant permissions to and click **Delegate Control**.
3. Follow the steps in the **Delegation of Control Wizard** to provide the desired permissions.



Privileged Access Workstations (PAWs)

Privileged Access Workstations (PAWs) are used in part with developing an administrative environment which may reduce the ability of attackers to gain access to your sensitive systems, provided other security controls are properly implemented.

PAWs can be dedicated or virtual devices that are intended to be used for administrative activities in your network.

Here are some initial tips toward setting up PAWs:

- Use Windows Hello for Business to provide MFA security on PAW devices.
- Avoid open internet access.
- Run Windows 10 Enterprise and keep it current.
- Enable Credential Guard and Device Guard.
- Only have the core software necessary for the technical activity intended.
- If running virtually, run non-privileged workstations on top of administrative to reduce privilege escalation risks caused by hardware or kernel vulnerabilities.

Additional guidance and more advanced configuration details on PAWs can be found at:

<https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations>

Domain Controller Hardening

There are a series of steps you can take specifically targeted toward your Domain Controllers that should have a low time expense to deploy and have a large amount of benefit. This is in addition to other changes mentioned throughout this document.

Turn on the Windows Firewall

The windows firewall can be a great resource to control the flow of communication to and from your domain controller to reduce the risk of exposure.

Here are some common ports for Active Directory:

Application protocol	Protocol	Ports
Active Directory Web Services (ADWS)	TCP	9389
Active Directory Management Gateway Service	TCP	9389
Global Catalog	TCP	3269
Global Catalog	TCP	3268
ICMP		No port number
LDAP Server	TCP	389
LDAP Server	UDP	389
LDAP SSL	TCP	636
IPsec ISAKMP	UDP	500
NAT-T	UDP	4500
RPC	TCP	135
RPC randomly allocated high TCP ports ¹	TCP	1024 - 5000 49152 - 65535 ²
SMB	TCP	445

Additionally, use scoping to limit administrative such as RDP to the subnet or range of IPs where your administrative activity will occur from.

To view the full details on ports required for various Windows related services and processes, visit the following site: <https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows>

Forward Your Logs

Forwarding your logs can help maintain the integrity of the information being stored by reducing the potential that an attacker is able to modify or manipulate them.

If you roll-over your logs to an archive. Make sure you keep track of the archive location and the space used. There are several solutions to either truncate or copy these files to a central system as needed.

Details about log forwarding can be found here:

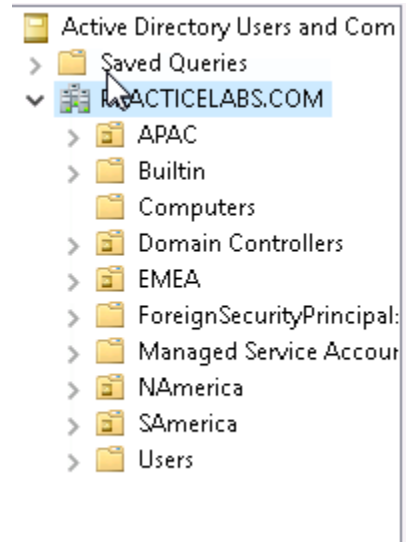
<https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>

(Re) Structuring Your OUs

AD organizes its objects primarily in OUs (Organizational Units). By default, you have a series of OUs provided when you deploy a domain controller.

The default OU's are as follows:

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Managed Service Accounts
- Users



Creating an Effective Structure

When (re)structuring your OU architecture, consider how policy should be applied and to what set of systems. Designing your OU structure around your GPO applications will ease administration over time.

If you are unsure where to start in an established environment, a great way I've used that has generally worked is to evaluate all the current GPOs. This can be time consuming depending on the amount of GPOs the environment has, and how many settings are applied. I break these all down into an Excel Workbook and keep record of:

- Location of Setting in GPO
- Name of Setting
- The value of the setting
- Name of the GPO
- Name of New GPO (to be defined)

I then create another sheet where I note the name of the current GPOs, and where they are linked.

Once you take the time to evaluate the settings of all the GPOs, you may find where policy has been duplicated, contradicted, or cancelled out. Look for ways you can reduce the policies. If you find settings in other GPOs that you want to eliminate, mark it in red to tell yourself you are removing it. If adding an additional column or sheet to notate settings eliminated and why, such as redundant, then feel free to do so! Whatever works for you to keep a good record.

I'll then create a sheet where I document the current OU structure, utilizing the columns and lines to mimic the table design, like this:

Users		
	Chicago	
		VIP
	Seattle	

Now that I have the current configuration planned out. I'll do two new sheets. One to begin outlining the proposed OU design, and another that begins to outline the new GPOs I create from consolidation and cleanup, and where they are linked in the new design.

This method may not be effective if you have a high number of setting variations in your network unless these settings can be patterned. In which case, you may need to evaluate if you can reasonable support such a spread variance of settings, or if you can get the business to accept a consolidated structure to improve administrative management and security.

Security Considerations

From a security standpoint, it has been useful to avoid using the Computers, Users, and Managed Service Accounts OUs and instead building custom OUs for those objects.

By doing so, we can use the default OUs to look for suspicious object creation in our environment. Another honeypot opportunity. Consider setting a strongly limited GPO on computers and users that apply to your default Computers and Users group to limit internet and network access until they are moved to an appropriate OU with rights.

Do not change the default OU within AD's configuration in order to make this method effective.

Privileged users and groups should be separate from your regular users and groups. Tier the OUs if you setup a secure administrative environment. Use GPOs to assign the user rights and avoid explicit permission assignments!

Separating Distribution and Security Groups

To maintain security controls, it is generally advised to keep your distribution groups and security groups separate. While some Administrations mail-enable Security Groups, this can come with unintended consequences and complications in operation as needs change. Some users may only need access to a resource, others may just need to receive emails through the group but should not be able to access files.

Maintaining separate groups may increase administration time but prevents complicated separation later on when requirements change. It reduces the potential for accidental data leaks resulting from managers of groups adding users with the intent of making them part of an email group but providing them access to secured data as well.

Adding security groups to users adds to the SIDs that are part of the user's tokens. As the amount of SIDs in a user token increases, so does their login times as systems process to determine what the user does and does not have access to.

Learn more about groups here:

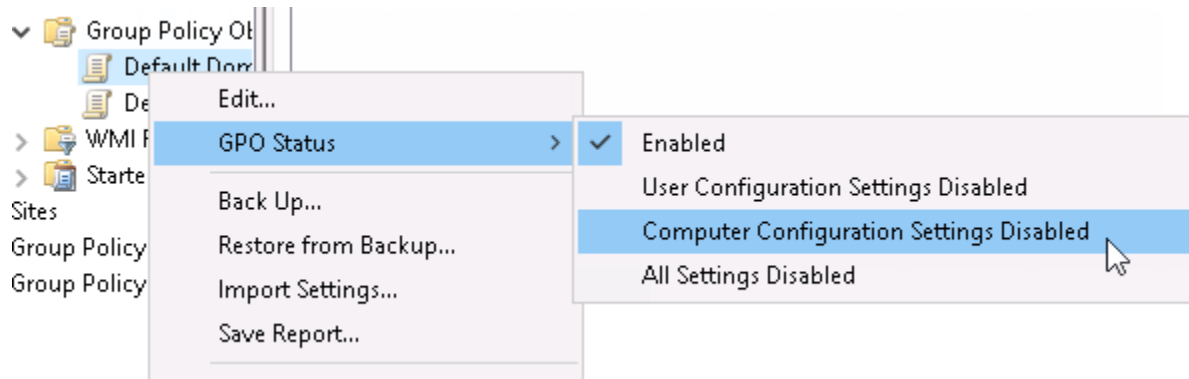
<https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups>

Simplifying Your GPOs

Simplifying your GPOs can reduce login delays and help you better manage your security settings. Overly complicated GPO structures often lead to insecure systems when there is not enough oversight over policy application and associated documentation.

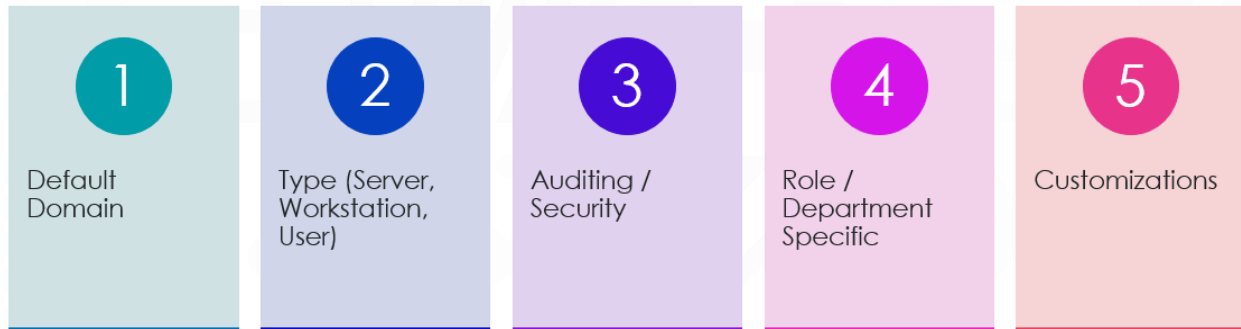
You can separate user and computer settings to ensure that if a computer must be used by multiple users, that the settings specific to them apply. While user settings can be looped back, some computer settings require a system reboot.

For policies that only have user configuration or computer configuration, be sure to change the GPO status. This will reduce how many settings the computer must evaluate in each policy and can improve load time when multiple policies are being used.



Sample GPO Policy Flow Configuration

Below is a sample GPO policy flow I use with clients when considering efforts to consolidate and redesign their Group Policy structure. This may assist in providing ideas for how you can improve how policies work in your environment.



1. **Default Domain** - This should be the bare bones policy that applies to all systems. Remember to avoid changing your de-facto Default Domain Policy and instead create a copy and make appropriate changes.
2. **Type (Server, Workstation, User)** – The type can be broad or specific based on use case in the environment.
3. **Auditing / Security** – This policy can be separate or consolidated partly into your default domain and type GPOs, based on your overall configuration.
4. **Role or Department Specific** – These are policies you usually set to a business unit or group.
5. **Customizations** – These are intended for variations that cannot be applied higher-up and specifically require their own policy.

Modernize Your Authentication

There are several changes you should consider in modernizing the authentication and authorization processes within your network. By default, Microsoft keeps a lot of settings to a lower-level to ensure compatibility.

The majority of settings I note are found under this GPO Path:

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

LDAP Signing and Binding

LDAP signing is particularly important after Microsoft released MSRC Advisory #190023 in early September. LDAP signing will become mandatory by patch in January 2020, so implementing it now while you have time is ideal. I recommend setting each setting listed in order, one per week until completed.

Change Setting – Network Security: LDAP Client Signing Requirements

Check the box for *define this policy setting* and set the policy to *Negotiate Signing*.

Change Setting - Domain Controller: LDAP Server Signing Requirements (1 week later)

Check the box for *define this policy setting* and set the policy to *Require Signing*.

Change Setting – Network Security: LDAP Client Signing Requirements (1 week later)

Set the policy from *Negotiate Signing* to *Require Signing*.

For setting LDAP Channel Binding, please read the following Microsoft KB for the appropriate registry keys: <https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry>

Like the LDAP signing requirements, it is recommended you set the DWORD value to 1 and then evaluate LDAP traffic going to the Domain Controller. Setting the DWORD value to 2 will enforce it outright.

Additional Details: <https://portal.msrm.microsoft.com/en-us/security-guidance/advisory/ADV190023>

Patch Details: <https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirement-for-windows>

Digitally Sign Communication

These settings apply to SMB (Server Message Block) and CIFS (Common Internet File System) traffic. Signing your traffic helps combat man-in-the-middle attacks. If you are using non-Microsoft SMB implementations such as SAMBA, you may want to verify you are running a version compatible with digital signing.

Change Setting – Microsoft Network Server: Digitally Sign Communications (Always)

Check the box for *define this policy setting* and set to *Enabled*.

Change Setting – Microsoft Network Server: Digitally Sign Communications (If Client Agrees)

Check the box for *define this policy setting* and set to *Enabled*.

Change Setting – Microsoft Network Client: Digitally Sign Communications (Always)

Check the box for *define this policy setting* and set to *Enabled*.

Change Setting – Microsoft Network Client: Digitally Sign Communications (If Client Agrees)

Check the box for *define this policy setting* and set to *Enabled*.

SMB Unencrypted Transmission

If you are not using Linux or Unix based file servers that are outdated, consider setting this to avoid cleartext transmission of user credentials across your environment.

Change Setting – Microsoft Network Client: Send unencrypted password to third-party SMB servers.

Check the box for *define this policy setting* and set to *Enabled*.

NTLM Changes

Like SMB, NTLM has its share of legacy components that should be discontinued from use if they are not necessary for proper network or application functionality. If you keep legacy LM and NTLMv1 running in your environment, you leave potential for adversaries to negotiate older authentication protocols more susceptible to man-in-the-middle, hash passing, and other exploitations.

If you need to determine what versions are in use, set the following:

Change Setting – Restrict NTLM: Audit Incoming NTLM Traffic

Check the box for *define this policy setting* and set to *enable auditing for all accounts*.

Change Setting – Restrict NTLM: Audit NTLM authentication in this domain

Check the box for *define this policy setting* and set to *enable auditing for all accounts*.

To observe the results, navigate to the *Microsoft Windows NTLM / Operational log* under Application and Services logs in event viewer and look for Event ID 8004 that records NTLM authentication and the type.

If you have enabled logon auditing as detailed later in this document, Event ID 4624 in the security log should also record the authentication protocol and version.

Once you have determined that NTLMv1 or lower is not in use, you can unset the audits and change the authentication level of the domain as noted below.

Change Setting – LAN Manager Authentication Level

Check the box for *define this policy setting* and set to the highest setting possible, if you can, which is *Send NTLMv2 response only. Refuse LM & NTLM*.

If your environment is no longer using NTLM (any version), or only a few systems are, then consider blocking NTLM level authentication from your environment all together.

Details on how to perform this is provided here:

<https://blogs.technet.microsoft.com/askds/2009/10/08/ntlm-blocking-and-you-application-analysis-and-auditing-methodologies-in-windows-7/>

Require SSL and 128-Bit Encryption for NTLM SSP

If you are running an environment where Windows 7 and Server 2008 R2 or higher is in use, then just set these and move on. If not, you will need to upgrade your environment.

You should make this changes in conjunction with your increase in NTLM settings earlier mentioned.

Network Security: Minimum session security for NTLM SSP based (including secure RPC) clients

Check the box for *define this policy setting* and check both boxes for *Require NTLMv2* and *Require 128-bit encryption*.

Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers

Check the box for *define this policy setting* and check both boxes for *Require NTLMv2* and *Require 128-bit encryption*.

Other Settings to Consider Enabling

Here are some other settings not mentioned during the talk that may be of benefit to your environment. As always, test before fully applying across your environment. Additional details on these settings may be posted at a later date on my website, www.syntaxbearror.io.

Network Security: Configure Encryption Types Allowed for Kerberos

AES_128_HMAC_SHA1

AES_256_HMAC_SHA1

Future Encryption Types

Network Security: Do not store LAN Manager hash value on next password change.

Enabled

Elevating Your Passwords

This guidance does not supersede the basics of change your passwords regularly but is intended to focus on settings and passwords commonly forgotten or misplaced.

DSRM Password

Your DSRM password is the literal keys to the database of your realm. In event of a disaster, you'll need this password to restore the environment or booting into the recovery console. This password should be changed regularly as passwords can be cracked. I recommend storing this password non-digitally to ensure that it is available in a disaster.

To change the DSRM Password

1. Open an administrative PowerShell or Command Prompt from your PDC.
2. Type *ntdsutil* and press enter.
3. At the *ntdsutil* command prompt, type *set dsrm password*.
4. At the DSRM command prompt, type one of the following lines:

To reset the password on the server on which you are working, type *reset password on server null*. The null variable assumes that the DSRM password is being reset on the local computer. Type the new password when you are prompted. Note that no characters appear while you type the password.

-or-

To reset the password for another server, type:

reset password on server servername, where *servername* is the DNS name for the server on which you are resetting the DSRM password. Type the new password when you are prompted. Note that no characters appear while you type the password.

5. At the DSRM command prompt, type *q*.
6. At the *Ntdsutil* command prompt, type *q* to exit.

For more details on changing the DSRM Administrator password, please visit:

<https://support.microsoft.com/en-us/help/322672/how-to-reset-the-directory-services-restore-mode-administrator-account>

Implement LAPS (Local Administrator Password Solution)

LAPS helps administrators manage the local administrator accounts on workstations and servers. These passwords are often replicated and never changed or set in GPOs which can be stolen and used to gain unauthorized access.

Use the below links for additional information and how to deploy in your environment.

Additional Details: <https://support.microsoft.com/en-us/help/3062591/microsoft-security-advisory-local-administrator-password-solution-laps>

Step by Step Deployment Guide: <https://gallery.technet.microsoft.com/Step-by-Step-Deploy-Local-7c9ef772/file/150657/1/Step%20by%20Step%20Guide%20to%20Deploy%20Microsoft%20LAPS.pdf>

To download: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>

Disable the Storage of LM Hashes

LM hashes are well known susceptible to various attacks to gain the plain text version of the password. These hashes are often no longer in use in environments, but they remain getting generated and stored provided the password is under 15 characters in length.

While the below setting will prevent new LM hashes from being generated, it will take some time to clear them from the AD database.

To make this change, go to this location in your Default Domain Policy:

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

Modify the following:

Network Security: Do not store LAN Manager hash value on next password change.

Check the box for *define this policy setting* and set to *Enabled*.

Change the KRBTGT Account Password Annually

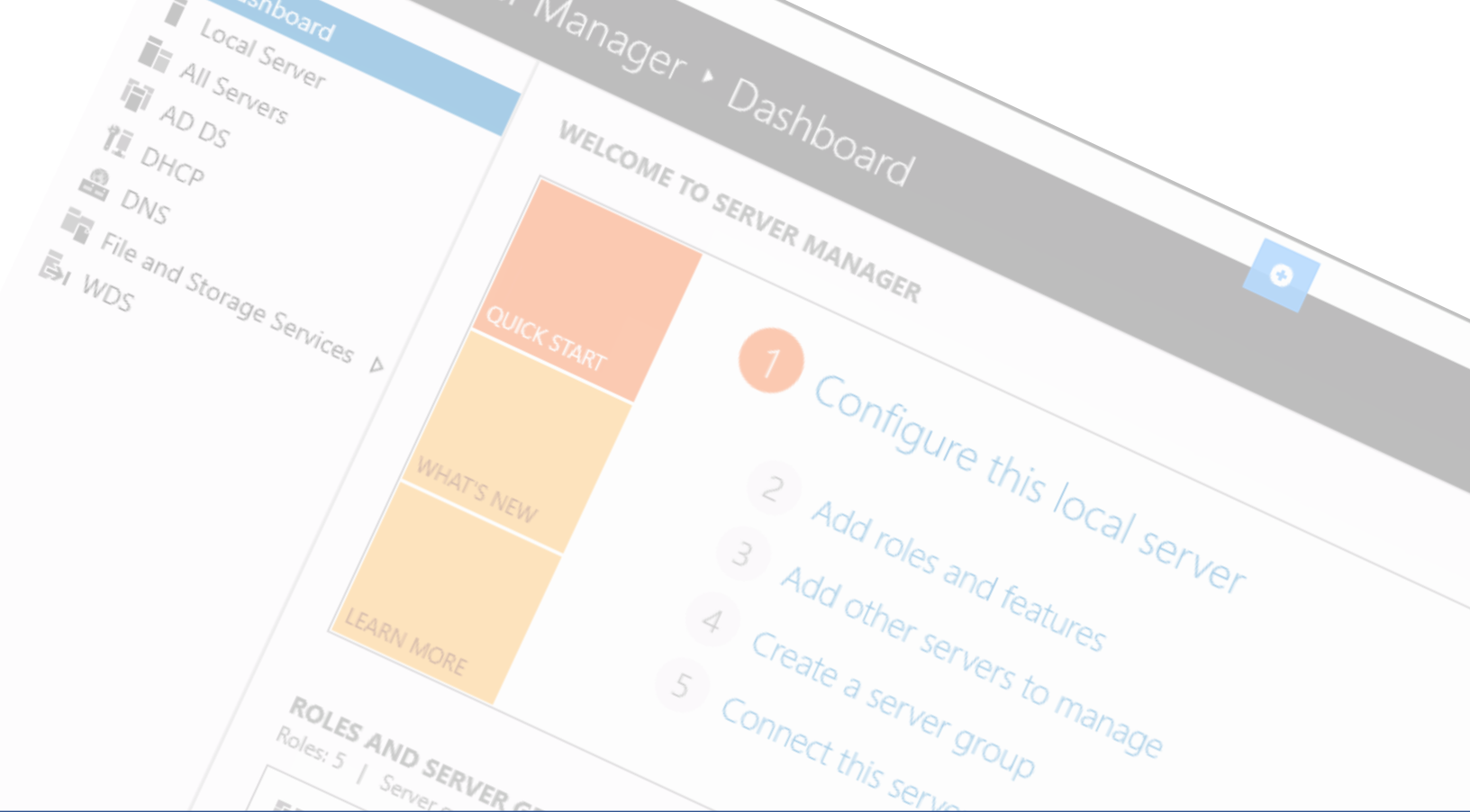
The KRBTGT password is used by the Kerberos service to derive symmetric keys that encipher Ticket Granting Tickets (TGT) which are used as part of the Kerberos authentication protocol.

It is now recommended to change this password annually or when a Domain Administrator has departed. The general process is to change the password, wait a day, then change it again.

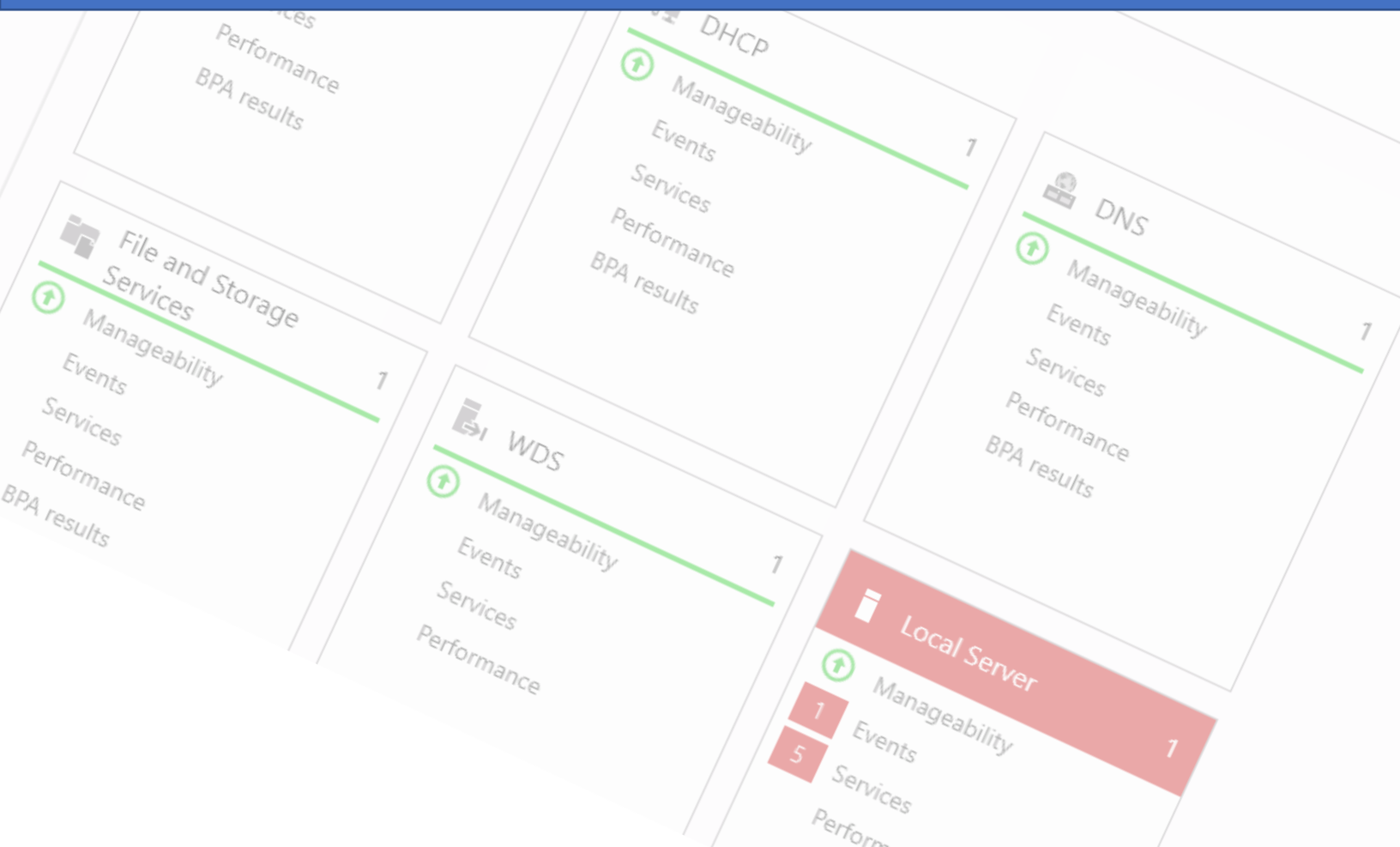
Here are two methods to perform this change:

Method 1: <https://www.microsoft.com/security/blog/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/>

Method 2: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password>



Managing, Monitoring, and Auditing Active Directory



Managing Beyond the DC

There are two ways to manage Domain Controllers beyond logging into them directly.

Remote Server Administrative Tools (RSAT)

RSAT is a collection of administrative tools that Microsoft provides that allows you to manage various Windows Server roles and features from a Windows 7 SP1 or newer PC.

Starting with Windows 10 October 2018 Update, RSAT is included as a set of **Features on Demand** in Windows 10 itself.

For Details on the RSAT tools via Features on Demand on Windows 10, please visit:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-server-administration-tools#install-uninstall-and-turn-offon-rsat-tools>

For download details and the full tools available in RSAT, please visit:

<https://support.microsoft.com/en-us/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems>

PowerShell

There are two methods within PowerShell that you can use to administer Active Directory.

Method 1 – PS Module

After installing RSAT tools, you can use the command: `Import-Module ActiveDirectory` and run Active Directory related PowerShell commands as you would on a DC.

Method 2 – Remote PS Session

If you prefer to create a remote session to a Domain Controller, you can use the following commands, substituting `<Server>` with the name of the Domain Controller. To exit out of a PS Session, just type `exit` and press enter.

`Enter-PSSession -ComputerName <SERVER>`

Using Different Credentials?

`$mycred = Get-Credential`

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

For additional details on using `Enter-PSSession`, visit:

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/enter-pssession?view=powershell-6>

Setting Up Auditing

Use group policy to define your audit settings to maintain a more consistent application. Remember to consider how broad each policy should apply to reduce the potential risk of repeating settings.

It's recommended that you set audit settings by category for more granular control over what is being recorded. You can turn that on by going to:

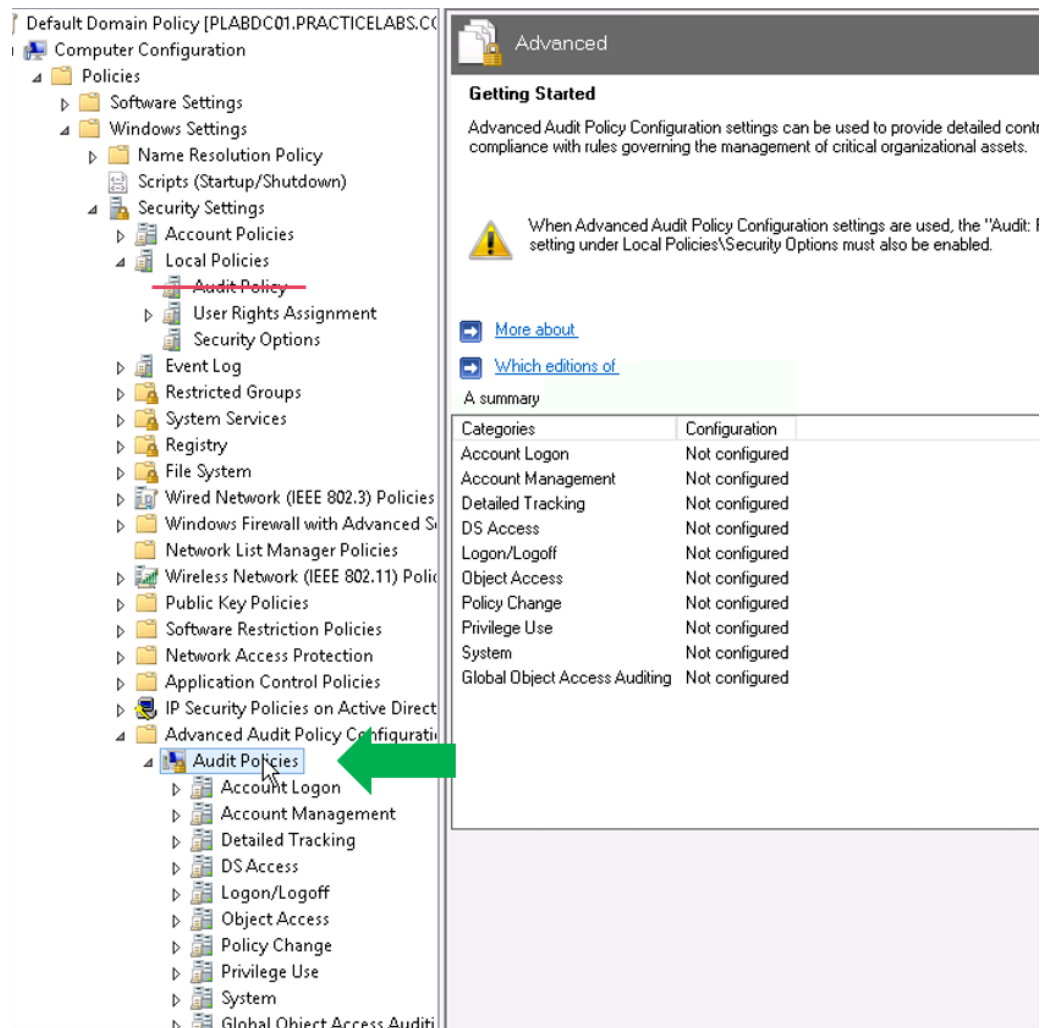
Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options

Change This Setting – Audit: Force Audit Policy Subcategory Settings...

Check the box next to *define this audit setting* and choose *Enabled*.

Your audit settings should reflect what you are required to record to meet compliance requirements, but enough to provide your IT technicians with the right information.

The following few pages will detail out each audit category, what the suggested settings should be for an ideal environment, along with the associated Event IDs and their purpose.



The screenshot shows the Group Policy Editor window. The left pane displays the tree structure: Default Domain Policy [PLABDC01.PRACTICELABS.CO] > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > **Audit Policy** (highlighted with a red line). Below this, the 'Audit Policies' subcategory is expanded, showing a list of audit categories. A green arrow points to the 'Audit Policies' subcategory. The right pane shows the 'Advanced' tab for the 'Audit Policy' settings. It includes a 'Getting Started' section with a warning icon and text: 'When Advanced Audit Policy Configuration settings are used, the "Audit: Force Audit Policy Subcategory Settings..." setting under Local Policies\Security Options must also be enabled.' Below this are links for 'More about' and 'Which editions of'. A summary table is also present.

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

Understanding Audit Guidance

Audit Event	Event IDs	Success	Failure
Bad Guy Audit	5911	Yes	Yes
Good Guy Audit	5912	Yes	No

Initial audit details for each category are presented in a table as shown in the sample above and broken down by: Event Name, Event ID, and the suggested settings for success and failure.

An asterisk (*) next to a value indicates that it may or may not offer a benefit.

A hyphen (-) under success or failure indicates no guidance is available for the value.

For further details on any of the audit events please click on their names to be directed to the Microsoft Docs page about that event.

A short descriptive detail will follow below the table explaining how the event benefits you.

If you are low on space, failure tracking can be considered optional, but this may make it difficult to identify an attack that may have been attempted. From my own personal experience, I don't recommend this unless otherwise noted.

*** Please consult your compliance or legal team regarding any required auditing that may be necessary for your organization that may not be covered by this document. ***

Audit Category: Account Logon

Audit Event	Event IDs	Success	Failure
Audit Credential Validation	4774 - 4777	Yes	Yes
Audit Kerberos Authentication Service	4768, 4771 - 4772	Yes	Yes
Audit Kerberos Service Ticket Operations	4769, 4770, 4773	Yes	Yes
Audit Other Account Logon Events	Not Defined	Yes*	Yes*

Credential Validation and **Kerberos Authentication Service** audits provide us with details about user logon requests. This allows us to find brute force attempts, account enumeration, and account compromise.

Kerberos Service Ticket Operations allows us to record tickets requested. This allows us to track user activity through the network as they are used to gain access to protected resources.

Other Account Management Events are not currently defined by Microsoft, but to ensure you get data when it does get defined, you may want to set it to Yes.

Audit Category: Account Management

Audit Event	Event IDs	Success	Failure
Audit Application Group Management	4783 - 4792	-	-
Audit Computer Account Management	4741 - 4743	Yes	Yes
Audit Distribution Group Management	4744 – 4753, 4759 - 4763	Yes *	No
Audit Other Account Management Events	4782, 4793	Yes	Yes
Audit Security Group Management	4727, 4731 – 4735, 4764, 4799	Yes	Yes
Audit User Account Management	4720, 4722 – 4726, 4738, 4740, 4765 – 4767, 4780 – 4781, 4794, 4798, 5376, 5377	Yes	Yes

Application Group Management is deprecated as of Windows Server 2012 and was generally used for audits against Authorization Manager.

Computer Account Management audits the activity against a computer object in AD.

Distribution Group Management audits the activity against a distribution group in AD.

Other Account Management Events tracks whether the password hash of a user account was accessed, or a password audit was called.

Security Group Management audits the activity against a security group in AD.

User Account Management audits the activity against a user object in AD.

Audit Category: Detailed Tracking

Audit Event	Event IDs	Success	Failure
Audit DPAPI Activity	4692 – 4695	-	-
Audit PnP Activity (10/2016)	4616, 4619 – 4624	Yes	No
Audit Process Creation	4688, 4696	Yes	Yes *
Audit Process Termination	4689	-	-
Audit RPC Events	5712	-	-

DPAPI Activity is for when encryption or decryption calls are made into the data protection application interface (DPAPI). It is not something often tracked.

PnP Activity is new for Windows 10 / Server 2016 or higher and allows you to track changes with external hardware through Plug n Play.

Process Creation tracks who and what spawned a process, the associated process ID and when.

Process Termination tracks what terminated a process, its associated ID, and when.

RPC Events tracks when an inbound remote procedure call is attempted.

Audit Category: DS Access

Audit Event	Event IDs	Success	Failure
Audit Detailed Directory Service Replication	4928 – 4931, 4934 - 4937	Yes *	-
Audit Directory Service Access	4661 - 4662	Yes	Yes
Audit Directory Service Changes	5136 – 5139, 5141	Yes	Yes
Audit Directory Service Replication	4932 - 4933	Yes *	-

Detailed Directory Service Replication tracks replication activity between domain controllers or applications seeking to replicate AD. While this is considered informational, there are ways to steal account details through fraudulent replication activities, so consider tracking if you can.

Directory Service Access tracks when an object is accessed from AD.

Directory Service Changes tracks of changes to objects in AD.

Directory Service Replication tracks when replication starts and ends between devices. This is considered informational and generally used for diagnostics.

Audit Category: Logon and Logoff

Audit Event	Event IDs	Success	Failure
Audit Account Lockout	4625	Yes	No
Audit User / Device Claims	4626	-	-
Audit Group Membership (10/2016)	4627	Yes	-
Audit IPsec Extended Mode	4978 - 4984	-	-
Audit IPsec Main Mode	4646, 4650 – 4655, 4976, 5049, 5453	-	-
Audit IPsec Quick Mode	4977, 5451 - 5452	-	-
Audit Logoff	4634, 4647	Yes	No
Audit Logon	4624 – 4625, 4648, 4675	Yes	Yes
Audit Network Policy Server	6272 - 6280	Yes *	Yes *
Audit Other Logon / Logoff Events	4649, 4778 – 4779, 4800 – 4803, 5378, 5632 - 5633	Yes	Yes
Audit Special Logon	4672, 4964	Yes	Yes

Account Lockout tracks when accounts are locked out.

User / Device Claims tracks resource audits on local systems. You generally do not want this on for your Domain Controllers but may want to consider it for your workstations or file servers.

Group Membership is new for Windows 10 and Server 2016 or higher, and tracks when a group membership is enumerated on a client system and what group information is obtained in a user's logon token.

IPSec Extended, Main, and Quick Mode all track events generated by Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP). It is generally considered diagnostic but the IPSec Main Mode may be useful for tracing or monitoring IPSec activity.

Logoff and **Logon** track basic user logon activity.

Network Policy Server tracks activity generated by Radius and Network Access Protection (NAP)

Other Logon / Logoff Events tracks remote desktop sessions, workstation lock and unlock, screen save invocation or dismissal, replay attacks, wireless network, or 802.1x network authentication.

Special Logon tracks when processes get elevated permissions with users who have administrator-equivalent permissions, and track logons by a defined special group.

To define the special group(s) in registry, you need to modify the following key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Audit
SpecialGroups=<REG_SZ semicolon-separated SID value list>
```

To learn more on the registry setting and how to obtain and define a SID list, please visit:

<https://blogs.technet.microsoft.com/askds/2008/03/11/special-groups-auditing-via-group-policy-preferences/>

Audit Category: Policy Change

Audit Event	Event IDs	Success	Failure
Audit Audit Policy Change	4670, 4715, 4719, 4817, 4902, 4904 – 4908, 4912	Yes	Yes
Audit Authentication Policy Change	4670, 4706 – 4707, 4713, 4716 – 4718, 4739, 4864 – 4867	Yes	Yes
Audit Authorization Policy Change	4703 – 4705, 4670, 4911, 4913	-	-
Audit Filtering Platform Policy Change	4709 – 4712, 5040 – 5048, 5440 – 5444, 5446 – 5450, 5456 – 5468, 5471 – 5474, 5477	Yes *	Yes *
Audit MPSSVC Rule-Level Policy Change	4944 - 4958	Yes	-
Audit Other Policy Change Events	4714, 4819, 4826, 4909 – 4910, 5063 – 5070, 5447, 6144 - 6145	-	-

Audit Policy Change tracks changes made to audit policies.

Authentication Policy Change tracks creation, modification, and removal of forest and domain trusts, changes to Kerberos under Account Policies in a GPO, and in general, tracking changes in domain-level and forest-level trust and privileges granted to user accounts or groups.

Authorization Policy Change tracks assignment and removal of user rights in user right policies.

Filtering Platform Policy and **MPSSVC rule-level Policy Change** tracks changes to Microsoft Protection Services and the Windows Firewall.

Other Policy Change Events tracks various other events with EFS Data Recovery Agent policies, the Windows Filtering Platform, Security Policy for local systems, Central Access Policy and Cryptographic Policies. These events can get rather frequent when Windows Firewall is enabled.

Audit Category: System

Audit Event	Event IDs	Success	Failure
Audit IPsec Driver	4960 – 4963, 4965, 5478 – 5479, 5480, 5483 - 5485	Yes	Yes
Audit Other System Events	5024 – 5030, 5032 – 5037, 5058 – 5059, 6400 - 6409	-	-
Audit Security State Change	4608, 4616, 4621	Yes	Yes
Audit Security System Extension	4610 – 4611, 4614, 4622, 4697	Yes	Yes
Audit System Integrity	4612, 4615, 4618, 4816, 5038, 5056, 5062, 5057, 5060 – 5061, 6281, 6410	Yes	Yes

IPSec Driver tracks events generated by the IPSec driver such as startup and shutdown of the service, network packet drops, and packets with incorrect security parameters. It is nice to have enabled if you use IPSec in your environment.

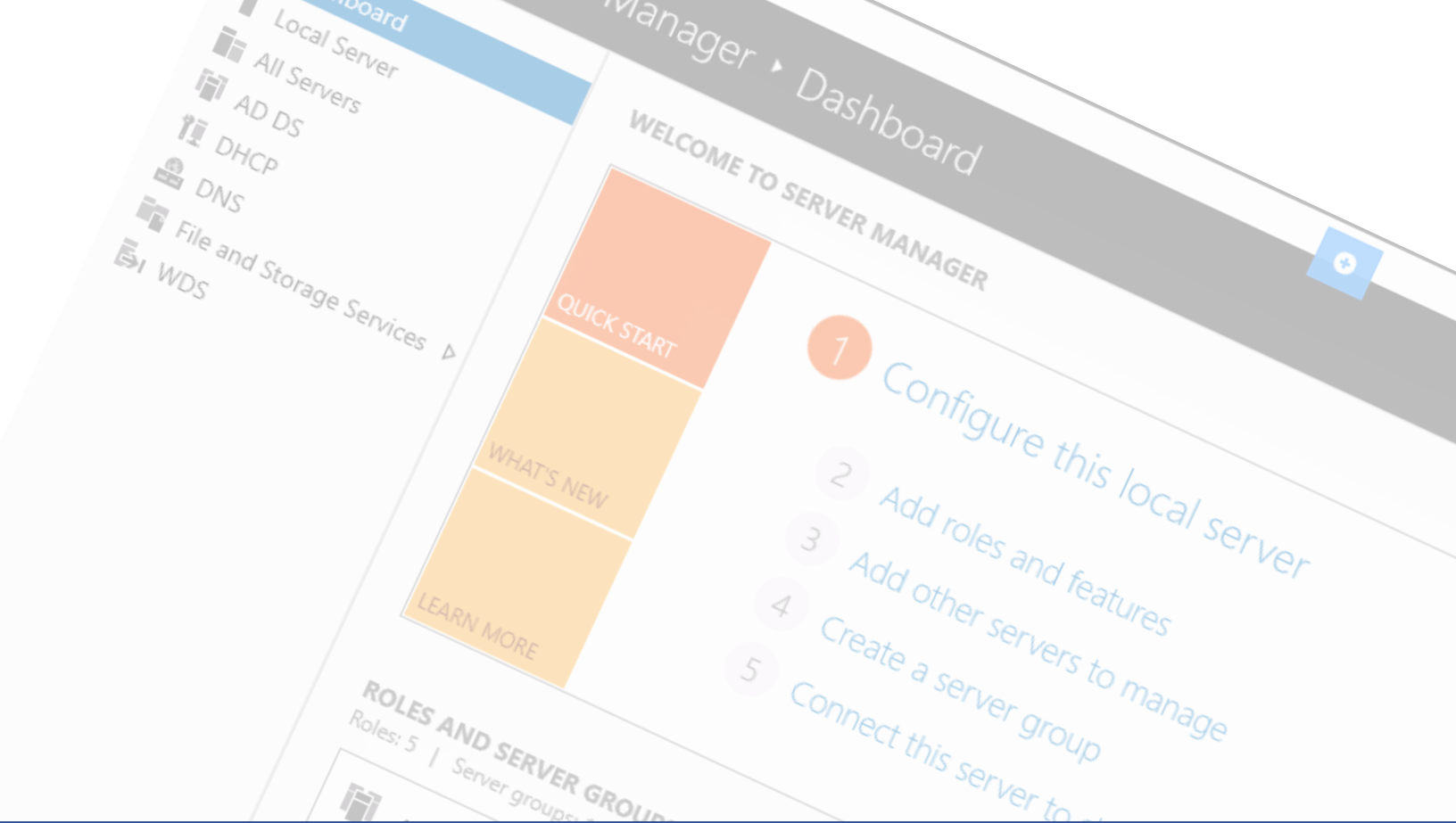
Other System Events tracks security policy processing by Windows Firewall, BranchCache changes, crypto operations, and state changes in the Windows Firewall driver and service.

Security State Change contains startup, recovery, shutdown, and tracks system time changes.

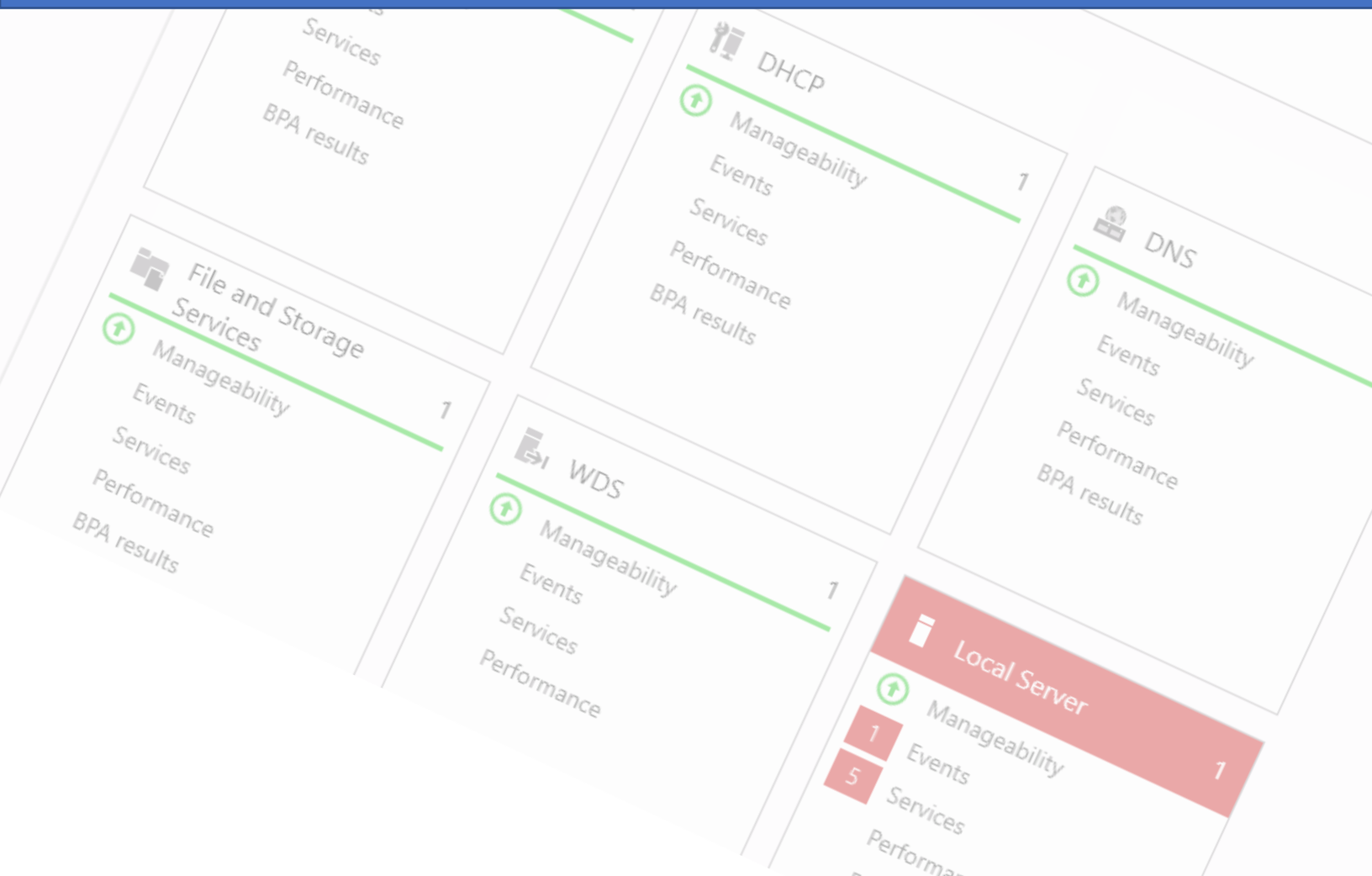
System Integrity tracks audit failures, invalid local procedure calls to impersonate a client, replies or writes to a client address space, RPC calls that lose integrity, an invalid hash on an executable is detected, or cryptographic tasks are performed.

Audit Categories: Global Object Access Auditing, Object Access, and Privilege Use

These audit categories have no suggested settings for Domain Controllers but may be used for other types of systems.



Identifying Suspicious Activity



System Logs

System logs are your greatest source of information once you level up your security and auditing around your domain controllers.

While Windows has a considerable number of logs at your fingertips, there are a few I prefer to use in my everyday for auditing, investigations, and remediation.

All logs beyond Security and System noted in the below table will be located under Application and Services Logs in the Event Viewer.

Log Name	Purpose
Security Log	This is where your audit data we defined earlier generally records to.
System Log	Allows us to identify time changes, system state changes like startup and shutdown, driver changes, and service state changes.
Directory Service	This log helps us track entries regarding directory synchronization, replication, and overall errors.
Windows PowerShell	This log keeps track of PowerShell behavior in our environment.
Microsoft > Windows > App Locker	This can help us find what was and was not run if AppLocker is in use.
Microsoft > Windows > PowerShell	Provides additional verbose data for PowerShell tracking, including connection information.
Microsoft > Windows > Windows Firewall w/ Advanced	Provides us with data on how our rules are running, what connections were approved or denied. This requires that logging is enabled on Windows Firewall.

Log Management Tips

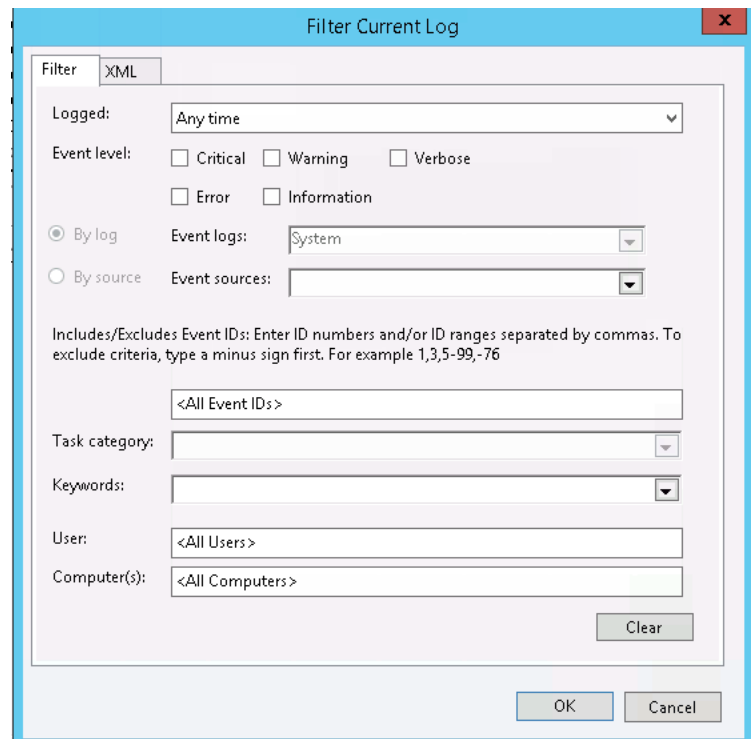
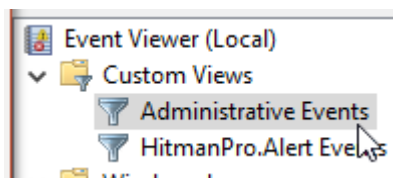
Here are some tips that can help you maximize the most out of your log management that I have found useful in my travels.

- Define the maximum size of your Application, Security, and System event logs via GPO. You can find these settings under:
Computer Configuration > Policies > Windows Settings > Security Settings > Event Log
- Changing the size of any of the Application and Service logs require manual change through the Event Viewer.
- Do not allow your logs to get larger than 4 GB in size (4,194,304 kilobytes) as this will impact the performance of your system and lead to login issues.
- Do not allow the size of your logs to exceed the available RAM on your Domain Controllers as this can impact performance. If you have under 4 GB of RAM on your Domain Controllers, you have bigger problems.
- Set your retention method to *As Needed*.
- Use a PowerShell script to clear out the archive folder after a specified amount of days.
- Forward your logs whenever possible whether that is a copy of the archives or streaming the events through Windows Event Forwarding. This also helps maintain the integrity of the data.

GUI Searching Tips for Event Viewer

Here are some tips for making the most of the *Filter Current Log* action logs available in the event viewer.

- When searching security logs, you can filter successful or failed events by using the dropdown for *keywords* and selecting **Audit Failure** or **Audit Success**.
- The user field requires a match for an existing domain user such as: *Domain\Username*. For more abstract searches, use the *Find* tool on the action bar instead.
- When in doubt or results are blank, use the Find tool on the action bar.
- *Create Custom Views* for frequent searches by using the associated action on the action bar or if you have an existing filter on a log, the action to *Save Filter to Custom View* should be available to click on the action bar.



- Use the *Administrative Events* Custom View that comes default to review errors and warnings that may indicate a system issue or other suspicious activity.

Searching via PowerShell

PowerShell can be a great tool to help you search event logs. You want to run event log searches in an Administrative PowerShell window.

Get-EventLog –List

This command will list the available logs to you. From there, you can replace <log> in the command noted below to retrieve the entries associated with that log.

Get-EventLog –LogName <Log>

This is the basic part of the command to retrieve the contents of a particular log. You can further manipulate your results with these additional parameters:

-Newest

Replace # with the amount of records you are looking for.

-EntryType <Error,Warning,FailureAudit,SuccessAudit>

If you are only looking for a particular type of entry, use the EntryType option.

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

If you are looking for a user, or part of a username, you can use the UserName parameter to search along with * for wildcards.

-Message <*description*>

If you remember part of the event information, use this parameter to search for it.

| Export-CSV –Path <Path and CSV Detail> -NoTypeInfo

If you want to export your results to CSV, pipe this command, and replace <path and csv detail> with the name or path and name of your target CSV. (Eg: C:\result.csv or result.csv)

Sample Command

Here is a command I use for searching for modifications made to security or distribution groups and exporting the data to CSV.

```
Get-EventLog –LogName Security | Where-Object {($_.eventid –eq 4732 –or ($_.eventid –eq 4733) –or ($_.eventid –eq 4746))} | Select EventID, MachineName, EntryType, Message, InstanceId, TimeGenerated, Timecreated, UserName | Export-CSV search.csv
```

For additional cmdlet guidance, please visit:

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-eventlog?view=powershell-5.1>

Look for Sessions

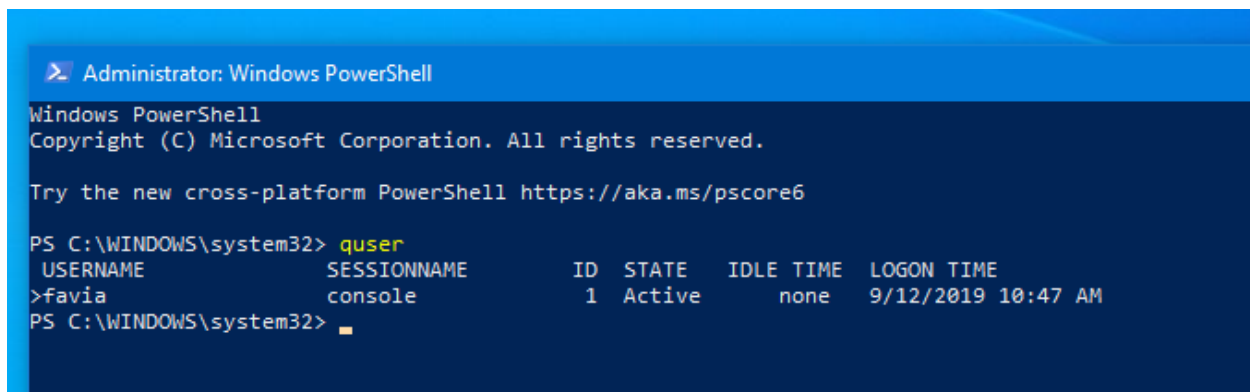
Stale sessions auditing can be something you do daily or whenever you feel is appropriate for your environment. When sessions are left in a disconnected or inactive state, they keep their credentials in memory.

Given the steady increase in CPU and memory related exploits, having credentials persist in memory provides a chance for malicious actors to gain access to them. While Windows 10 has increased the security of credential in memory, it should not be used as a reason to not maintain healthy sessions.

You can run the below command in an administrative PowerShell or Command Shell prompt. Replace *<System Name>* with the name of the computer you are targeting.

`quser /server <System Name>`

A PowerShell script to run this against your environment for all workstations or servers can be found on www.pshell.dev.



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

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

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>
```

If a computer does not respond to this or other commands, you may need to Allow Remote RPC commands. This is a task I've had to do time to time in Windows 7 environments.

To alter the key, run the following PowerShell command on the local system.

`set-itemproperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server' -Name AllowRemoteRPC -Value 0x1`

Alternatively, you can set this via GPO and push it to systems. If you push it via GPO, set the value to 1. No reboot should be required for the setting to apply once the system updates its GPO.

Session Management problems?

A tool I've deployed at various locations before is called Lithnet Idle Logoff. It's a lightweight application that will force an idle session to be logged off after a specified amount of time, configurable by GPO through ADMX files. For more details please visit: <https://github.com/lithnet/idle-logoff>

Develop a Daily Routine

Developing a daily routine can be a good way to get familiar with your environment and begin to spot irregular or suspicious activity that may have occurred between your last review.

Depending on the nature of your environment, looking for suspicious user changes after hours may help you get a lead on a compromised account. For other environments, this could be expected behavior.

Here are some common things to consider evaluating on a regular basis in AD:

- New or Modified Accounts
- Changes to Privileged Accounts and Groups
- Password Changes (outside typical hours)
- Logins to Special Accounts (Like the Domain Administrator account, if it isn't in regular use).
- Group Policy modifications

Many of these can be tracked via PowerShell by keeping tabs on the event IDs associated with these actions. Review the Searching via PowerShell page for additional guidance on example commands.

If you prefer a GUI method of searching, please review the next few pages on system logs and the event viewer.

I will also post various support scripts that assist in reviewing the above, and other common activity periodically at my website www.pshell.dev.

Additional Resources

Here are some additional resources that compliment what was discussed during the panel and to further your knowledge and skills.

Other Best Practice Resources

Windows Server Best Practices for Securing Active Directory

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>

Audit Practice Recommendations

<https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

Windows 10 and Server 2016 Auditing and Monitoring Reference

<https://www.microsoft.com/en-us/download/details.aspx?id=52630>

Microsoft Windows 10 Security Guidance for Enterprises

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-compliance>

Other Security Settings to Consider

AppLocker Functionality

<https://www.rootusers.com/implement-applocker-rules/>

LLMNR and NBT-NS Attack Mitigation

<https://cccsecuritycenter.org/remediation/llmnr-nbt-ns>

Understanding User Rights

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh125917\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh125917(v=ws.10))

Other Auditing / Tracking Measures to Consider

Monitoring What Matters – Windows Event Forwarding for Everyone (Even if you already have a SIEM)

<https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/>

Sysmon Configuration for High-Quality Event Tracing

<https://github.com/swiftonsecurity/sysmon-config/>

Windows Event Forwarding: The Survival Guide

<https://social.technet.microsoft.com/wiki/contents/articles/33895.windows-event-forwarding-survival-guide.aspx>

Azure AD

Deploying Azure AD Password Protection

<https://aka.ms/deploypasswordprotection>

Protecting against password spray attacks on Azure AD

<https://aka.ms/PasswordSprayBestPractices>

Administrator Roles by Admin Task

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task#multi-factor-authentication>

Educational & General Knowledge Resources

Active Directory Attribute Recovery with PowerShell

<https://blogs.technet.microsoft.com/ashleymcglone/2014/04/24/oh-snap-active-directory-attribute-recovery-with-powershell/>

Advanced Security Auditing FAQ

<https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq>

Domain Controller Cloning via Hyper-V

<https://blogs.technet.microsoft.com/canitpro/2013/06/11/step-by-step-domain-controller-cloning/>

Enabling Restricted Administrative Mode for Remote Desktop Services

<https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx>

Introduction to Active Directory Administrative Center Enhancements (Level 100)

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100->

The differences between NTLM authentication and Kerberos

<https://www.windows-active-directory.com/tag/difference-between-ntlm-and-kerberos-authentication>

Threats and Countermeasures Guide – Security Options in GPO

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh125918\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/hh125918(v=ws.10))

Threats and Vulnerability Mitigation Guide (Serv 2008 – Older, but still useful)

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755181\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755181(v=ws.10))

Well Known Security Identifiers in Windows OS

<https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems>

Enabling Restricted Administrative Mode for Remote Desktop Services

<https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx>

Other Good Resources

<https://www.adsecurity.org>

<https://www.rootusers.com/>

<https://www.active-directory-security.com/>

<https://www.ultimatewindowssecurity.com/>

<https://secureinfra.blog/>

<https://blog.harmj0y.net/>

<http://www.rebeladmin.com/>

Copyright, Legal Disclaimer, and Contact Information

Copyright

©2019 Christopher Clai (www.syntaxbearror.io). This document is intended for distribution as part of a talk at SpiceWorld 2019 in Austin, TX and cannot be used for commercial purposes. You are free to distribute this in its entirety only with the copyright and disclaimer intact provided.

Additional content, links, and images are property their respective owners.

Legal Disclaimer

This document provides best practices and information gathered from personal and professional experience in the field. The use of this does not imply a formal agreement of services has been entered between the reader or attendee, and the presenter.

Use the information provided in this document at your own risk. There is no expressed or implied warranty.

Use of company and product names do not imply endorsement.

Feedback?

Please send your feedback to Christopher Clai at chris.clai@ieee.org.