

Episode Title: Harden and secure domain controllers

Objectives:

At the end of this episode, I will be able to:

1. Explain methods to harden domain controllers
2. Configure the Windows Defender Advanced Firewall
3. Configure domain controller audit policies

Key Points:

Key Point 1

Domain Controllers should be secured by limiting Remote Desktop connections and ensuring security patches are applied.

Key Point 2

External internet access from a domain controller should be limited to only known services that are in use. For example, outbound connectivity to Microsoft Entra ID.

Key Point 3

Domain controllers should have auditing enabled for account and privileged activity. Use Group Policy to define these settings for all DCs.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- Securing Domain Controllers Against Attacks
: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack>