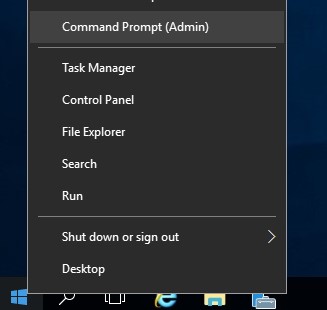
Lab 6 Service Accounts and Account Policies

1. On DC1 right click on the start menu and select Command Prompt (Admin)



1. At the command prompt type **sc query**

This command will display all active services and drivers

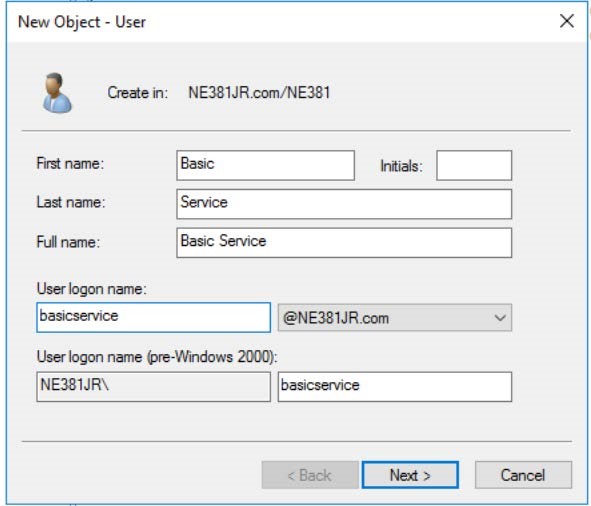
1. Type **sc** to see what other options are available to this command line program

Services link back to programs and drivers in windows Another way to view services is from the service panel.

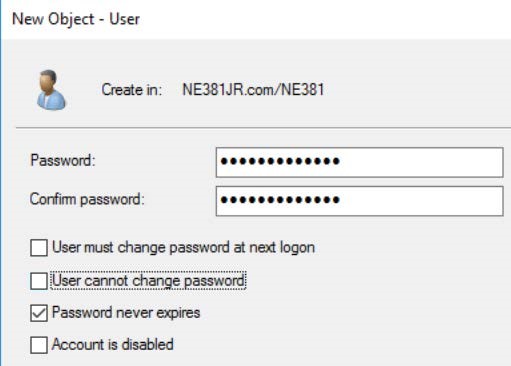
1. Right click on the start menu again and type **services.msc**

Here you will see a list of all the service definitions on the computer. Each service links back to a program. Some programs require special accounts to run them. You should never run a service with administrator, local system access or domain administrator access. Use this procedure to create a service account.

1. Open Active Directory Users and Computers
2. Right Click on the NE381 OU and select new user 7. Create an account with the following properties

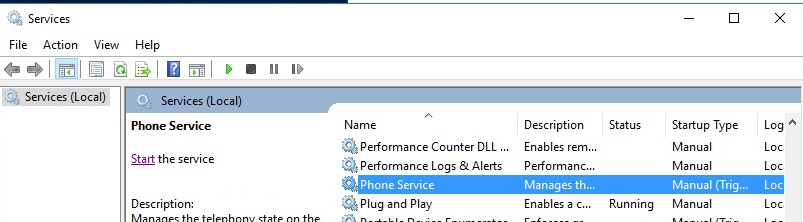


1. Set the password to Password#1 and set the following properties.

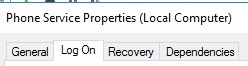


Screenshot this account in ADUC for submission to canvas.

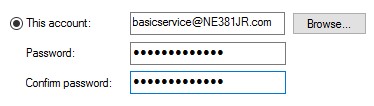
1. While on DC1 open the services console using **services.msc** command and locate the Phone Service.



1. Right click on the service and select properties
2. Select the Log On tab



1. Adjust the account settings to use the newly created AD account. (You will have to update the password)



1. Click on Apply then screenshot the message that pops up. In the previous example we set the account password to never expire. This is a bad security practice. If we let the password expire then we would have to update service settings according to the domain policy. This would cause a lot of administrative overhead.

~~Part 2 Managed Service Accounts (SKIP THIS SECTION)~~

~~Managed Service account are a special object class. Its password is updated to a random 120 character password every 30 days by the computer it is setup on.~~

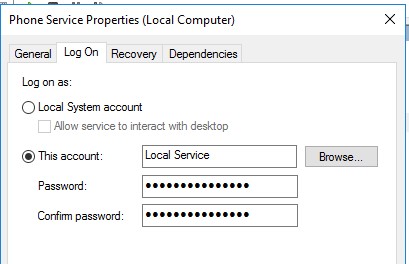
* 1. ~~Launch an administrative PowerShell command prompt on DC1~~
  2. ~~Type~~ **~~New-ADServiceAccount -Name msaDC2 RestrictToSingleComputer -Enabled $true~~**

~~~~

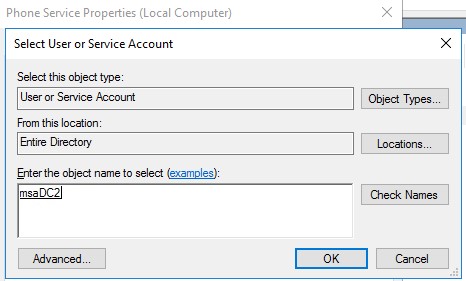
* 1. ~~Now type~~ **~~Add-ADComputerServiceAccount -Identity DC2 ServiceAccount msaDC2~~**

~~~~

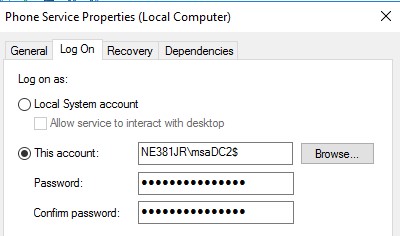
* 1. ~~Log onto DC2 with a domain administrator account~~
  2. ~~Open a PowerShell command prompt and run the following~~
  3. **~~Install-ADServiceAccount -Identity msaDC2~~**
  4. ~~Open the~~ **~~services.msc~~** ~~panel on DC2 and locate the phone service.~~
  5. ~~Go to the properties of the service then the log on tab~~

~~~~

* 1. ~~Click Browse then type in~~ **~~msadc2~~** ~~then click check names~~

~~~~

* 1. ~~Click ok~~
  2. ~~On the properties dialog box clear out the password properties.~~ **~~Then click ok.~~** ~~It should look like this.~~

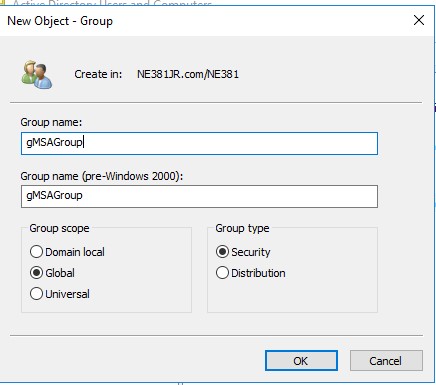
~~~~

|  |
| --- |
| **~~Screenshot your service account setup.~~** |

~~The password will auto generate. The account will be good for running services on DC2. The reason we did it from DC2 is that DC2 already has the required PowerShell module installed.~~

Part 3 Group managed service accounts   
The previous account can only be used on the computer it was created for. We can create a Group managed service account to use on multiple computers.

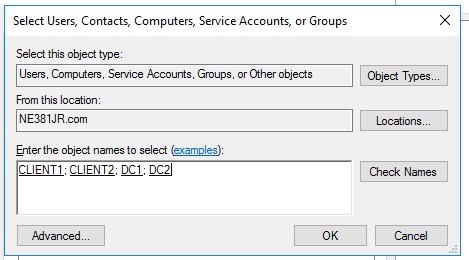
* 1. From DC2 Create a new security group in the NE381OU called gMSAGroup

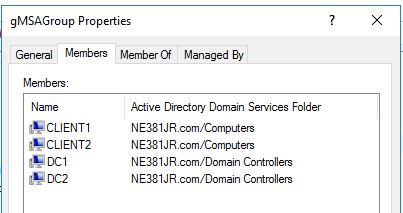


* 1. Click the Start Menu -> Windows Powershell -> Right-Click Windows Powershell -> More -> Run as Administrator. From PowerShell console type **Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))**

This will allow the KDS to issue passwords to each computer that uses the service.

* 1. Still in PowerShell type **New-ADServiceAccount -Name gMSAAcct -DNSHostName gMSAAcct.ne381xx.com PrincipalsAllowedToRetrieveManagedPassword gMSAGroup -Enabled $true**
  2. Locate the gMSAGroup that you created previously in ADUC.
  3. Go to the properties of the Group then the members tab
  4. Add CLIENT1, CLIENT2, DC1 and DC2 as members. (Note you will have to make sure that computer is selected as an object type. Click ok then Apply and OK



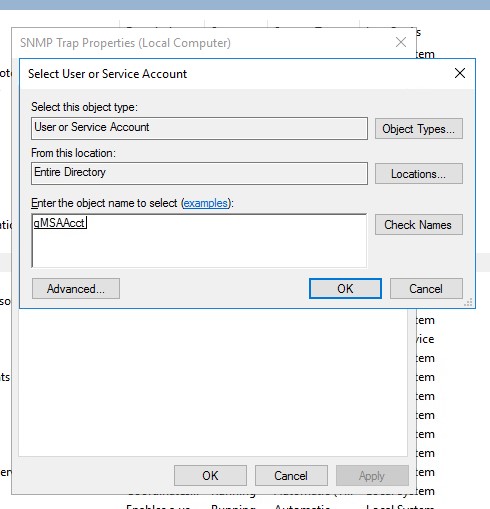


|  |
| --- |
| Screenshot the group membership dialog box: |

1. **From DC1 open a powershell command prompt and type the following.**

**Install-ADServiceAccount -Identity gMSAAcct**

1. Like before open the services panel locate the SNMP Trap Service and set the service to use the new gmSAAcct

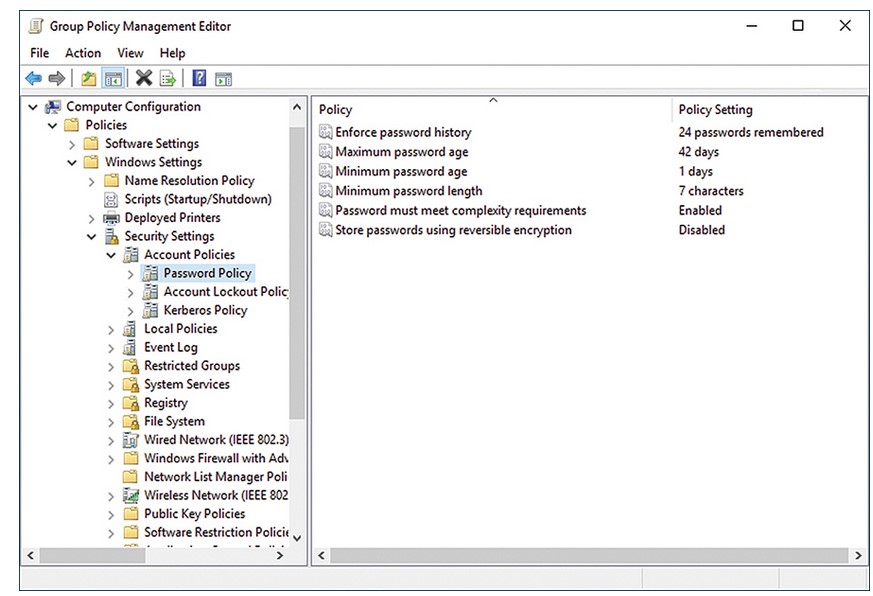


Part 4 Policies

1. From DC2 open Server Manger then go to Tools then Launch **Group Policy Management**
2. Expand the Forest, Domains, domain node, and Group Policy Objects node to expose the Default Domain Policy.
3. Right-click the Default Domain Policy and select Edit.
4. The Group Policy Management Editor utility launches.

Expand the Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies node and select Password Policy.

The panel on the right displays the following Password Policies



1. Modify the policies with the following values

Enforce password History 24

Maximum password age 30

Minimum password age 15

Minimum password Length 8

Password Must meet complexity requirements Enabled

# \*Screenshot your password policy settings for upload\*

# 

1. Close out of all the settings
2. Launch a command prompt
3. Type **gpmc**

Group Policy Management utility launches. Expand the Forest, Domains, domain node, and Group Policy Objects node to expose the Default Domain Policy

1. Expand the Forest, Domains, domain node, and Group Policy Objects node to expose the Default Domain Policy.
2. Expand the Computer Configuration, Policies, Windows Settings, Security Settings, Account Policies node and select Account Lockout Policy.
3. Adjust settings to match the following



# \*Screenshot these settings for upload to canvas\*