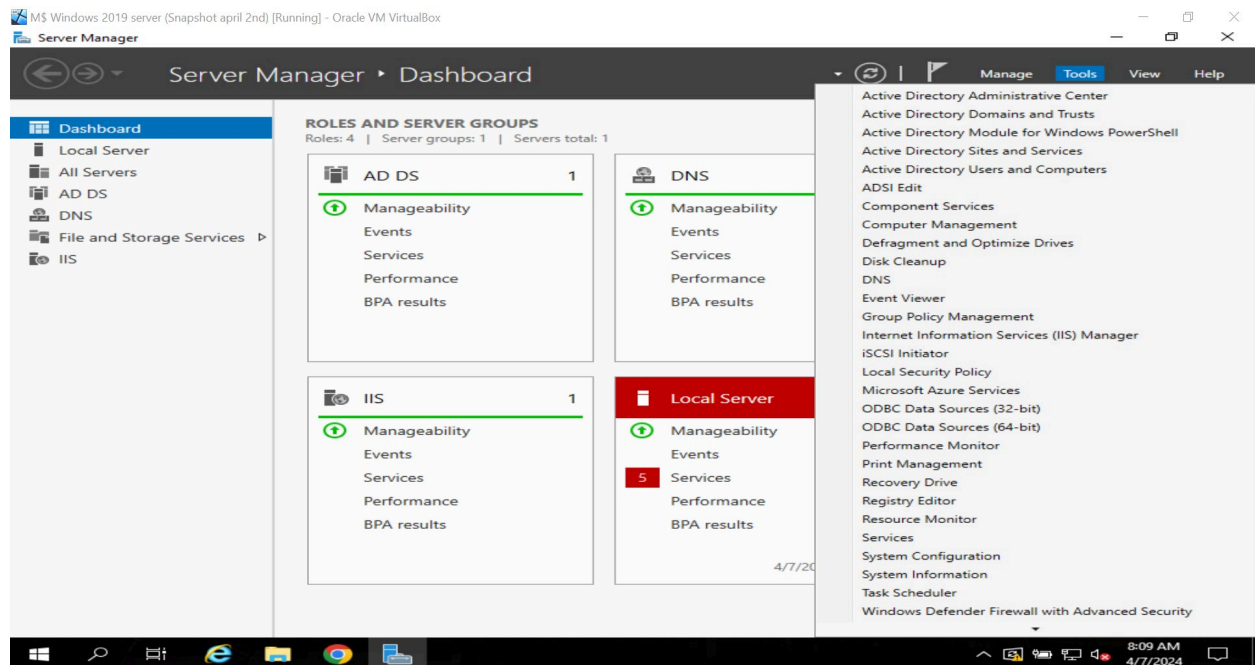


Name: Cristian Barreno

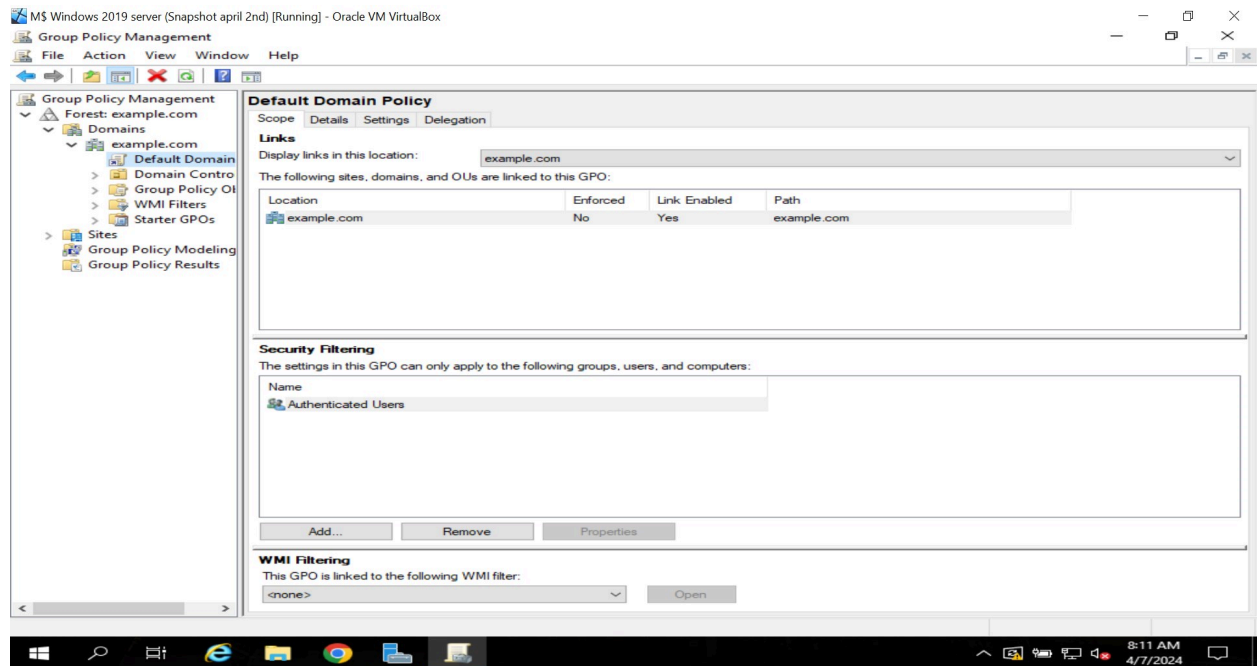
Modifying a Group Policy Object (GPO) related to Windows Password Policy

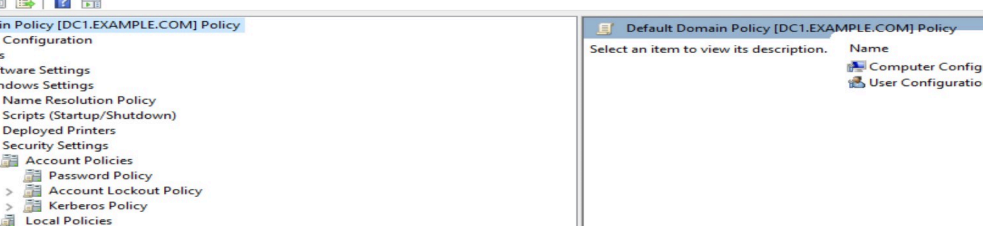
Group Management Policies let Administrators manage, and apply policies or rules to a group of users, or computers. An administrator has the power to enforce different policies to users to maintain security across the board. Some examples are password length, complexity requirements, minimum and maximum password age, and enforce password history.

The first step is to open The Group Policy Management Console from the Server Manager Dashboard.



In the Group Management Console, expand the Forest(example.com), expand the Domain, open the example.com Domain, and right click on the Default Domain Policy Folder, and click edits.





The screenshot shows the Windows Group Policy Management Editor interface. The left pane displays the hierarchy: Default Domain Policy [DC1.EXAMPLE.COM] Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy. The right pane shows the configuration for the Password Policy:

| Policy | Policy Setting |
|---|-------------------------|
| Enforce password history | 20 passwords remembered |
| Maximum password age | 180 days |
| Minimum password age | 1 days |
| Minimum password length | 12 characters |
| Minimum password length audit | Not Defined |
| Password must meet complexity requirements | Enabled |
| Store passwords using reversible encryption | Disabled |