

Episode Title: Recover Active Directory database using Directory Services Restore Mode

Objectives:

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

1. Use the Directory Services Restore Mode
2. Reset the DSRM password
3. Use the NTDSUtil CLI tool

Key Points:

Key Point 1

Directory Services Restore Mode (DSRM) is essentially 'safe mode' for Active Directory. This is where you can recover Active Directory.

Key Point 2

The DSRM password is critical to being able to restore Active Directory and enter DSRM. This password is set during domain controller promotion and is different than the directory administrator account.

Key Point 3

The NTDSUtil CLI tool is the primary tool for interacting with the ntds.dit directory database file. You can use this tool to reset the DSRM password and perform integrity checks on the NTDS database.

- 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:

- How to reset the Directory Services Restore Mode administrator account password in Windows Server
: <https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/reset-directory-services-restore-mode-admin-pwd>