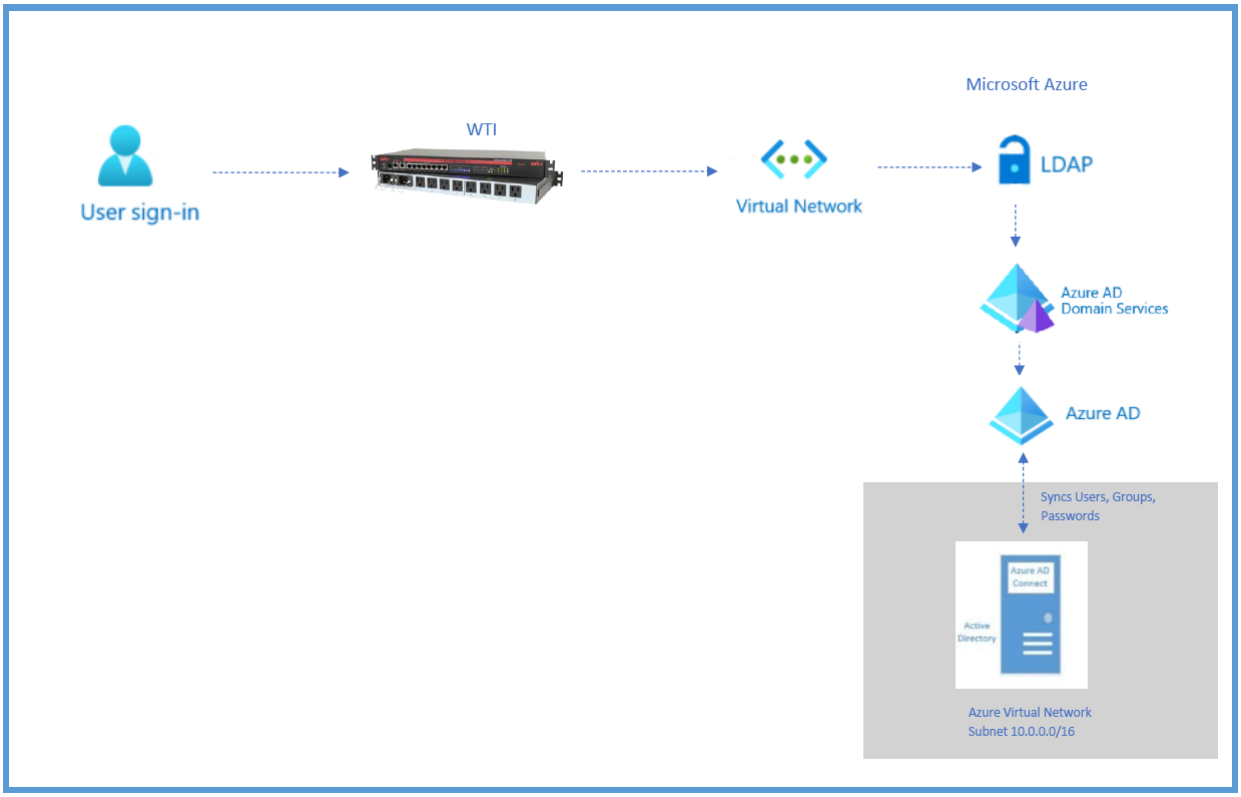
WTI with secure LDAP for an Azure Active Directory Domain Services (Azure AD DS)



Components of system

- **User:** Accesses WTI via a browse or SSH.
- **WTI:** The interface that the user interacts with to access secure LDAP via external IP address or FQDN from Azure AD DS.
- **Virtual Network:** A private network in Azure through which the legacy application can consume LDAP services.
- **Legacy applications:** Applications or server workloads that require LDAP deployed either in a virtual network in Azure, or which have visibility to AD DS instance IPs via networking routes.
- **Azure AD:** Synchronizes identity information from organization's on-cloud/on-premises directory via Azure AD Connect.
- **Azure AD Domain Services (AD DS):** Performs a one- way synchronization from Azure AD to provide access to a central ser of users, groups, and credentials. The AD DS instance is assigned to a virtual network. Applications, services, and VMs in Azure that connect to the virtual network assigned to AD DS can use common AD DS features such as LDAP, domain join, group policy, Kerberos, and NTLM authentication.
- **Azure AD Connect:** A tool for synchronizing on cloud/on premises identity information to Microsoft Azure AD. The deployment wizard and guided experiences help you configure

prerequisites and components required for the connection, including sync and sign on from Active Directory to Azure AD.

- **Active Directory:** Directory service that stores on-cloud/on-premises identity information such as user and account information, and security information like passwords.

Setup & Configuration requirement

Please follow each tutorial step by step to create a secure LDAP with Azure AD DS.

1. Tutorial: Create and configure an Azure Active Directory Domain Services managed domain.

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance

2. Tutorial: Create a management VM to configure and administer an Azure Active Directory Domain Services management domain.

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-management-vm

3. Tutorial: Join a Windows Server virtual machine to an Azure Active directory Domain Service managed domain.

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/join-windows-vm

4. Tutorial: Configure secure LDAP for an Azure Active Directory Domain Services managed domain.

https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-configure-ldaps

5. LDAP Setup for WTI.

A few notes on setup:

When using SSL and Check Certificate is ON, the Primary Host and (secondary if defined) needs to be fully qualified name defined in the certificate and at least on DNS server needs to be defined to the name lookup and Fallback should be turn ON during setup, just in case.

To configure WTI device LDAP from CLI type /n option 27.

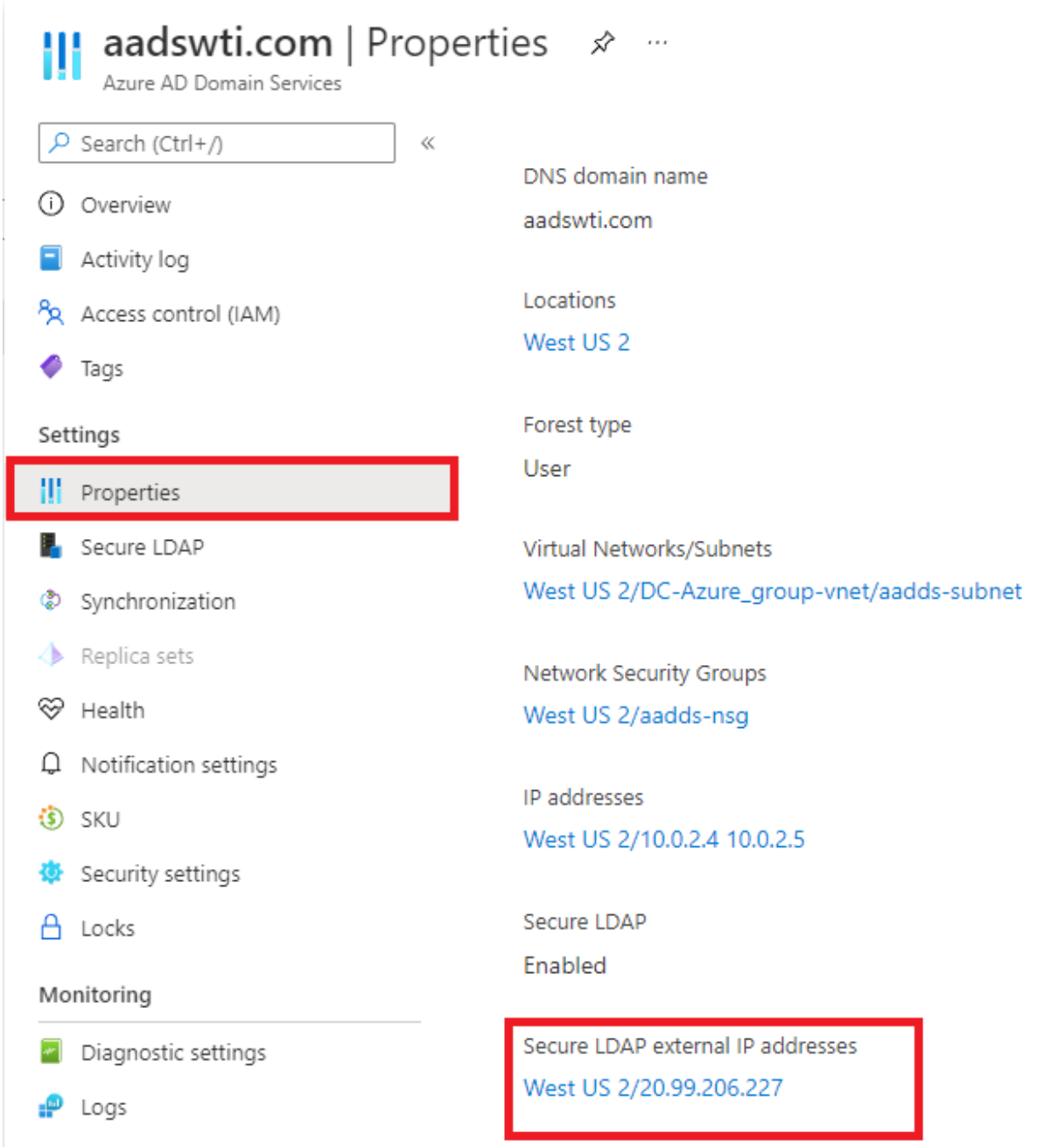
1. Enable: On
2. Primary Host/Address: ldaps.aadswti.com
3. Secondary Host/Address: (undefined)
4. LDAP Port: 636
5. TLS/SSL: SSL
   50. Check Certificate: On
   51. Import Certificate:
6. Bind Type: Simple
7. Search Bind DN: CN=ldapuser,OU=AADDC Users,DC=aadswti,DC=com
8. Search Bind Password: (defined)
9. User Search Base DN: DC=aadswti,DC=com
10. User Search Filter: sAMAccountName=%s
11. Group Membership Attribute: AAD DC Administrators
12. Group Membership Value Type: DN
13. Fallback: On
14. LDAP Group Setup
15. LDAP Kerberos Setup
16. Debug: Off
17. Ping Test

```
LDAP: [Shared]

1.  Enable:                         On
2.  Primary Host/Address:           ldaps.aadswti.com
3.  Secondary Host/Address:         (undefined)
4.  LDAP Port:                      636
5.  TLS/SSL:                        SSL
    50. Check Certificate:          On
    51. Import Certificate:
6.  Bind Type:                      Simple
7.  Search Bind DN:                 CN=ldapuser,OU=AADDC Users,DC=aadswti,DC
                                    =com
8.  Search Bind Password:           (defined)
9.  User Search Base DN:            DC=aadswti,DC=com
10. User Search Filter:             sAMAccountName=%s
11. Group Membership Attribute:     AAD DC Administrators
12. Group Membership Value Type:    DN
13. Fallback:                       On
14. LDAP Group Setup
15. LDAP Kerberos Setup
16. Debug:                          Off
17. Ping Test

Enter: #<CR> to change,
       <ESC> to return to previous menu ...
```

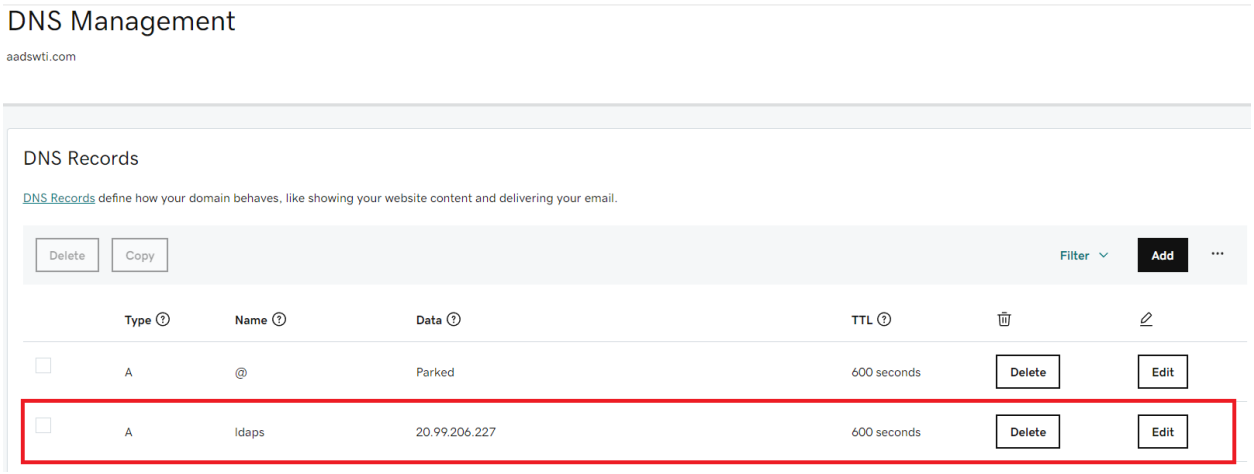
Configure DNS zone for external access

With secure LDAP access enabled over the internet, update the DNS zone so that client WTI device can find this managed domain. The *Secure LDAP external IP address* is listed on the **Properties** tab for your managed domain:

The following example DNS entry, either with your external DNS provider or in the local hosts file, resolves traffic for *ldaps.aaddswti.com* to the external IP address of *20.99.206.227*



In this example we will use GoDaddy as our external DNS provider. You will need to create an A record and point ***ldaps.aadswti.com to 20.99.206.227*** see screenshot below as example.



LDAP Setup Notes for WTI Products

In CLI /n option 27.

1. **Enable:** Turn LDAP on/off.

2. **Primary Host:** IP or fully qualified name of LDAP server. Example: **ldaps.aadswti.com**

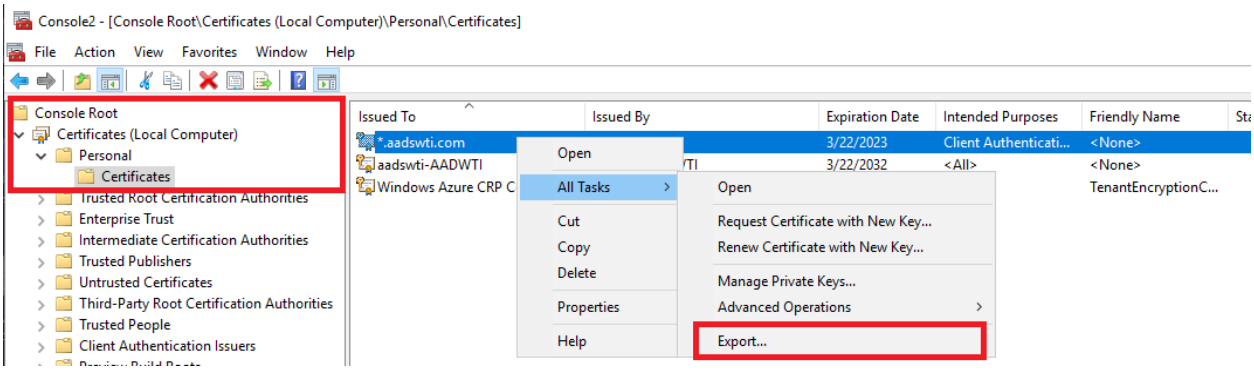
3. **Secondary Host:** IP or fully qualified names of the LDAP server.

4. **LDAP Port:** The number of the port that the LDAP server is listening on. Example: **636**

5. **TLS/SSL:** Turn LDAP encryption on.

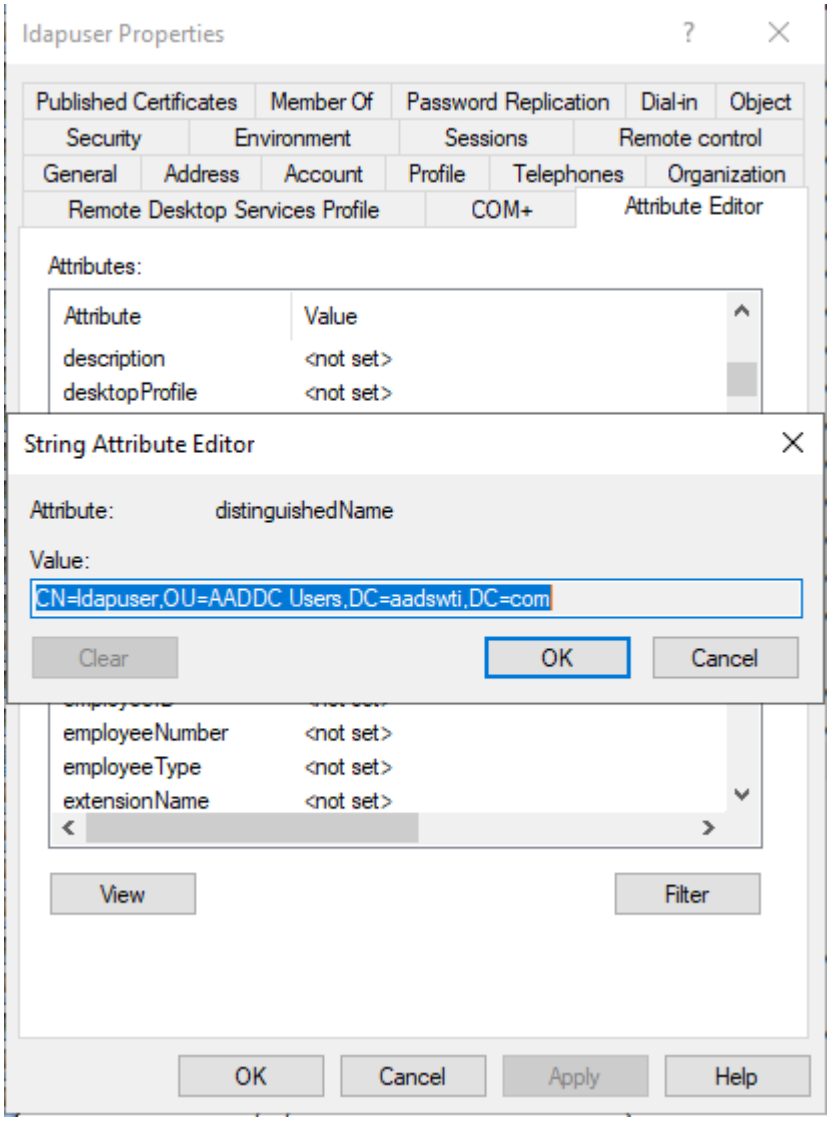
    50. **Check Certificate:** Make sure the FCN entered in 2 or 3 is the name in the certificate that was uploaded to prevent spoofing.

    51. **Import Certificate:** Import or upload certificate that export from Azure LDAP virtual machine server.



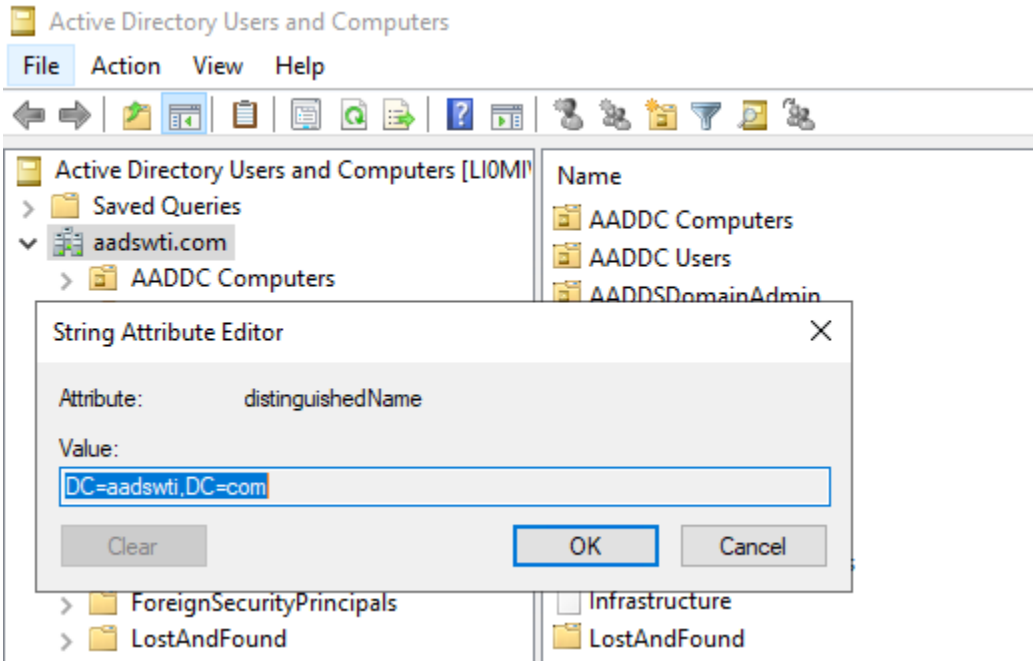
6. **Bind Type:** Essentially 1 (none) and 2 (Simple) are the same. Option 3 (Kerberos) turn on the Kerberos protocol.

7. **Search Bind DN:** This is the path to the user you are using to search the LDAP Tree for User lookup and Group lookup. This username must have sufficient rights to search the LDAP tree.

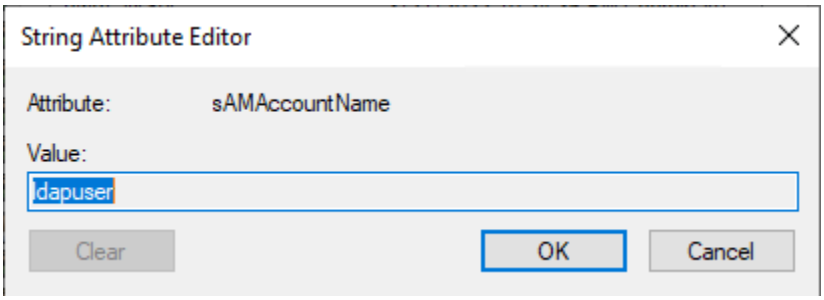


8. **Search Bind Password:** Password for the Search Bind DN user in item number 7.

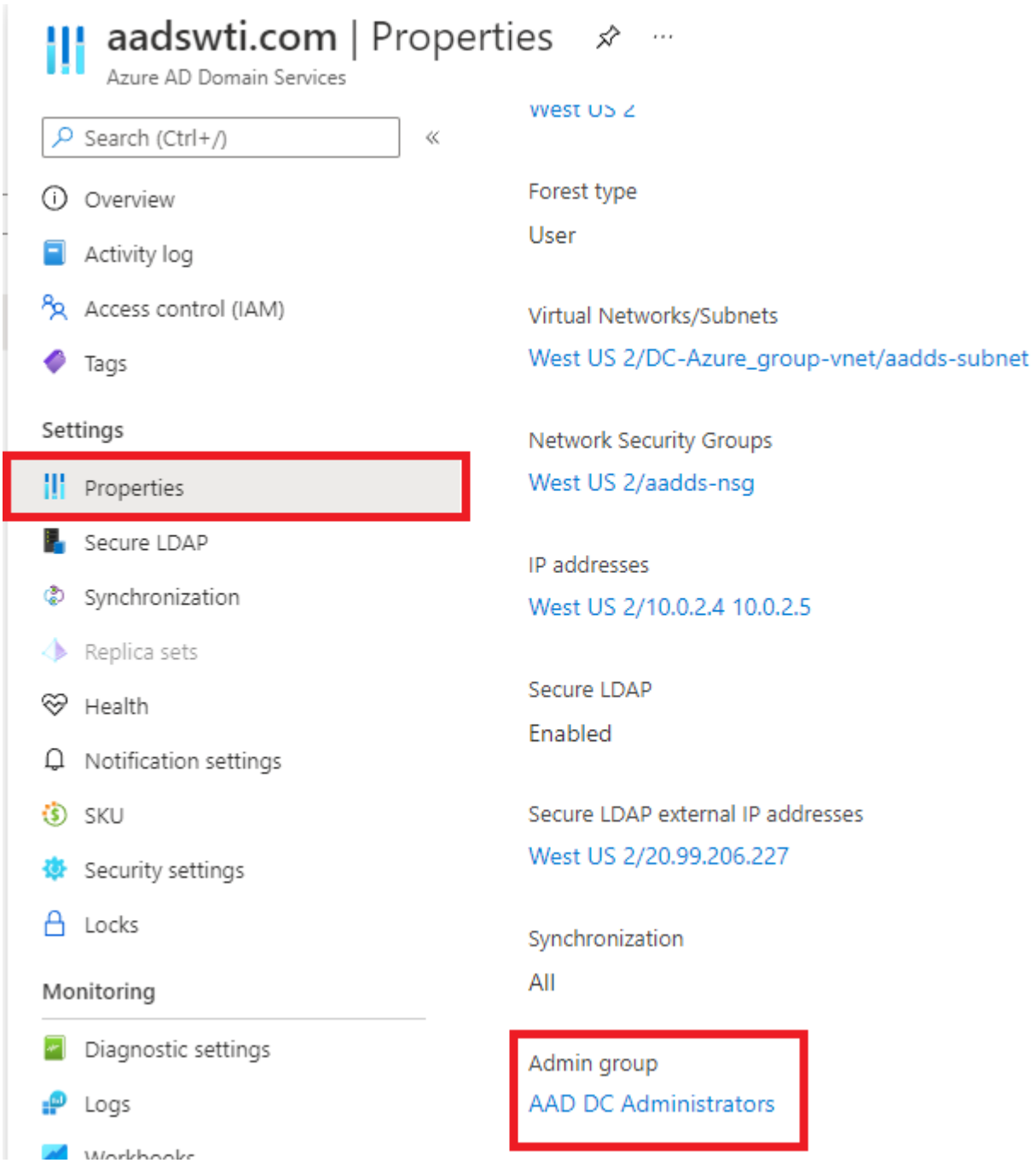
9. **User Search Base DN:** This is the starting point of our User and Group Search Activity. For debugging you could put this at the top of the tree, although this is time consuming on a full search and the rights of the Search Bind DN must be sufficient to do so.



10. **User Search Filter:** This is who the Username is matched to find the user and to find the user's Groups he is associated with **sAMAccountName=%s**



11. **Group Membership Attribute:** We define by using Admin group call **AAS DC Administrators** in Azure AD Domain Service under properties.



12. **Group Membership Value Type:** This item is compared against the group names.

13. **Fallback:** if ON, will search on the WTI box for users if the LDAP login fails.