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

1. Look at administrative tools tab, server manager is most important

2. If Kerberos is compromised, you must change the password 7+ times to invalidate the old one

Step 1: Enable audit policy.

This step includes procedures to enable change auditing with either the Windows interface or a command line:

* By using Group Policy Management, you can turn on the global audit policy, **Audit directory service access**, which enables all the subcategories for AD DS auditing. If you need to install Group Policy Management, click **Add Features** in Server Manager. Select **Group Policy Management** and then click **Install**.
* By using the Auditpol command-line tool, you can enable individual subcategories.

To enable the global audit policy using the Windows interface

1. Click **Start**, point to **Administrative Tools**, and then **Group Policy Management**.
2. In the console tree, double-click the name of the forest, double-click **Domains**, double-click the name of your domain, double-click **Domain Controllers**, right-click **Default Domain Controllers Policy**, and then click **Edit**.
3. Under **Computer Configuration**, double-click **Policies**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then click **Audit Policy**.
4. In the details pane, right-click **Audit directory service access**, and then click **Properties**.
5. Select the **Define these policy settings** check box.
6. Under **Audit these attempts**, select the **Success**, check box, and then click **OK**.

To enable the change auditing policy using a command line

1. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
2. Type the following command, and then press ENTER:

**auditpol /set /subcategory:"directory service changes" /success:enable**

Step 2: Set up auditing in object SACLs.

The following procedure presents an example of just one of many different types of SACLs that you can set based on the operations that you want to audit.

To set up auditing in object SACLs

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click the organizational unit (OU) (or any object) for which you want to enable auditing, and then click **Properties**.
3. Click the **Security** tab, click **Advanced**, and then click the **Auditing** tab.
4. Click **Add**, and under **Enter the object name to select**, type Authenticated Users (or any other security principal), and then click **OK**.
5. In **Apply onto**, click **Descendant User objects** (or any other objects).
6. Under **Access**, select the **Successful** check box for **Write all properties**.
7. Click **OK** until you exit the property sheet for the OU or other object.

### Domain Controller Recommended Group Policy Settings

This section outlines recommended security settings for Domain Controllers, many of which are described and set in the Microsoft security baseline in SCM.  
Please fully test these settings before applying.

**Enable NTLM Auditing**

Restrict NTLM: Audit Incoming NTLM Traffic: Enable auditing for all accounts

Restrict NTLM: Audit NTLM authentication in this domain: Enable all

**LAN Manager authentication level: Send NTLMv2 response only. Refuse LM & NTLM**

**Lsass.exe audit mode: Enabled**

**Enable LSA Protection: Enabled**

**Domain member: Require strong (Windows 2000 or later) session key: Enabled**

**Network security: Minimum session security for NTLM SSP based (include secure RPC) servers: Require NTLMv2 session security, Require 128-bit encryption**

**Network security: Minimum session security for NTLM SSP based (include secure RPC) clients: Require NTLMv2 session security, Require 128-bit encryption**

**Microsoft network server: Digitally sign communications (if client agrees): Enabled**

**Microsoft network server: Digitally sign communication (always): Enabled**  
**Microsoft network client: Digitally sign communication (always): Enabled**

**Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled**

**WDigest Authentication (disabling may require KB2871997): Disabled**