ADVANCED WINDOWS AUDITING

Introduction

Many organisations have insufficient visibility of activity occurring on their workstations and servers. Good visibility and detection of what is happening on an organisation's Windows hosts are essential for conducting an effective investigation. It is increasingly difficult to detect malicious activity, which makes it extremely important to monitor and collect log data from as many useful sources as possible.It also aids incident response efforts by providing critical insights into the events relating to a cyber security incident and reduces the overall cost of responding to incidents. Many SIEM systems handle different types of event logs when it comes to Windows.

In addition, Logsign aggregates and normalizes different messages from Windows sources above 400, so that you can even parse the most specific system events and correlate them with other user actions. Logsign's extensive Windows Audit capacity is increasing at the same rate as Windows products evolve and customer needs grow. This document has been developed by Logsign as a guide for the setup and configuration of Windows event logging. This advice is also designed to complement existing HIDS/NIDS systems.

Event log retention

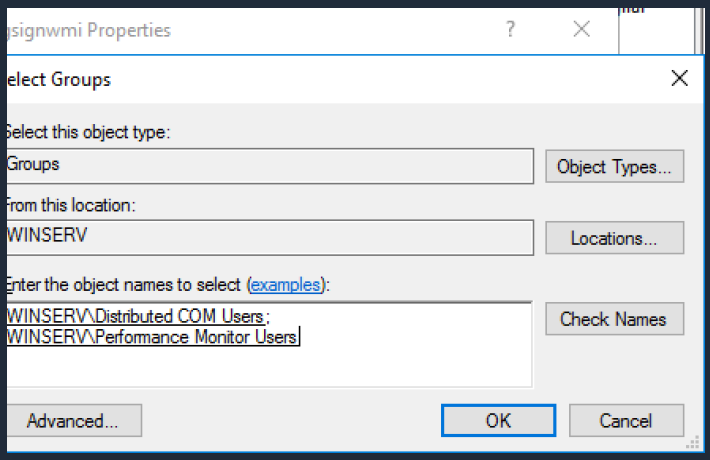
The Windows default settings have log sizes set to a relatively small size and will overwrite events as the log reaches its maximum size. This introduces a risk as important events could be quickly overwritten. To reduce this risk, the Security log size needs to be increased from the default file size of 20 MB. Log size requirements are specified in the table.

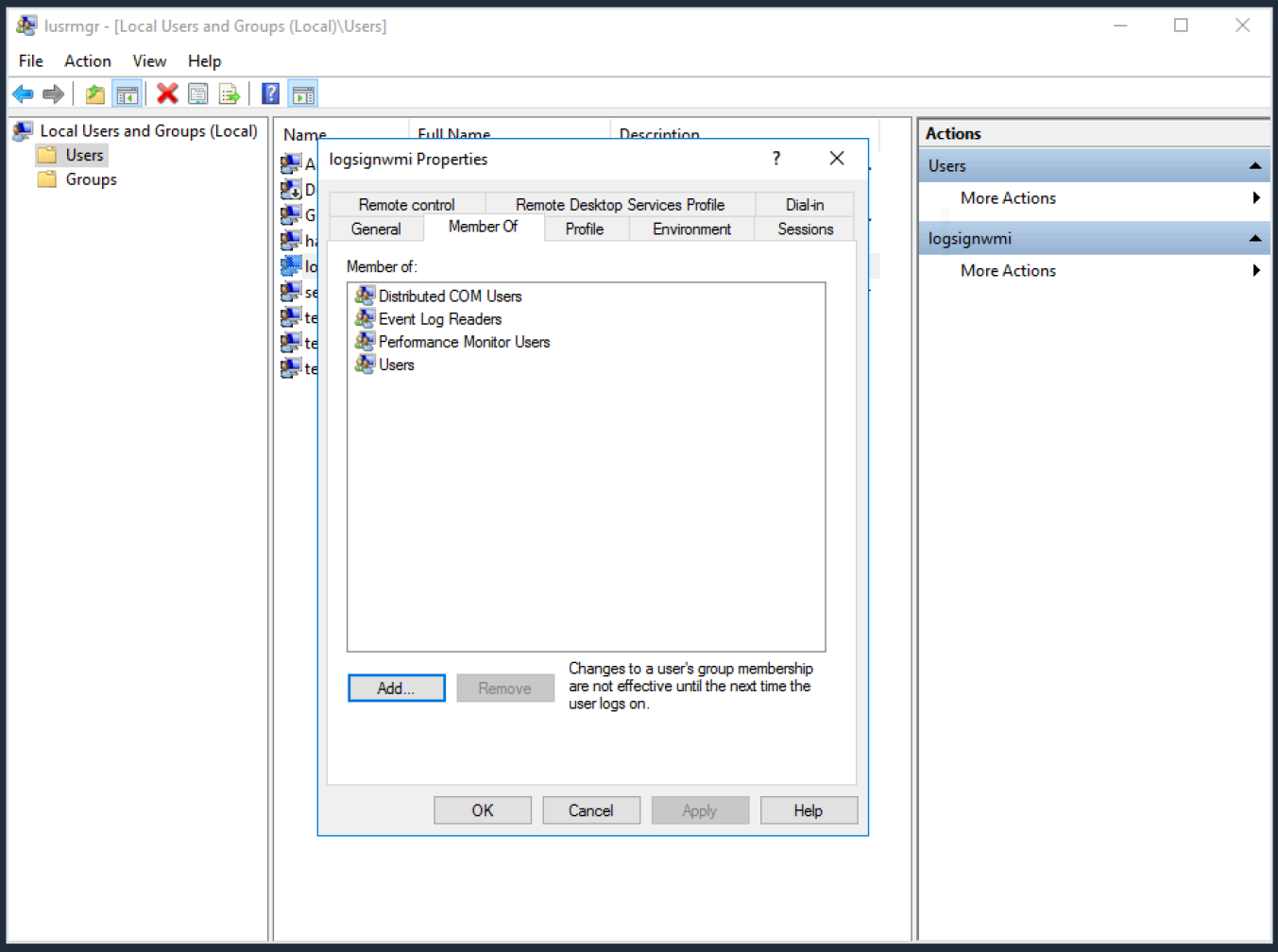
Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application	
Specify the maximum log file size (KB)	**Enabled** Maximum Log Size (KB): 65536
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security	
Specify the maximum log file size (KB)	**Enabled** Maximum Log Size (KB): 2097152
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System	
Specify the maximum log file size (KB)	**Enabled** Maximum Log Size (KB): 65536

Configuring Windows

In any case you should configure a non-admin user for WMI monitoring. Do not use an administrator account for WMI monitoring of Windows for security reasons. Do not use the administrator account in a productive environment,use it only for testing.

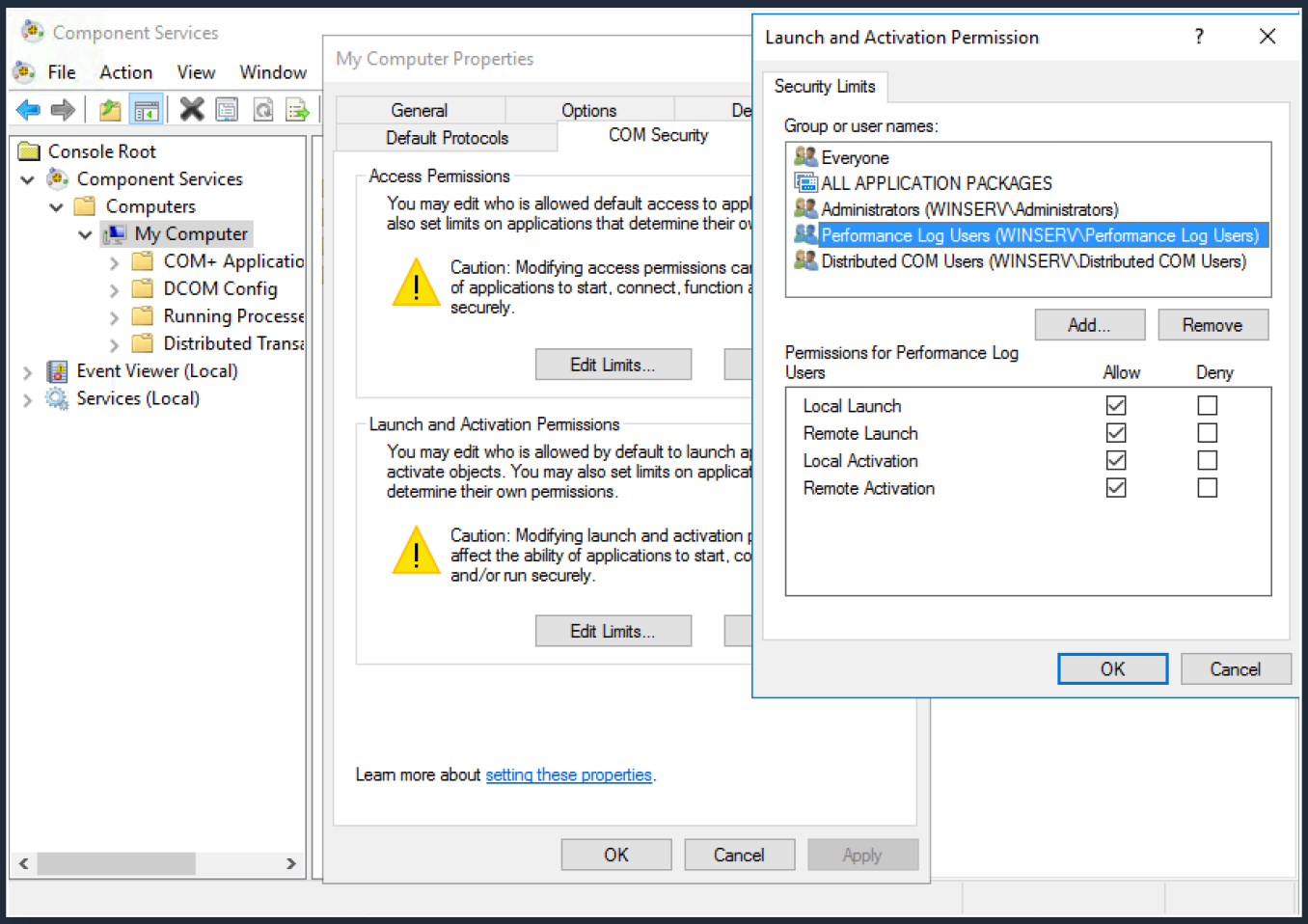
1. Click Start > Run..., type **lusrmgr.msc** and click OK.
2. In the **Users** folder, right click the user to bring up the menu, and select **Properties**.
3. Click over to the **Member Of** tab, and click **Add**...
4. Under **Enter the object names to select** add the **Distributed COM Users** group and Performance Monitor Users group, then click **OK**.





Next, configure the **DCOM Security Settings** to allow the groups to access the system remotely.

5. Click Start > **Run**..., type **dcomcnfg** and click **OK**
6. Drill down into the **Component Services** tree until you get to **My Computer**. Right-click "**My Computer**" to bring up the menu, and click **Properties**.
7. Click the **COM Security** tab, then click **Edit Limits** under the **Launch and Activation Permissions** section.
8. Click **Add**...
9. Under **Enter the object names to select**, type **Distributed COM** Users and **Performance Monitor Users**, then click **OK**.
10. Check **Allow** for each of the permissions (Local Launch, Remote Launch, Local Activation, Remote Activation) for each of these groups, and click **OK**.



Finally, set the **WMI Control** security settings to be applied to all namespaces.

11. Click Start > **Run**..., type **wmimgmt.msc** and click **OK**
12. Right-click **WMI Control** (Local) to bring up the menu, and click **Properties**.
13. Click over to the **Security** tab, then click **Root**, then click **CIMV2**, then click **Security** and click the **Security** button.
14. Click **Add**.
15. Under Enter the object names to select, type **Distributed COM Users** and **Performance Monitor Users** , click **Check Names**, then click **OK**.
16. Click **Advanced**
17. Highlight the row with **Distributed COM Users** in it and click **Edit**.
18. From the drop-down list, select **This namespace and subnamespaces**
19. Under the **Allow** column check **Execute Methods**, **Enable Account**, and **Remote Enable**.
20. Repeat steps **16-19** for the **Performance Monitor Users** group.
21. Click **OK** to close all windows.

Audit Settings Recommendations

The recommendations are for enterprise-class computers, which Microsoft defines as computers that have average security requirements and require a high level of operational functionality. Entities needing higher security requirements should consider more aggressive audit policies.

Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 Audit Settings Recommendations			
Audit Policy Category or Subcategory	**Windows Default**	**Baseline Recommendation**	**Stronger Recommendation**
	Success / Failure	**Success /Failure**	**Success /Failure**
Account Logon			
Audit Credential Validation	No/No	Yes / Yes	Yes / Yes
Audit Kerberos Authentication Service			Yes / Yes
Audit Kerberos Service Ticket Operations			Yes / Yes
Audit Other Account Logon Events			Yes / Yes
Account Management			
Audit Application Group Management			
Audit Computer Account Management		Yes / DC	Yes / Yes
Audit Distribution Group Management			
Audit Other Account Management Events		Yes / Yes	Yes / Yes
Audit Security Group Management		Yes / Yes	Yes / Yes
Audit User Account Management	Yes / No	Yes / Yes	Yes / Yes
Detailed Tracking			
Audit DPAPI Activity			Yes / Yes
Audit Process Creation		Yes / No	Yes / Yes
Audit Process Termination		Yes / No	Yes / Yes
Audit RPC Events			
DS Access			
Audit Detailed Directory Service Replication			
Audit Directory Service Access		DC DC	DC DC
Audit Directory Service Changes		DC DC	DC DC
Audit Directory Service Replication			
Logon and Logoff			
Audit Account Lockout	Yes / No		Yes / No
Audit User/Device Claims			
Audit IPsec Extended Mode			
Audit IPsec Main Mode			IF IF
Audit IPsec Quick Mode			
Audit Logoff	Yes / No	Yes / No	Yes / No
Audit Logon	Yes / No	Yes / Yes	Yes / Yes
Audit Network Policy Server	Yes / Yes		
Audit Other Logon/Logoff Events			Yes / Yes
Audit Special Logon	Yes / No	Yes / No	Yes / Yes

Object Access			
Audit Application Generated			
Audit Certification Services			
Audit Detailed File Share			
Audit File Share			
Audit File System			
Audit Filtering Platform Connection			
Audit Filtering Platform Packet Drop			
Audit Handle Manipulation			
Audit Kernel Object			
Audit Other Object Access Events			
Audit Registry			
Audit Removable Storage			
Audit SAM			
Audit Central Access Policy Staging			
Policy Change			
Audit Audit Policy Change	Yes / No	Yes / Yes	Yes / Yes
Audit Authentication Policy Change	Yes / No	Yes / Yes	Yes / Yes
Audit Authorization Policy Change			
Audit Filtering Platform Policy Change			
Audit MPSSVC Rule-Level Policy Change			Yes / -
Audit Other Policy Change Events			
Privilege Use			
Audit Non Sensitive Privilege Use			
Audit Other Privilege Use Events			
Audit Sensitive Privilege Use			
System			
Audit IPsec Driver		Yes / Yes	Yes / Yes
Audit Other System Events	Yes / Yes		
Audit Security State Change	Yes / No	Yes / Yes	Yes / Yes
Audit Security System Extension		Yes / Yes	Yes / Yes
Audit System Integrity	Yes / Yes	Yes / Yes	Yes / Yes
Global Object Access Auditing			
Audit IPsec Driver			
Audit Other System Events			
Audit Security State Change			
Audit Security System Extension			
Audit System Integrity			

Windows PowerShell

Windows keeps a detailed log of PowerShell scripts and interactive access. Excessive use of large PowerShell scripts can cause event logging and generation of events, if they are used frequently.

We recommend that the organization be configured in the test environment before deployment.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	
Turn on Module Logging	Enabled only if versions prior to PowerShell 5 are installed on the network.Enabled Module Names: *
Turn on PowerShell Script Block Logging	**Enabled**

*** References**

https://www.asd.gov.au/publications/protect/Windows_Event_Logging_Technical_Guidance.pdf
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Logsign is a Security Information and Event Management (SIEM) solution which provides security analyses and compliance to regulations in one platform. Founded in 2010, Logsign believes that cyber security is a teamwork and that security products have to be much smarter. With this conviction, it focused its endeavors on Security Intelligence and SOC solutions. It actively provides services for more than 500 medium and large scale firms and governmental agencies. It is working to be an irreplaceable team-mate for all of its stakeholders in the field of cyber security, to raise its customers' security awareness to the maximum and to reinforce their position concerning security. It also proved its competence in the field of technology as a cyber security software producer, landing among Deloitte Technology EMEA Fast 500 in 2017 for the second time.