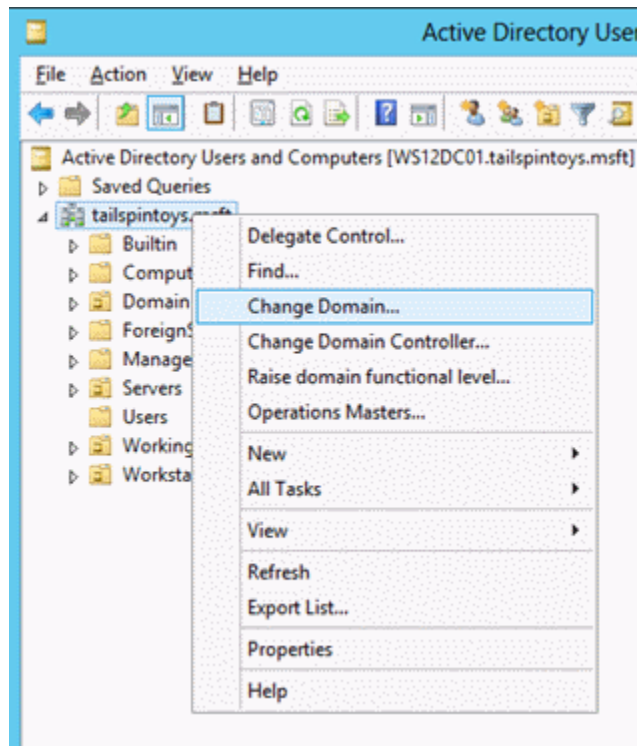# Ultimate Windows Server 2019 Checklist
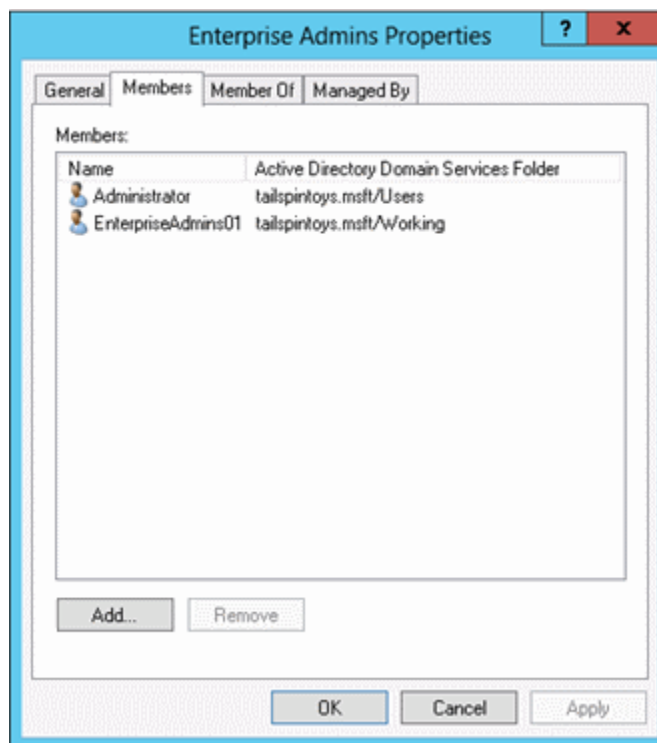
1. User ExUser is not an Enterprise Admin

1. In Server Manager, click Tools, and click Active Directory Users and Computers.
2. If you are not managing the root domain for the forest, in the console tree, right-click <Domain>, and then click Change Domain (where <Domain> is the name of the domain you're currently administering).

3. In the Change domain dialog box, click Browse, select the root domain for the forest, and click OK.

Change domain

Domain: |

☐ Save this domain setting for the current console

OK   Cancel   Help
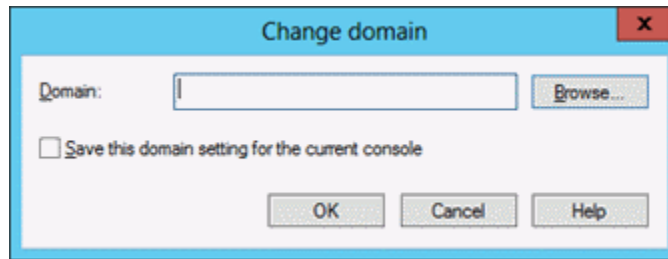
4. To remove all members from the EA group:
    1. Double-click the Enterprise Admins group and then click the Members tab.

Enterprise Admins Properties   ?   x

General | Members | Member Of | Managed By

Members:

Name	Active Directory Domain Services Folder
Administrator	tailspintoys.msft/Users
EnterpriseAdmins01	tailspintoys.msft/Working

Add...   Remove

OK   Cancel   Apply

    2. Select a member of the group, click Remove, click Yes, and click OK.
5. Repeat step 2 until all members of the EA group have been removed.

2. Domain Users removed from DnsAdmins group

3. IIS default website directory browsing disabled

4. IIS HTTP error responses for remote requests not set to Detailed

5. IIS server information is not included in response header

Run as administrator:

%systemroot%\system32\inetsrv\appcmd.exe set config
-section:system.webServer/security/requestFiltering /removeServerHeader:"True"
/commit:apphost

6. IIS web server requires SSL connections

https://enterprise.arcgis.com/en/web-adaptor/10.3/install/iis/enable-https-on-your-web-server-server-.htm

7. Audit DNS events

Launch **Server Manager** in your Windows Server instance.
Under Manage, select **Group Policy Management** and launch the Group Policy

Management console.

Navigate to **Forest --> Domain --> Your domain --> Domain Controllers.**

Create a new GPO and link it to the domain containing the computer object, or edit any

existing GPO that is linked to the domain to open the **Group Policy Management Editor.**

Navigate to **Computer Configuration -> Windows Settings -> Security Settings ->Local**

Policies -> Audit Policy.

Under **Audit Policy** turn auditing on for Success and Failure for everything

8. DNS Service restarts after failure

9. DNS zone transfers to any server is disabled

10. Dynamic updates to the DNS server are disabled

11. SIGRed workaround implemented