

SVC and Storwize V7000 Release 6.3: Configuring LDAP

Once your SVC or Storwize V7000 is upgraded to version 6.3 you can start using LDAP for authentication. This means that when you logon, you authenticate with your domain user-id and password rather than a locally created user-id and password.

So why is this important?

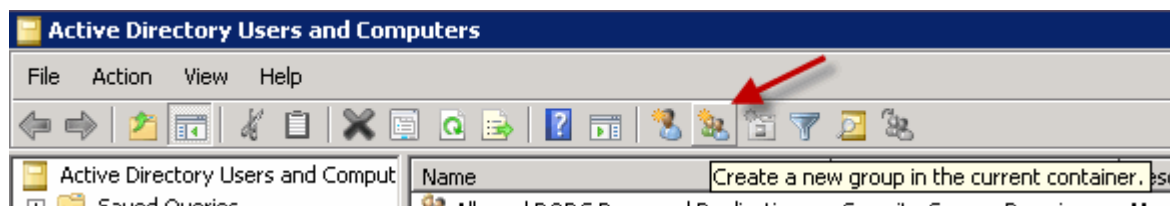
- It saves you having to configure every user on every SVC or Storwize V7000. If you have multiple machines this makes it far more efficient to set up authentication.
- It means that when commands are executed on the SVC or Storwize V7000, the audit log will show the domain username that issued that command, rather than a local username, or worse just superuser (i.e. who mapped that volume? The superuser did.... who?)
- It gives you central control over access. If someone leaves the company you just need to remove access at the domain controller, meaning there won't be orphan user-ids left on your Storage equipment.

So as an exercise I added my lab Storwize V7000 to our domain to show how it is done. This example also applies to an SVC so don't be confused if I only refer to Storwize V7000 from now on.

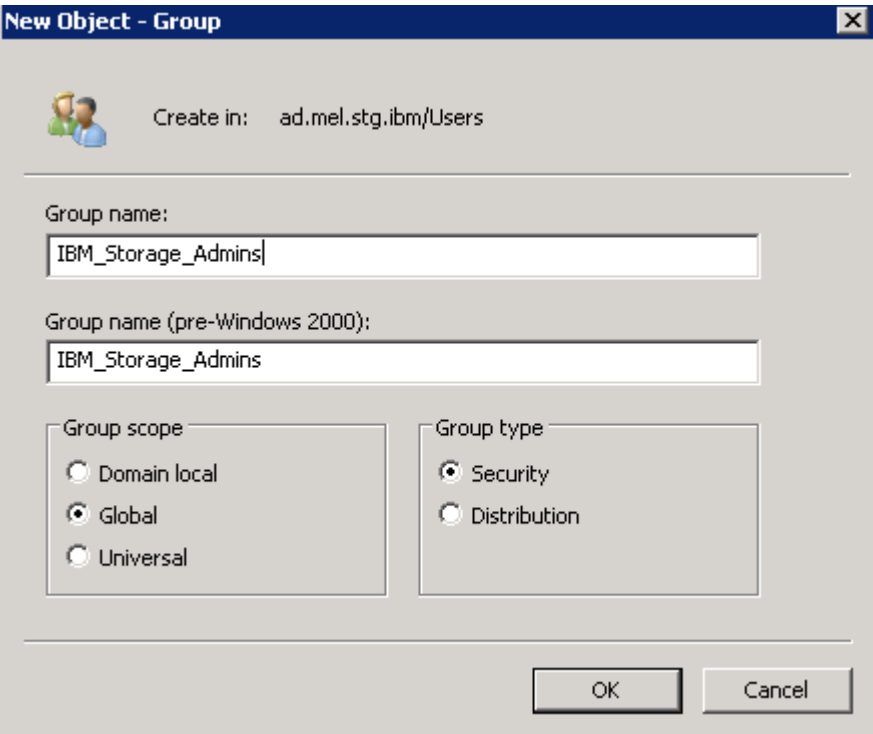
The first task is to negotiate with your Domain administrator to get a new group setup on the domain. In this example I use a group called *IBM_Storage_Admins* which lets me use this group for various storage devices (such as an XIV or a SAN Switch).

To create this group we need to logon to the Domain Controller and configure Active Directory. An easy way to do this from the AD controller is to go to **Start** → **Run** and type **dsa.msc** and hit **OK**. The Active Directory Users and Computers Management Console should open.

Select the groups icon to create a new group.



Enter your group name, in my case: *IBM_Storage_Admns* and hit **OK**.



New Object - Group

Create in: ad.mel.stg.ibm/Users

Group name:
IBM_Storage_Admns

Group name (pre-Windows 2000):
IBM_Storage_Admns

Group scope

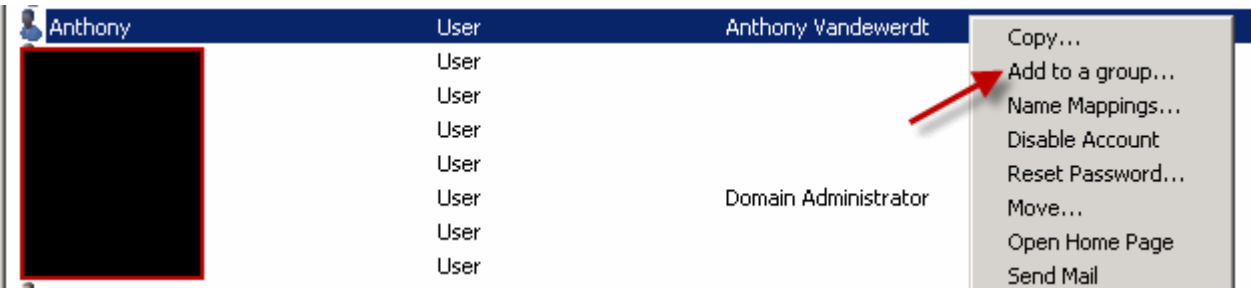
- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type

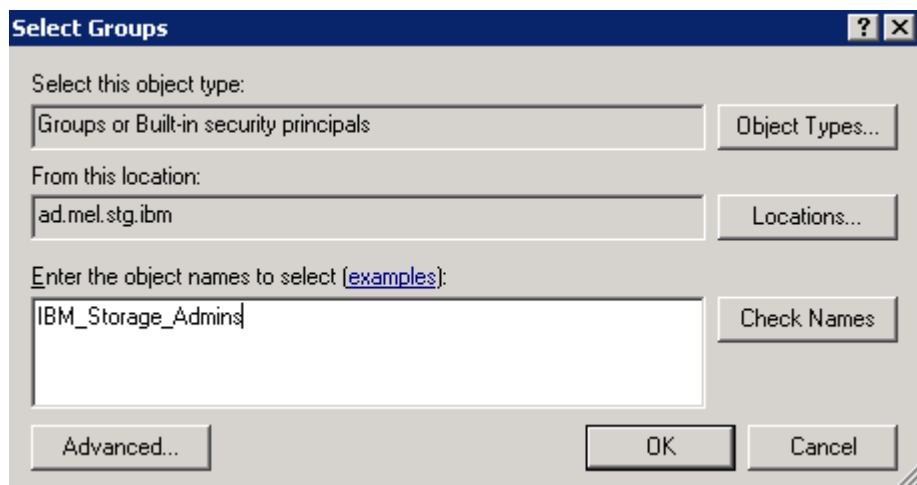
- ☒ Security
- ☐ Distribution

OK Cancel

Now right select relevant users who need access to the storage and add them to the *IBM_Storage_Admns* group. In this example I have selected *Anthony* (which uses *anthonyv* as a username).

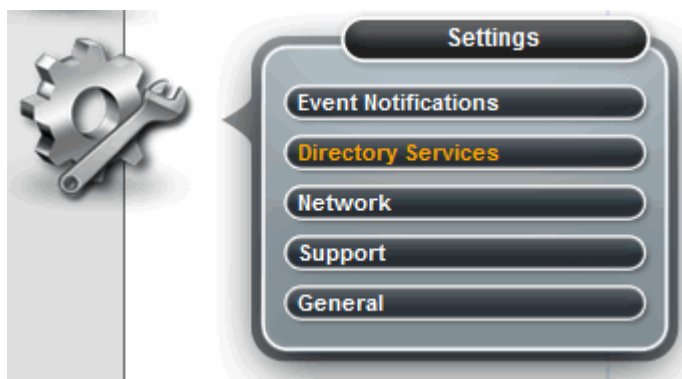


In this example we are adding *anthony* into the *IBM_Storage_Admns* group:

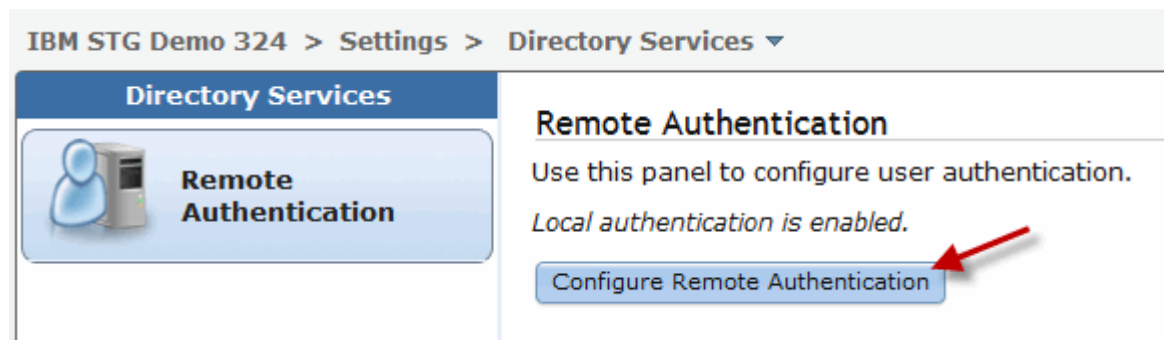


Now it is time to configure the Storwize V7000 so start the Web GUI and logon as Superuser.

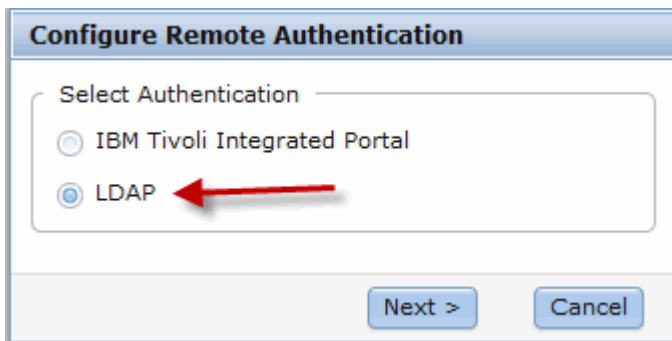
Firstly we go to **Settings** → **Directory Services**:



We choose the button to **Configure Remote Authentication**:




We choose LDAP and hit next.



Configure Remote Authentication

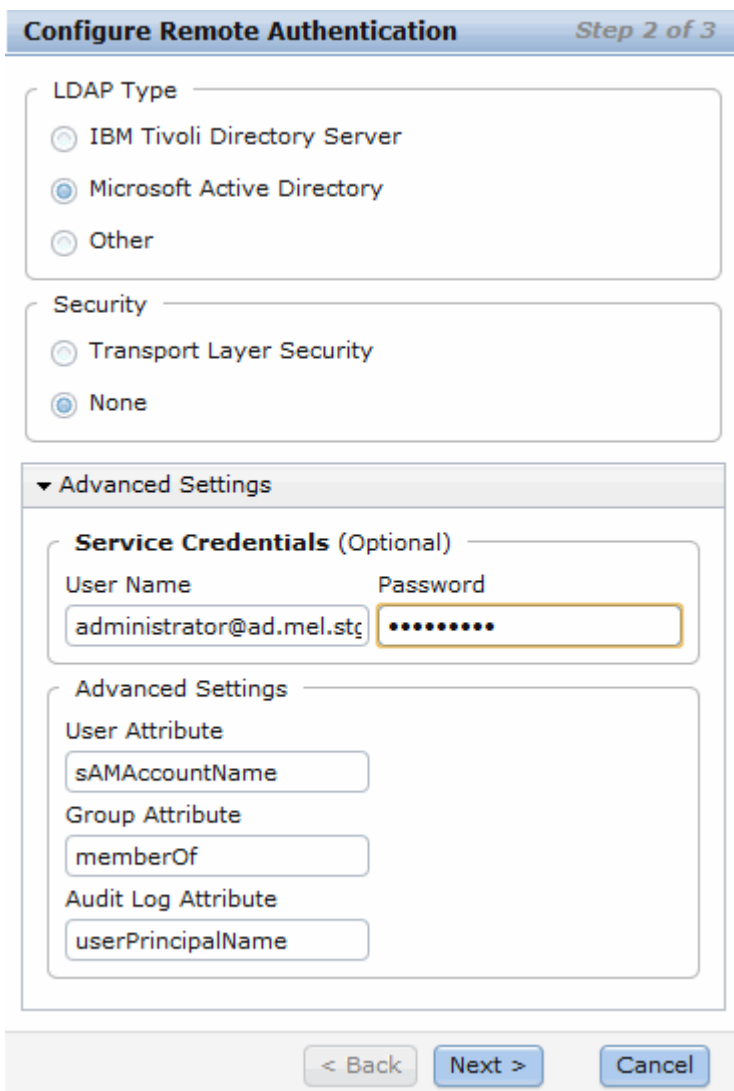
Select Authentication

☐ IBM Tivoli Integrated Portal

☒ LDAP 

Next > Cancel

We choose Microsoft Active Directory with no Transport layer Security. We then expand the **Advanced Settings**. My lab domain is *ad.mel.stg.ibm* so I use the Administrator ID on the Domain Controller to authenticate access. You could use any user that has authority to query the LDAP directory. We then hit **Next**.



Configure Remote Authentication *Step 2 of 3*

LDAP Type

☐ IBM Tivoli Directory Server

☒ Microsoft Active Directory

☐ Other

Security

☐ Transport Layer Security

☒ None

▼ Advanced Settings

Service Credentials (Optional)

User Name Password

administrator@ad.mel.stg

Advanced Settings

User Attribute

sAMAccountName

Group Attribute

memberOf

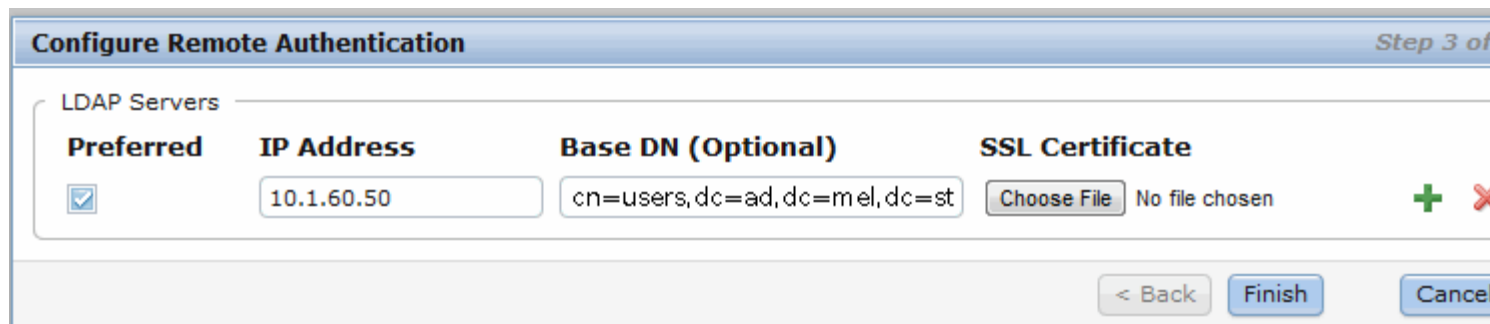
Audit Log Attribute

userPrincipalName

< Back Next > Cancel

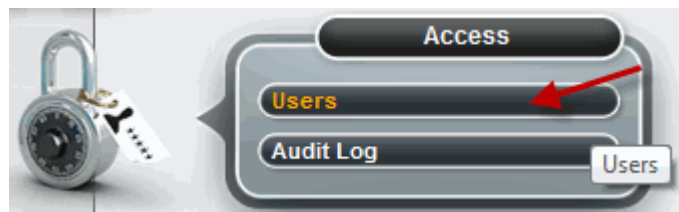
We then add the domain controller which in this example is 10.1.60.50 and the base domain name

chopped into pieces (so ad.mel.stg.ibm becomes cn=users,dc=ad,dc=mel,dc=stg,dc=ibm) and hit **Finish**.

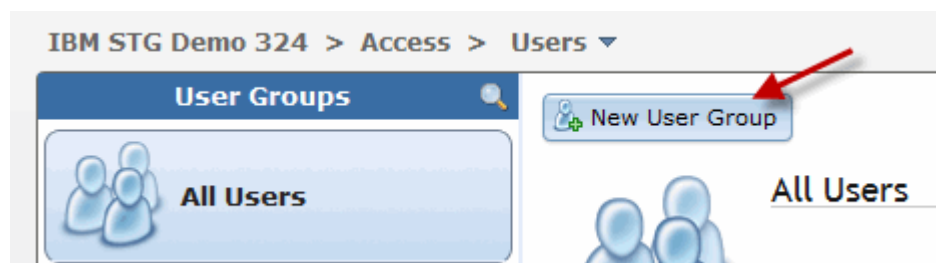


Preferred	IP Address	Base DN (Optional)	SSL Certificate
<input checked="" type="checkbox"/>	10.1.60.50	cn=users,dc=ad,dc=mel,dc=st	Choose File No file chosen

Provided the command completes successfully we have defined the domain controller to the Storwize V7000. Now we need to add a group. Go to **Access** → **Users**.



Select the option to add a **New User Group**.



In this example we want to add a group for users allowed full admin access to the Storwize V7000. This matches the group we created on the Domain Controller. So we call the group *IBM_Storage_Admns* and we use the Security Administrator role (which is the most powerful role) and tick the box to enable LDAP for this group.

New User Group

Group Name

Role

☐ Monitor

☐ Copy Operator

☐ Service

☐ Administrator ?

☒ Security Administrator ?

Remote Authentication

LDAP

☒ Enable for this group

Now to test, I logon to the Storwize V7000 using the domain user-id anthonyv with that users domain password. Remember this user is not defined on the Storwize V7000 itself and that if it all goes wrong, we can still logon as Superuser.

Storwize® V7000
Storage Management

User Name:

Password:

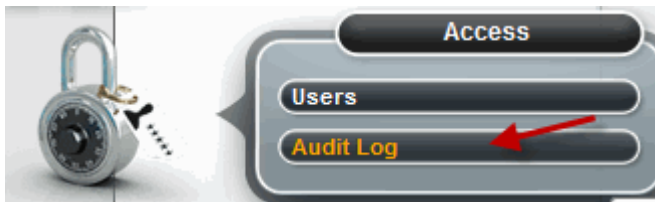
☐ Low graphics mode

Login

Licensed Material - Property of IBM Corp. © IBM Corporation and other(s) 2011. IBM and Storwize are registered trademarks of the IBM Corporation in the United States, other countries, or both.



Now I create a volume and delete it. Then I check the audit log from **Access** → **Audit log**.

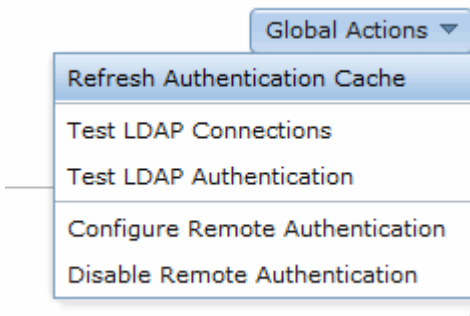


Sure enough, we see exactly who did that command.

IBM STG Demo 324 > Access > Audit Log ▾			
⋮ Actions ▾ ↻ Refresh			
Date and Time ▾	User Name	Command	Object ID
11/29/11 7:41:59 PM	AnthonyV@ad.mel.stg.ibm	svctask rmvdisk -force 6	
11/29/11 7:41:51 PM	AnthonyV@ad.mel.stg.ibm	svctask mkvdisk -name ddd -iogrp io_grp0 -mdiskgrp 'GM Test' -...	6

This is a great outcome for security, auditing and for easy access administration.

If you have issues, from the **Settings** → **Directory Services** menu, use the **Global Actions** dropdown on the right hand side to Test LDAP Connections and Authentication or re-configure LDAP.



By: anthonyv - corrections by tc