Article Number: 000187932

Print

# Data Domain: How to configure DDOS LDAPs type active directory for AD user login LDAPs mode

Summary: Steps to configure DDOS for AD user login (LDAPs mode). "DDOS 7.6 or above," "type active-directory," and "Windows AD DS (Active-Directory Domain-Service)" are required.

## Article Content

Instructions

Summary
Steps to configure DDOS for AD user login (LDAPs mode).

Prerequisites

1. DDOS version: 7.6 or above (DDMC not supported)
2. DD LDAP configuration: "type active-directory" and LDAPs (not LDAP)
3. Windows AD DS (Active-Directory Domain-Service) (not AD LDS (Active-Directory Lightweight-Directory-Service))
4. LDAP Users, which require access to data domain, must have UID numbers assigned for them.
5. LDAP group, on which the above users belong to, should also have the GID numbers assigned as well.
    1. If UID or GID numbers are not configured then, assign the numbers with the value in the range of 1000-1,00,000 but not exceed 100 Million Number.
    2. If assistance is required to assign these UID or GID numbers with the value in the range of 1000-1,00,000, then follow the steps in How to troubleshoot?

- Section 2 Login failure
- Part 2.2) check AD DC configuration
- Part C configure missing UID or GID value in AD DC

* If any of the prerequisites (1->5) are not satisfied, then the login will not work. Ensure all the above steps are followed.

**CAUTION:**
1 Do not configure

```
authentication ldap type active-directory
```

If the customer has already accessed or will access DD CIFS share using AD user, because

1.1) LDAP authentication must be disabled before joining an Active Directory domain.

1.2) LDAP authentication with Active Directory cannot be used after joining an Active Directory domain.

2 LDAP configuration does not grant "data or CIFS share" access, but only logs in to DD UI or CLI for administration tasks.

How to configure:
1. Prepare AD DC Root CA certificate file (type: Base-64 encoded X .509, file extension: .cer)
* Note that Root CA certificate is the certificate of CA authority who signed all the intermediary CAs and all Domain Controller hosts. So kindly fetch that from the Customer Active Directory Administrator.

2. Upload AD DC cert file to DDOS /ddvar/certificates using CIFS or NFS

3. Import AD DC cert file to DDOS

```
adminaccess certificate import ca application ldap file <file-name>
```

Example

```
adminaccess certificate import ca application ldap file dc22.cer
```

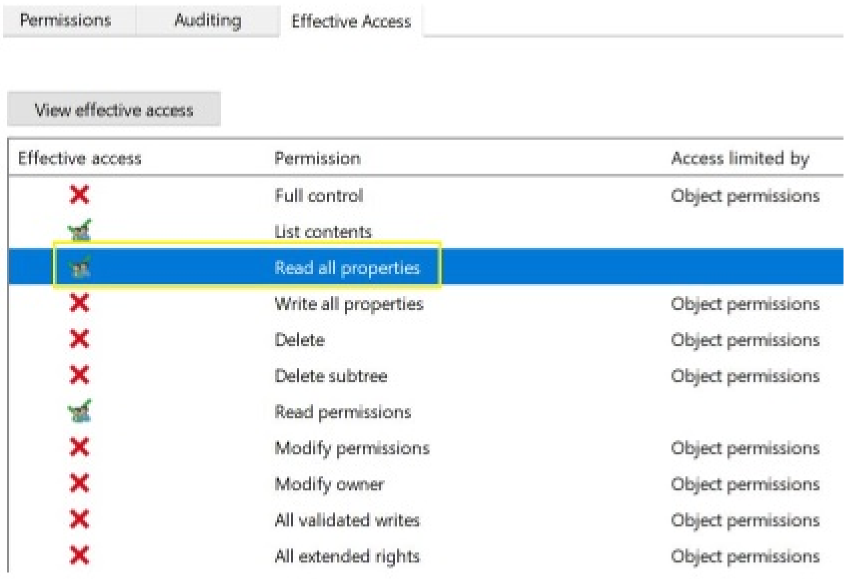
```
4. Configure and enable DDOS auth LDAPs for AD


4.1)
```

```
authentication ldap base set “<distinguishedName_for_search>" type active-directory
```

```
4.2)
```

```
authentication ldap client-auth set binddn "<distinguishedName_for_bind_account>"
```

```
         * enter password as prompted
         * The binddn(service account) must have Read all Permissions like below.
         AD DC: User Account Properties -> Security -> Advanced -> Effective Access -> Select a User -> View Effective Access
```



| Effective access | Permission | Access limited by |
|---|---|---|
| ✗ | Full control | Object permissions |
| ✓ | List contents | |
| ✓ | Read all properties | |
| ✗ | Write all properties | Object permissions |
| ✗ | Delete | Object permissions |
| ✗ | Delete subtree | Object permissions |
| ✓ | Read permissions | |
| ✗ | Modify permissions | Object permissions |
| ✗ | Modify owner | Object permissions |
| ✗ | All validated writes | Object permissions |
| ✗ | All extended rights | Object permissions |

```
4.3)
```

```
authentication ldap server add <AD_DC_FQDN>
```

```
         * use FQDN only or add :636 after FQDN


4.4)
```

```
authentication ldap ssl enable method ldaps
```

```
         * or
```

```
authentication ldap ssl enable method start_tls
```

```
4.5)
```

```
authentication ldap ssl set tls_reqcert demand
```

```
4.6)
```

```
authentication ldap groups add <AD-group-name> role <dd-role-name>
```

```
4.7)
```

```
authentication ldap enable
```

```
Example for 4.1->4.7
```

```
4.1) authentication ldap base set "CN=Users,DC=abc,DC=com" type active-directory

4.2) authentication ldap client-auth set binddn "CN=administrator,CN=Users,DC=abc,DC=com"
         * enter password as prompted

4.3) authentication ldap server add dc.abc.local
         * or
     authentication ldap server add dc.abc.local:636

4.4) authentication ldap ssl enable method ldaps
         * or
     authentication ldap ssl enable method start_tls

4.5) authentication ldap ssl set tls_reqcert demand

4.6) authentication ldap groups add "domain admins" role admin

4.7) authentication ldap enable
```

How to log in:
Log in to DD UI or CLI using <AD_user_name>, without <domain_name>
Example

```
admin
```

```
(not corp\admin)



How to troubleshoot?
1. Enable failure
Check /ddr/var/log/debug/messages.engineering for ldapsearch command and output using DD CLI.
```

```
log view /ddr/var/log/debug/messages.engineering
```

```
2. Login failure

2. 1) Check DD configuration
```

a. Does

```
authentication ldap show
```

report "Server Type: Active Directory"?
If no, run again

```
authentication ldap base set <base> type active-directory
```

Example

```
authentication ldap base set "CN=Users,DC=abc,DC=com" type active-directory
```

b. Does

```
authentication ldap groups show
```

Report "any domain group assigned with DD user role"?
If no, run again

```
authentication ldap groups add <AD-group-name> role <dd-role-name>
```

Example

```
authentication ldap groups add "domain admins" role admin
```

c. Could DD query AD user, group from AD DC using DD CLI bash mode (Support required)? If no, DD fails to communicate to AD DC.
Query user

```
id <AD_user_name>
```

Example

```
id admin
```

```
Query group
```

```
getent group "<AD_group_name>"
```

```
Example
```

```
getent group "domain admins"
```

```
2.2) Check AD DC configuration
```

Run Windows PowerShell as administrator

a. Does ad_user have uidNumber, gidNumber assigned?
Check uidNumber

```
get-aduser <ad_user> -properties *|findstr uidNumber
```

Example

```
get-aduser admin -properties *|findstr uidNumber
```

```
Check gidNumber
```

```
get-aduser <ad_user> -properties *|findstr gidNumber
```

```
Example
```

```
get-aduser admin -properties *|findstr gidNumber
```

```
b. Does ad_group have gidNumber assigned?
Check gidNumber
```

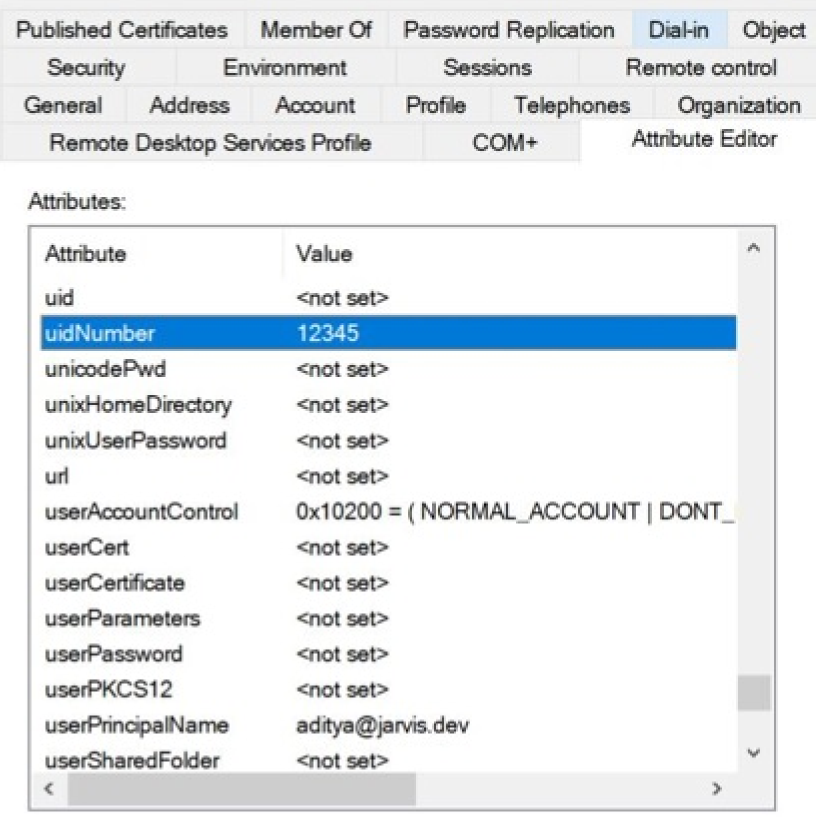
```
get-adgroup <ad_group> -properties *|findstr gidNumber
```

```
Example
```

```
get-adgroup "domain admins" -properties *|findstr gidNumber
```

c. If no numbers are seen in any of the above, configure missing value in
AD DC "Administrative Tools - Active Directory Users and Computers"

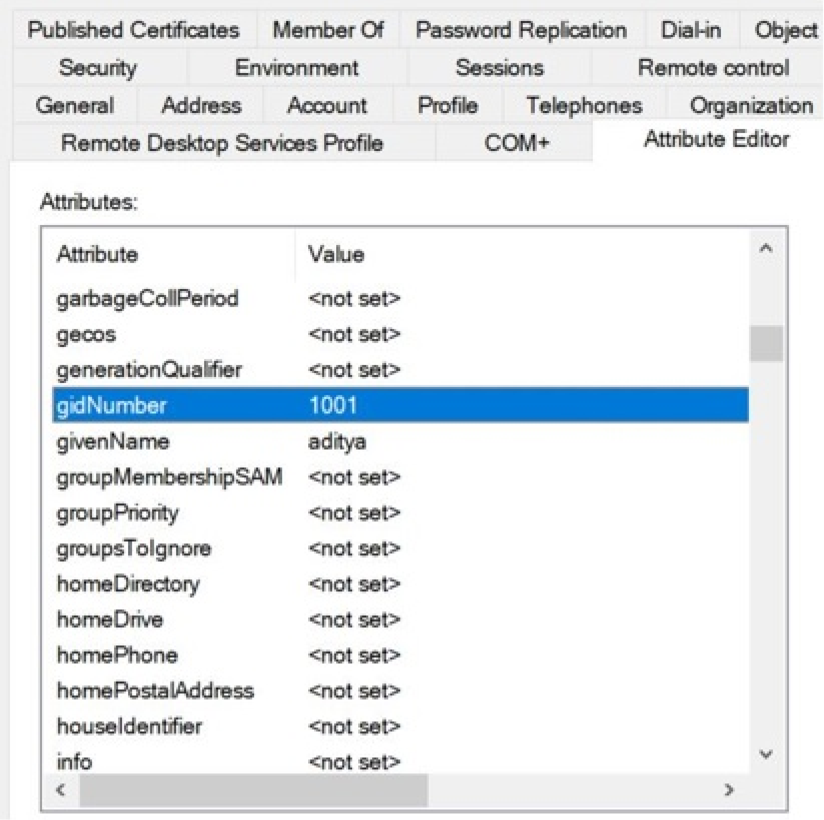
AD user UID or GID
User Properties -> Attribute Editor -> uidNumber and gidNumber
uidNumber



Attributes:

| Attribute | Value |
|---|---|
| uid | <not set> |
| uidNumber | 12345 |
| unicodePwd | <not set> |
| unixHomeDirectory | <not set> |
| unixUserPassword | <not set> |
| url | <not set> |
| userAccountControl | 0x10200 = ( NORMAL_ACCOUNT \| DONT_ |
| userCert | <not set> |
| userCertificate | <not set> |
| userParameters | <not set> |
| userPassword | <not set> |
| userPKCS12 | <not set> |
| userPrincipalName | aditya@jarvis.dev |
| userSharedFolder | <not set> |

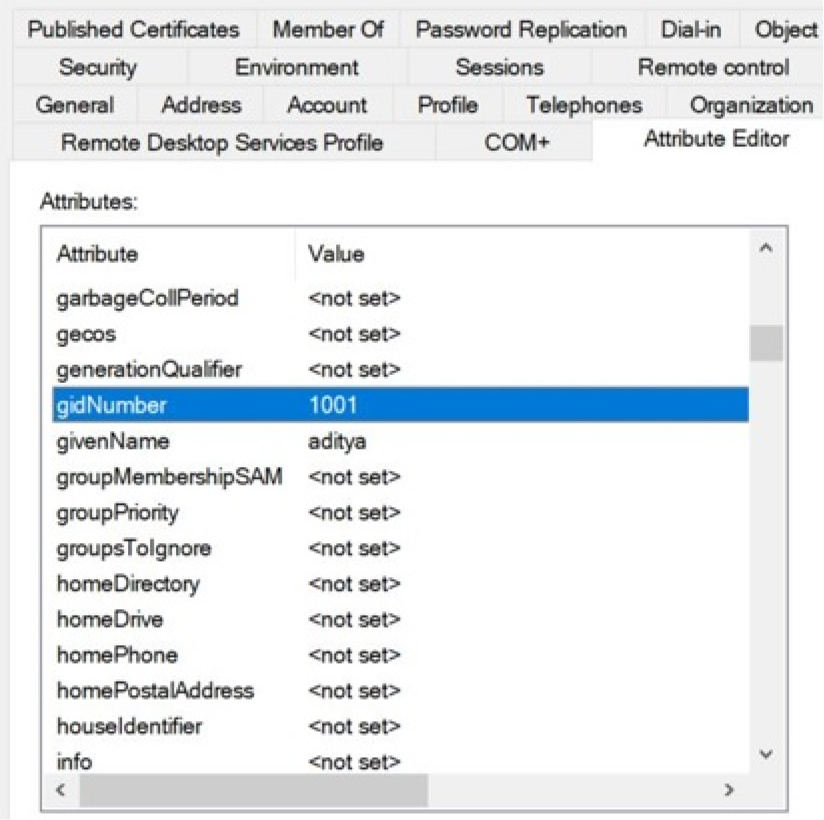
gidNumber



Attributes:

| Attribute | Value |
|---|---|
| garbageCollPeriod | <not set> |
| gecos | <not set> |
| generationQualifier | <not set> |
| gidNumber | 1001 |
| givenName | aditya |
| groupMembershipSAM | <not set> |
| groupPriority | <not set> |
| groupsToIgnore | <not set> |
| homeDirectory | <not set> |
| homeDrive | <not set> |
| homePhone | <not set> |
| homePostalAddress | <not set> |
| houseIdentifier | <not set> |
| info | <not set> |

AD group GID
Group Properties -> Attribute Editor -> gidNumber
gidNumber



Attributes:

| Attribute | Value |
|---|---|
| garbageCollPeriod | <not set> |
| gecos | <not set> |
| generationQualifier | <not set> |
| gidNumber | 1001 |
| givenName | aditya |
| groupMembershipSAM | <not set> |
| groupPriority | <not set> |
| groupsToIgnore | <not set> |
| homeDirectory | <not set> |
| homeDrive | <not set> |
| homePhone | <not set> |
| homePostalAddress | <not set> |
| houseIdentifier | <not set> |
| info | <not set> |

2.3) If the Log in prompt takes too long to respond or if it keeps spinning, or if there are lot of messages in messages.engineering about fetching uid/gid numbers for a larger LDAP group then there could be a chance that ldap_result request would have timed out or filling the log with lot of messages.

* In order to verify whether you are running into the issue, kindly check messages, engineering using Putty session, and "log view debug or

messages.engineering" and look for a word called ldap_result timedout message.

* Once you confirm that is the issue, we could troubleshoot the search criteria that LDAP Domain uses to look over and manage it using the CLI, by adding the base group to match the same LDAP group that was added in previous steps using

```
authentication ldap groups add
authentication ldap disable
authentication ldap config add "base group <CN=CNNAME>,OU=**,OU=**,DC=**,DC=**,DC=**,DC=**"
authentication ldap enable
```

* Kindly ensure that you have the proper information of the OU and CN name for the base group <dn> to ensure it matches the one used in the earlier step.

## Article Properties

**Last Published Date**

29 Jan 2024

**Version**

16

**Article Type**

How To