Integrate azure AD with LDAP

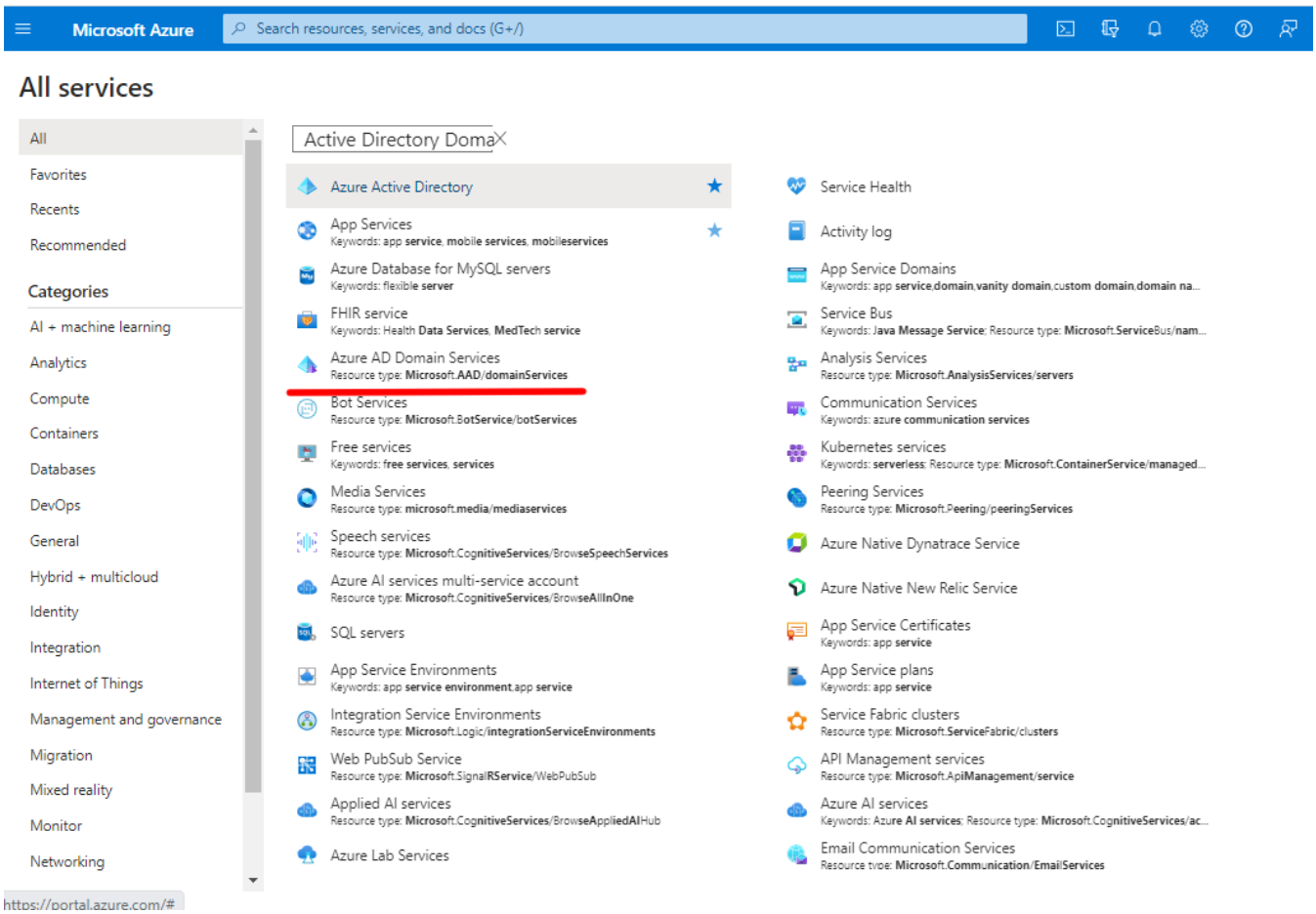
627 Manu Chacko April 30, 2024 Getting Started 1216

Enable LDAPS on Azure AD and integrate it into your application. Configure secure LDAP for an Azure Active Directory Domain Services

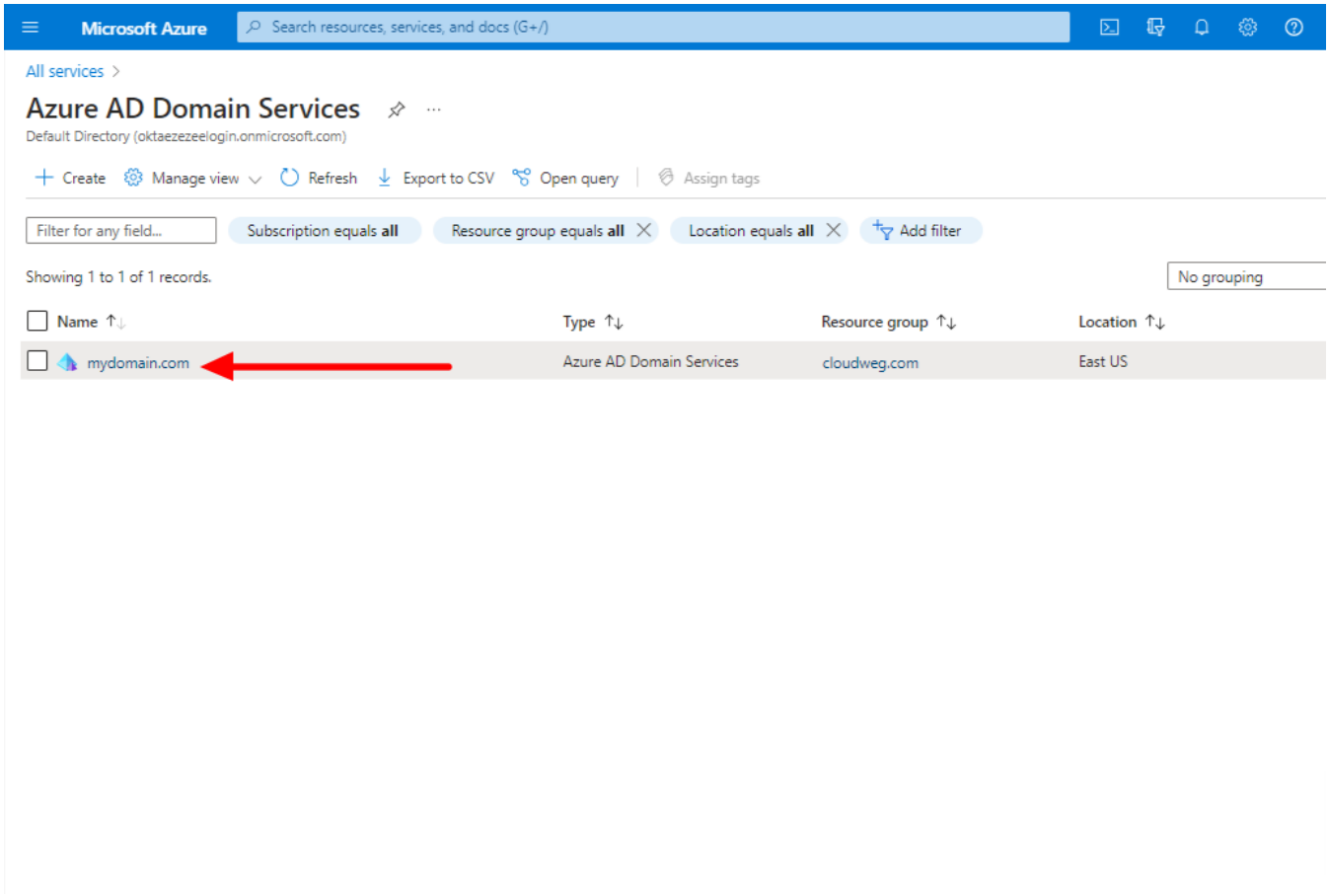
Refer to this article to Integrate Azure AD in Ezeelogin jump server

Make your Azure Active Directory Domain Service more secure and connect external systems easily with LDAPS. Follow the steps to enable LDAPS and test LDAP queries from an external system.

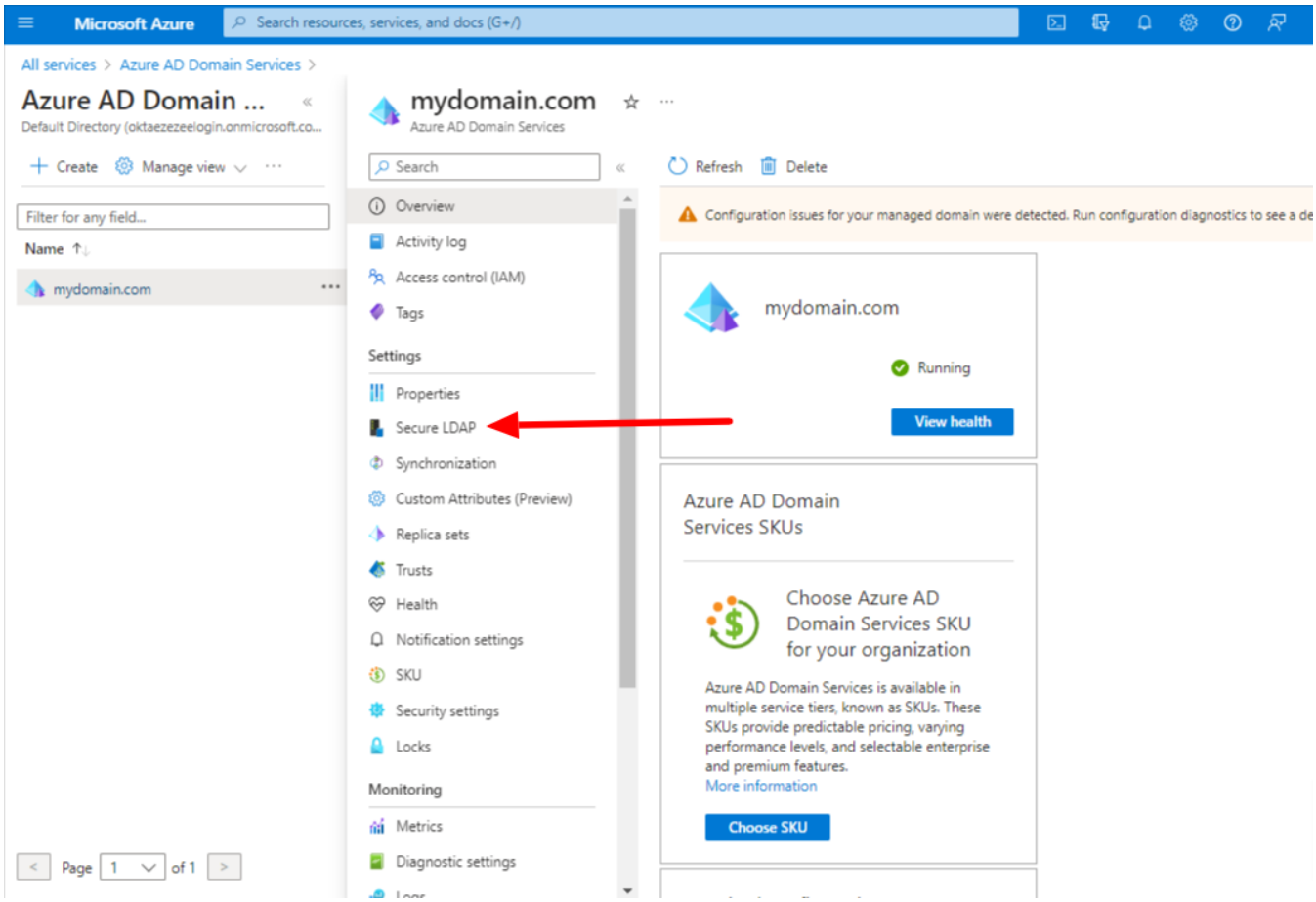
1.Log into the Azure portal, Search, and Select Azure AD Domain Services



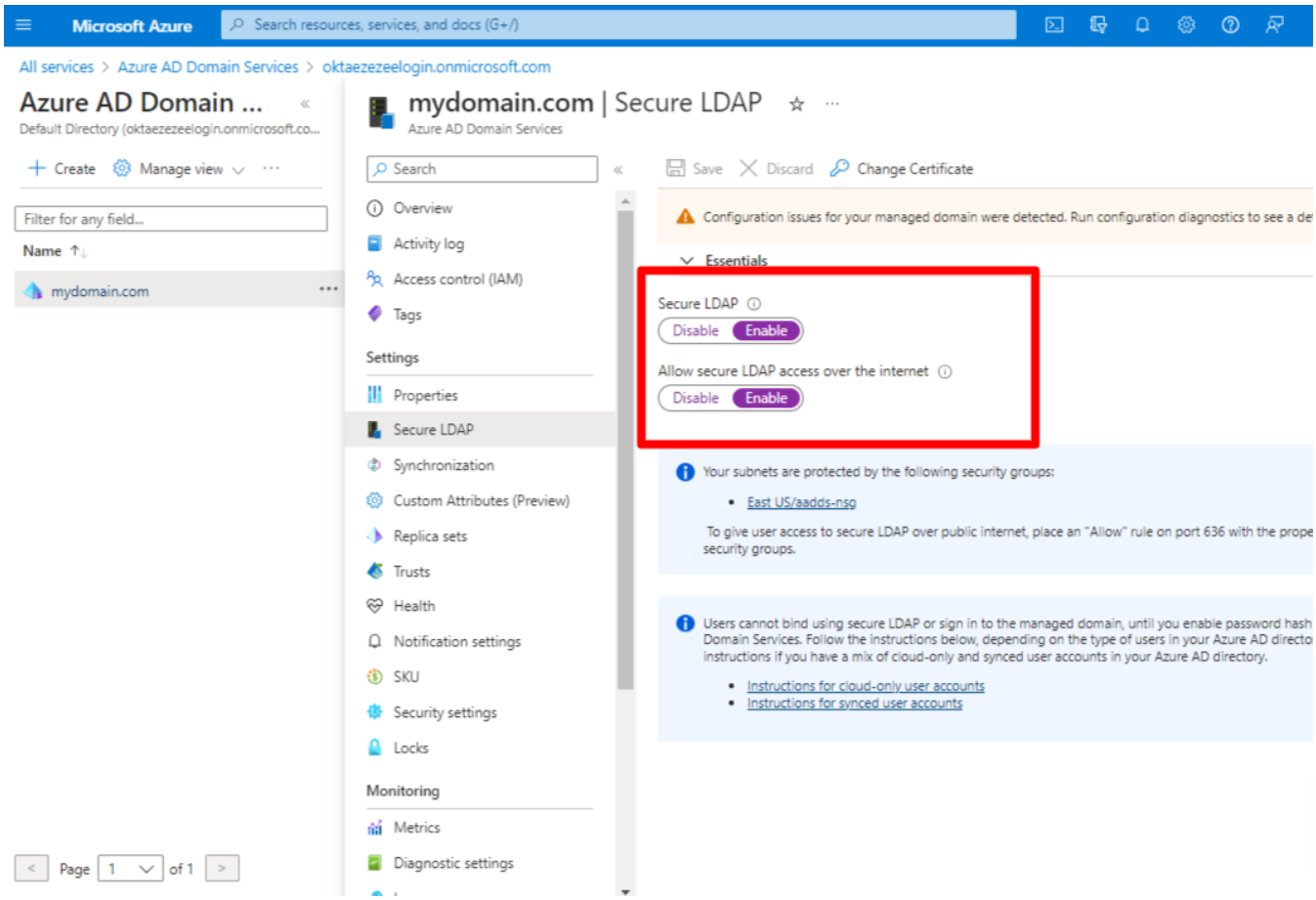
2. Select your Managed Domain service



3. Select **Secure LDAP**



4. Enable **secure LDAP** and **Allow secure access over the Internet**



You should need a digital certificate to encrypt the communication to use secure LDAP. You can get a certificate from a public certificate authority (CA) or an enterprise CA or a self-signed certificate

5. Follow the instruction to create and export a self-signed certificate

a) Open a PowerShell window as Administrator and run the following commands. Replace the $dnsName variable with your managed domain, For example mydomain.com

```
#Define your own DNS name used by your managed domain
$dnsName="mydomain.com"
#Get the current date to set a one-year expiration
$lifetime=Get-Date
```

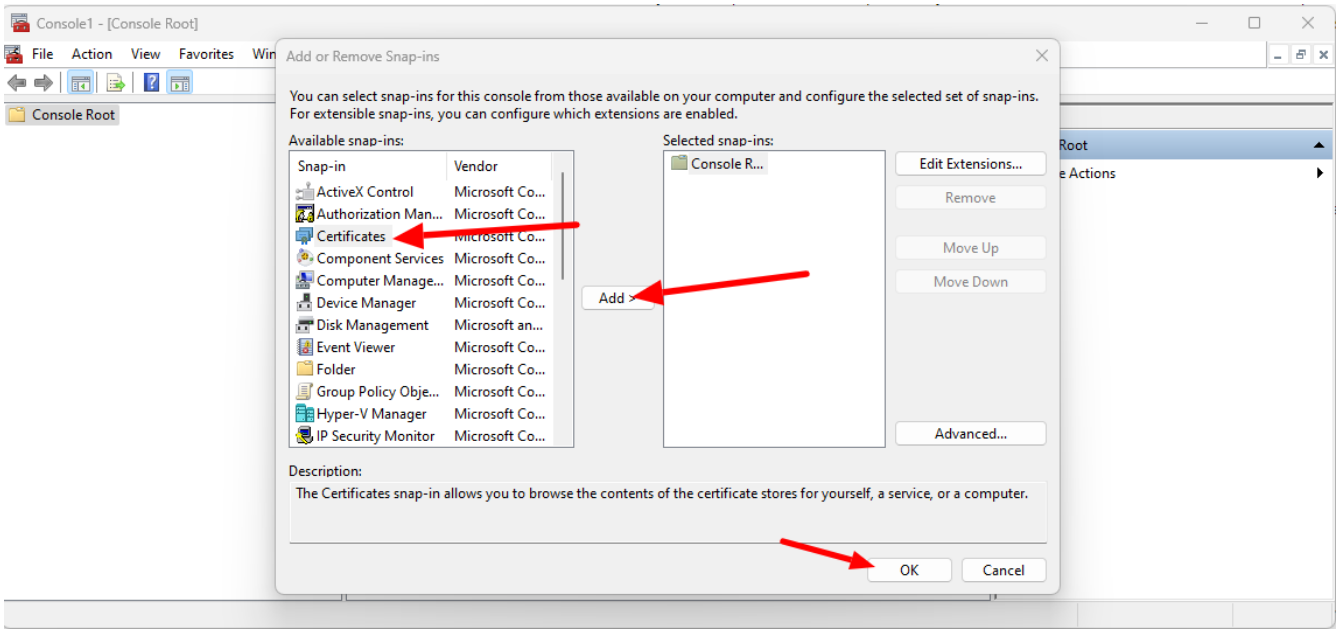
You can view the following output if the certificate was successfully created

```
PS C:\WINDOWS\system32> New-SelfSignedCertificate -Subject *.$dnsName `
>>   -NotAfter $lifetime.AddDays(365) -KeyUsage DigitalSignature, KeyEncipherment `
>>   -Type SSLServerAuthentication -DnsName *.$dnsName, $dnsName.com

   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\MY

Thumbprint                                Subject
----------                                -------
959BD1531A1E674EB09E13BD8534B2C76A45B3E6  CN=mydomain.com
```

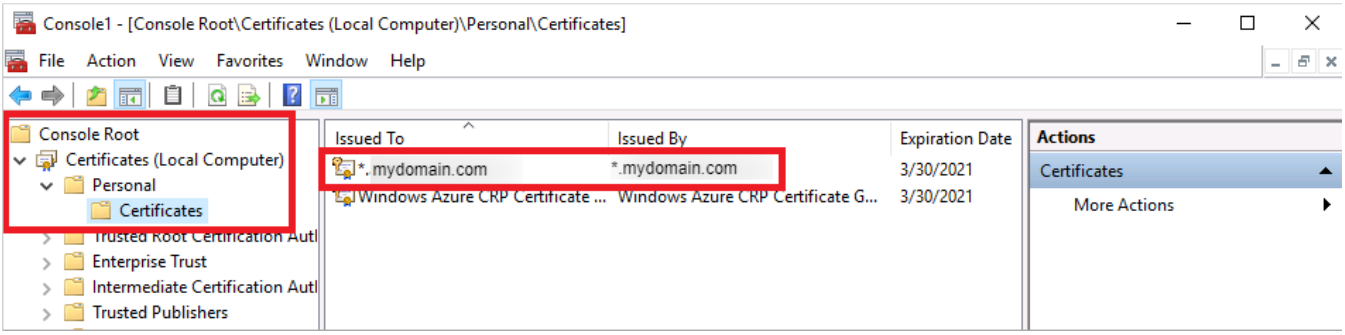
b) Export a certificate for Azure AD DS

- open run on windows machine and enter **mmc** , press ok
- click on the **File** and select **Add/Remove Snap-in**

select **certificates** and click on **Add** , click **ok**



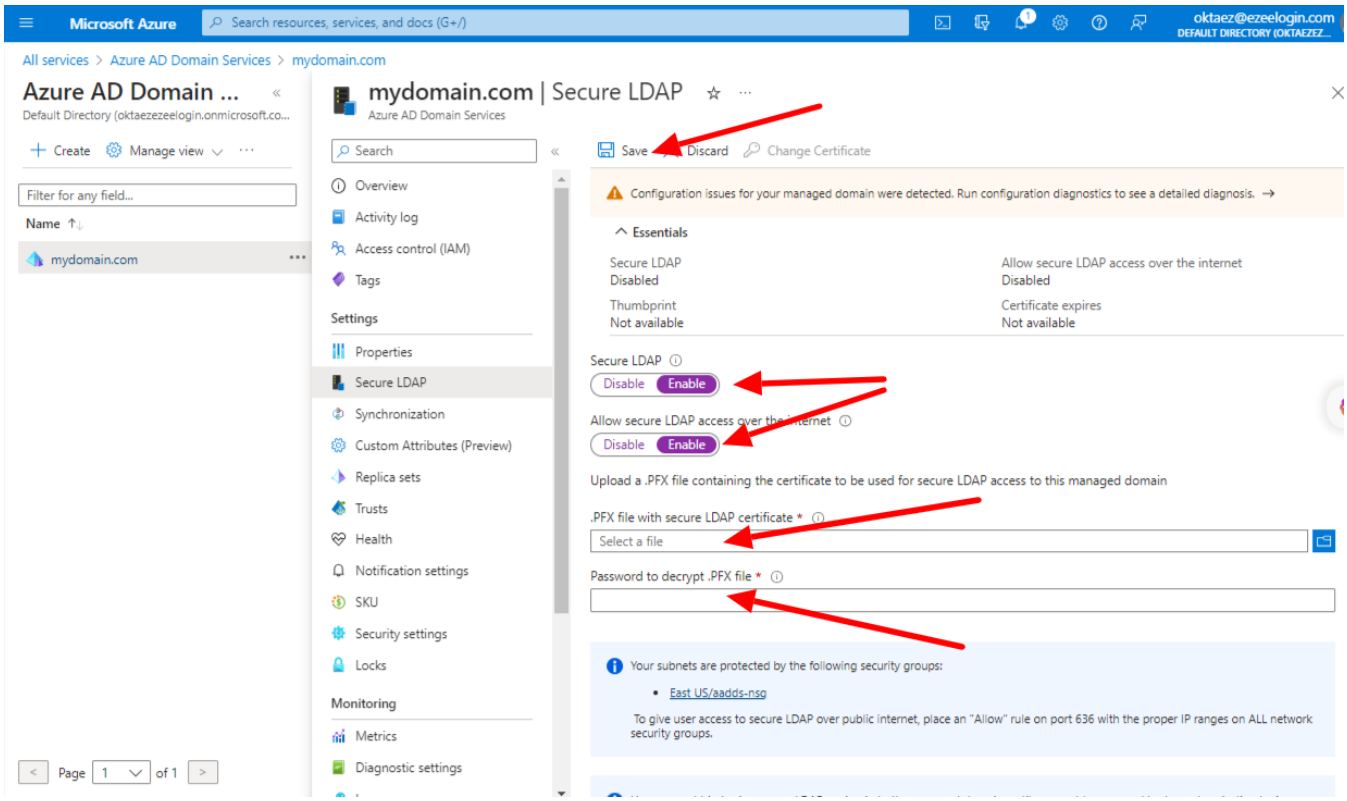
- then select **Local computer: (the computer this console is running on)** , then click **Finish** .
- In the MMC window, expand Console Root. Select **Certificates** (Local Computer), then expand the **Personal node** , followed by the Certificates node.



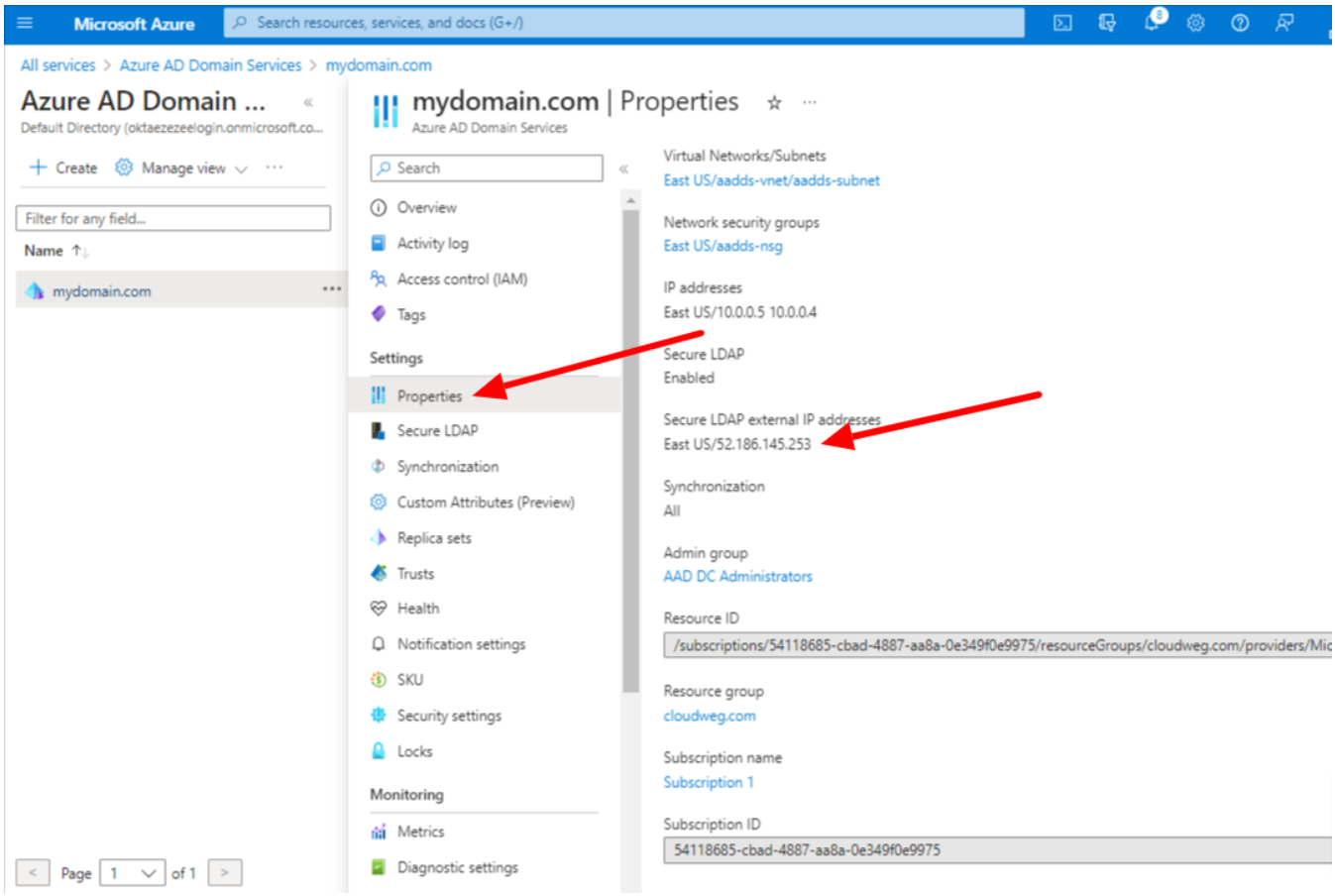
- Right-click on this certificate, then choose **All Tasks > Export**
- Export Private Key page, choose **Yes, export the private key,** then select **Next** .
- Select **Personal Information Exchange - PKCS #12 (.PFX)** as the file format for the certificate. Check the box for Include **all certificates in the certification path if possible**
- Click **Next** and type a password and follow the prompts

You will get the certificate exported in pfx format. Now you can continue on Azure portal

6. Select the folder icon next to .PFX file with secure LDAP certificate. Browse to the path of the .PFX file you exported in the previous step and enter the password to decrypt which you have used while exporting and save.



7. Click on **Properties** and add configure your DNS provider to create a host record to resolve to this **Secure LDAP external IP address**

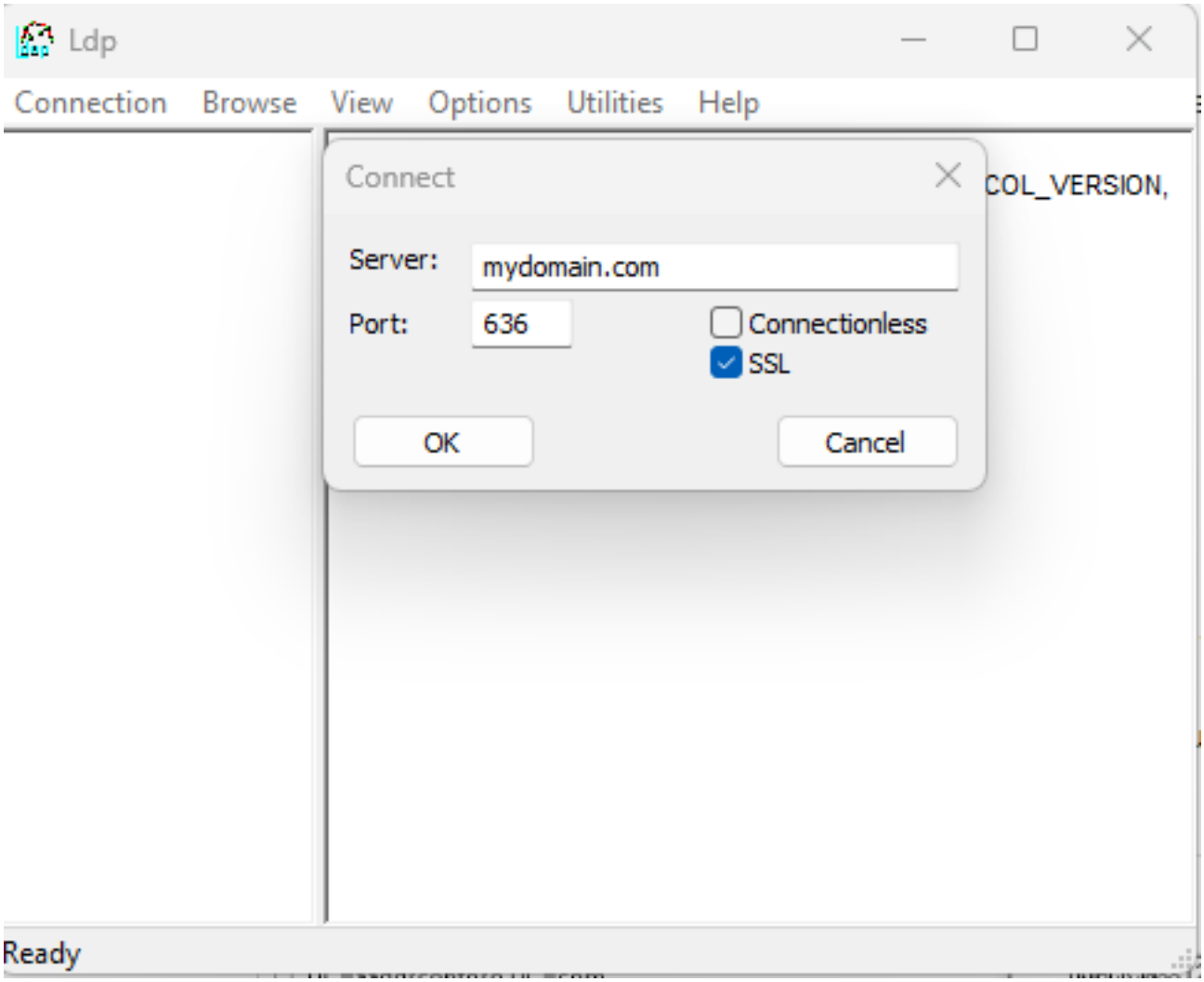


You can configure this to your Local DNS forwarder or to your system host to resolve locally for testing.

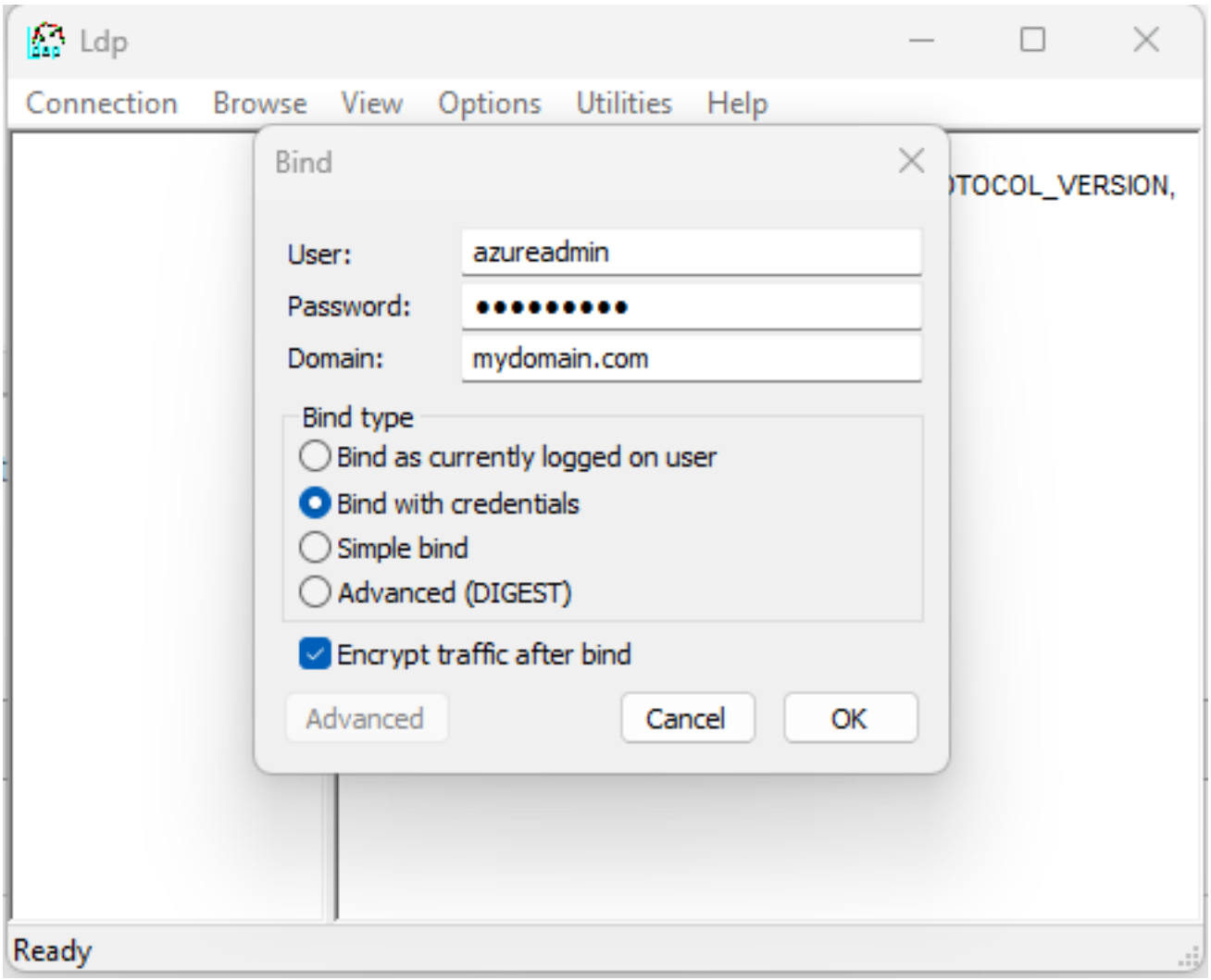
Test the LDAPS queries from an external system

Add the following **Secure LDAP external IP address** to your host file on the system

1. Open LDP.exe tools and enter the domain name, Port 636, select **SSL** and click **ok**



2. Open **Connection > Bind,** Select **Bind with credentials** and input your **Username**, P**assword, and Domain** of the **Azure Bind User**



3. Open **View > Tree** will list the entire Active Directory Tree.

You can also run LDAPSEARCH from your terminal as follows. You should use "LDAPTLS_REQCERT=never" if you are using a self-signed certificate.

Related Articles

[Can we map existing user group in ldap to ezeelogin as ezeelogin user group ?]

Assigning user group for LDAP users?

Online URL: https://www.ezeelogin.com/kb/article/integrate-azure-ad-with-ldap-627.html