SERVICENOW
LDAP INTEGRATION

REVANTH KARRA

ServiceNow Integrations|ITOM

revanth-karra

karrarevanth325@gmail.com

Hyderabad, India

ServiceNow LDAP Integration

What is LDAP?

Lightweight Directory Access Protocol (LDAP) is a protocol that helps applications find and access information about users, groups, and other resources in a network.

How?

Imagine that you have a large company with hundreds of employees. Each employee has a name, email address, phone number, and other information. You could store this information in a spreadsheet, but that would be difficult to manage and keep up to date. A better solution would be to use a directory service, such as LDAP. LDAP would store all of the employee information in a central location. Any application that needs to access this information could then query the LDAP directory.

Example:

When an employee logs in to their computer, the computer could query the LDAP directory to verify their identity and grant them access to their resources. Similarly, when an employee tries to print a document, the printer could query the LDAP directory to see if the employee is authorized to use it.

Pre-requisites:

- You must have an LDAP server. This can be a commercial LDAP server, such as Microsoft Active Directory, or an open source LDAP server, such as OpenLDAP.
- You must have a network connection between the LDAP server and the applications or services that will be using it.
- You must have the necessary permissions to configure and manage the LDAP server, user, accounts and groups.

TIPS:

- Make sure that your LDAP server is properly configured and secured.
- Use strong passwords for all LDAP user accounts.
- Regularly back up your LDAP server data.
- Have a plan in place for recovering from an LDAP outage.

For this Demo, I'm going use Public Open Source LDAP (FORUM SYSTEMS)

Link: https://www.forumsys.com/2022/05/10/online-ldap-test-server/

- We can get all the LDAP server Information here.
- This is a Public Open Source URL, which we can test in our Instance.

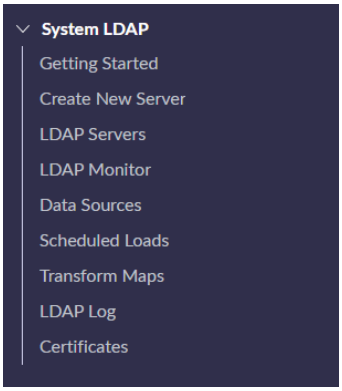
NOTE:

We only have read-only access to this LDAP server.

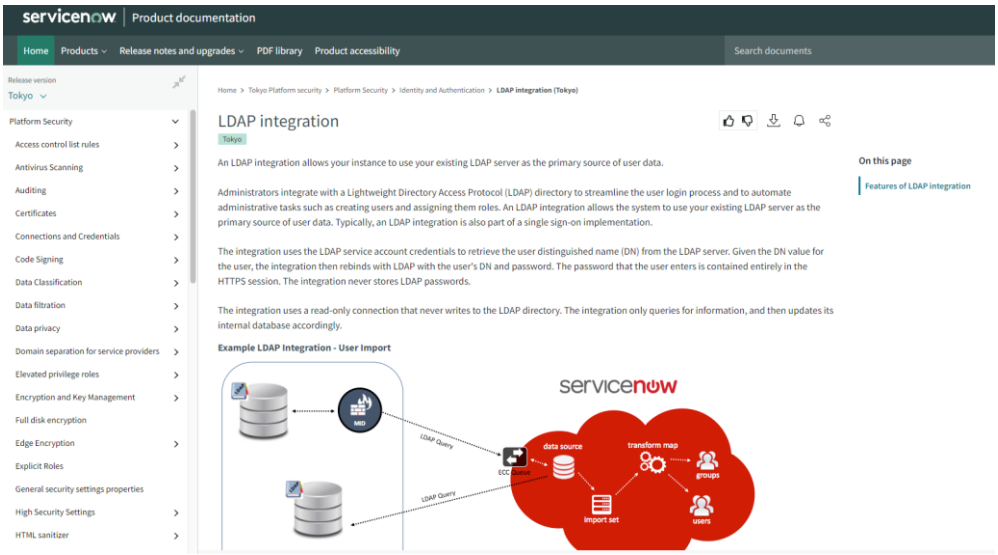
Let’s get started!

Initially, let us check all the modules present in this System LDAP

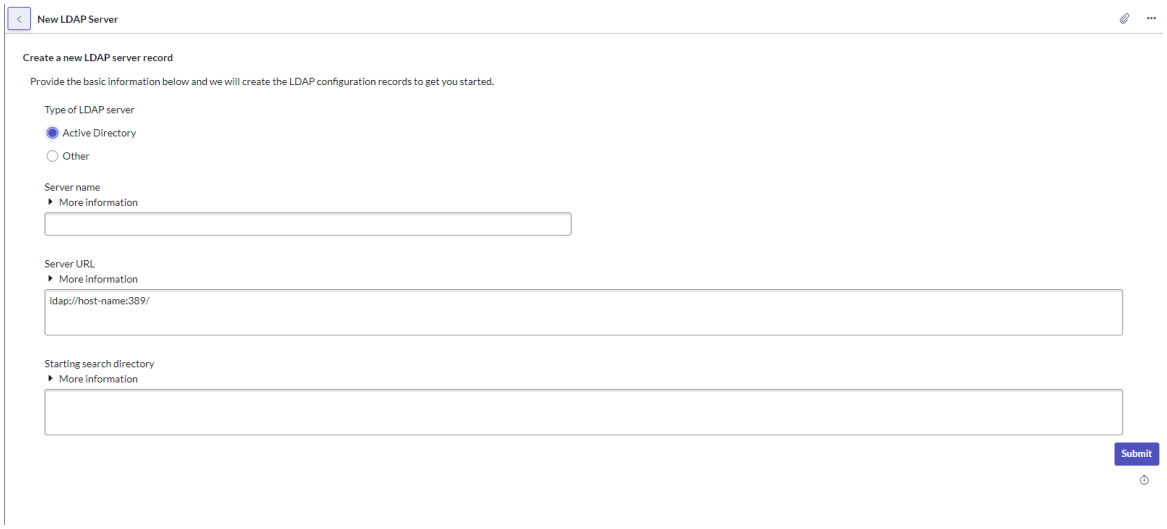
- For LDAP server, we have module in ServiceNow known as System LDAP



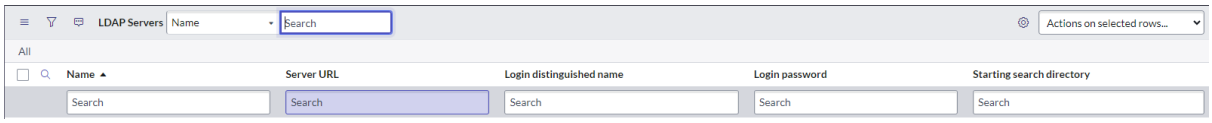
- If we click on Getting Started, we will redirect to LDAP product documentation by ServiceNow.



- If we click on Create New Server, we can see new LDAP Server record.

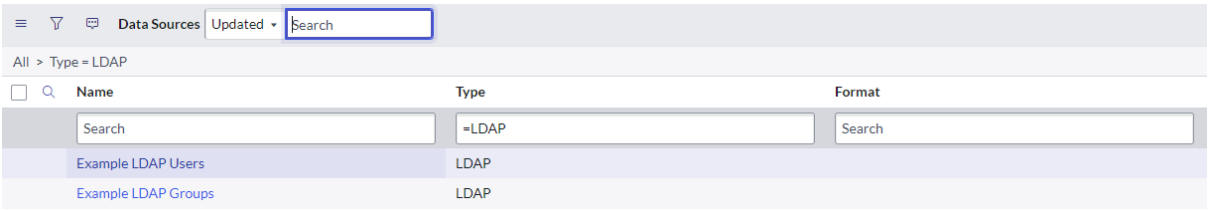


- If we click on LDAP Servers, it will show us all the LDAP Servers configured in our instance.

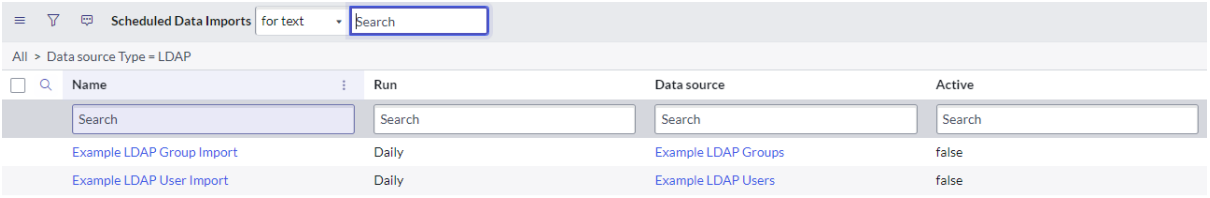


- If we click on LDAP Monitor, which shows the status of our LDAP whether it is connected or down or not connected. At present I don't have any active LDAP Server.

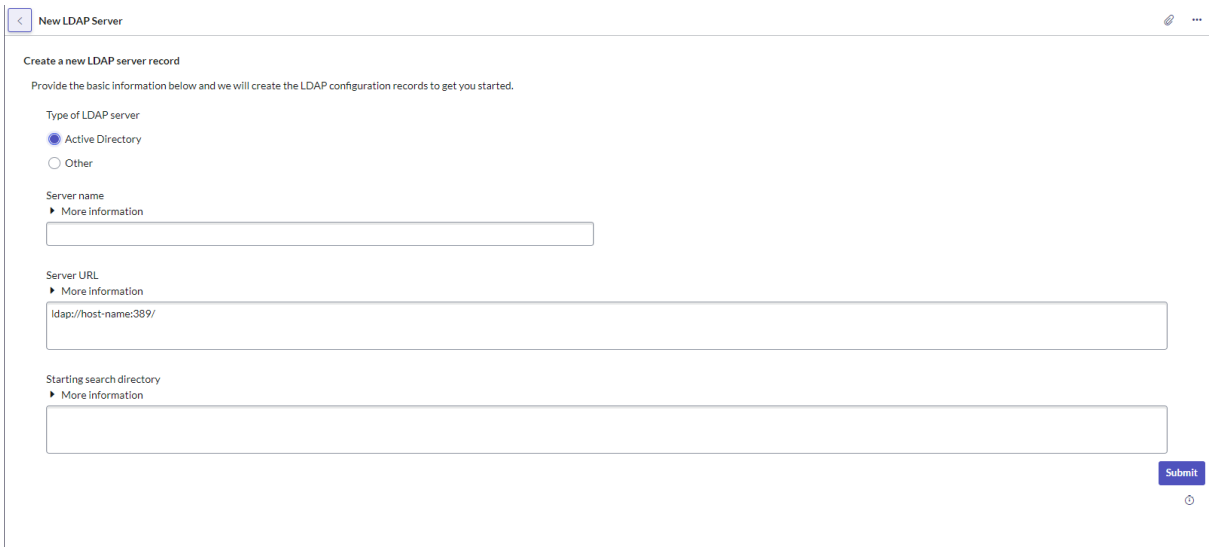
- If we click on Data Sources, we can see Data Sources in this record and these data sources are for Import.



- Basically, LDAP is being used to import Users and Groups of your organization. So, in your AD if you want to import some of your users and groups. You can use LDAP.
- Now let's go to schedule loads, if we need to run our scheduled imports. We can do it from here.



Let’s Create a new LDAP Server record



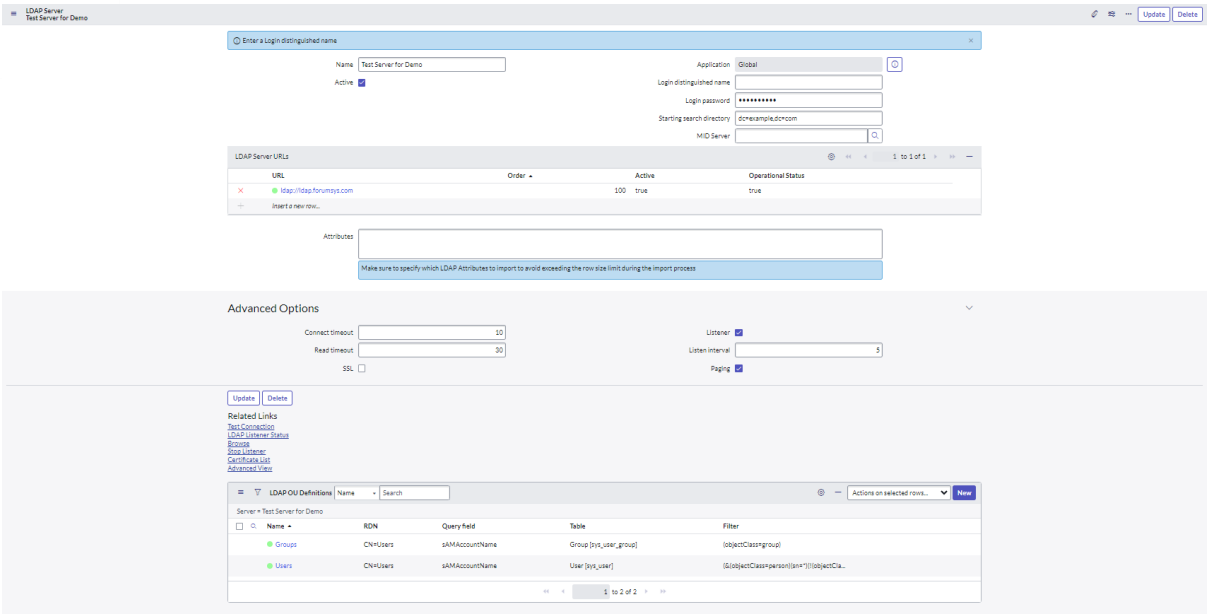
- Let’s make Active Directory option as default, Give a server name (example.: Test Server for Demo)
- For Server URL, let’s go to our Online LDAP Test Server website. Our Server URL is *ldap.forumsys.com*

LDAP Server Information (read-only access): Server: *ldap.forumsys.com* Port: *389* Bind DN: *cn=read-only-admin,dc=example,dc=com* Bind Password: *password*
All user passwords are *password*. You may also bind to individual Users (uid) or the two Groups (ou) that include: *ou=mathematicians,dc=example,dc=com*

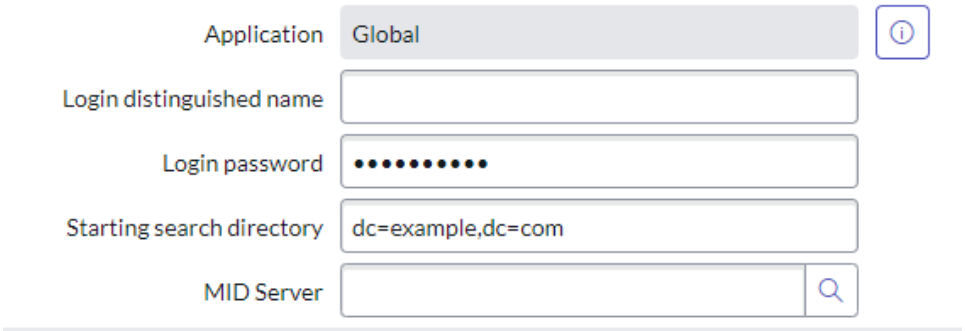
- Make sure our Server URL is in this format. (Example.: ldap://ldap.forumsys.com)
- In the Starting search directory column, we need to mention where exactly our LDAP will look for the Users.

All user passwords are *password*. You may also bind to individual Users (uid) or the two Groups (ou) that include: *ou=mathematicians,dc=example,dc=com*

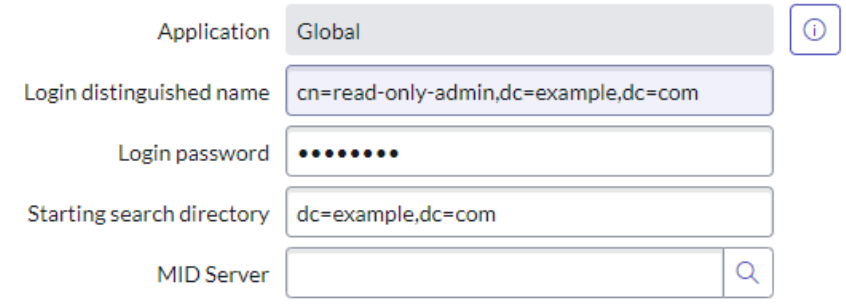
- From above credentials from our FORUM SYSTEMS website, let’s take *dc=example,dc=com* details and Insert it into our Starting search directory column.
- Click on Submit, it will create LDAP server record.



- We need to provide Login distinguished name.

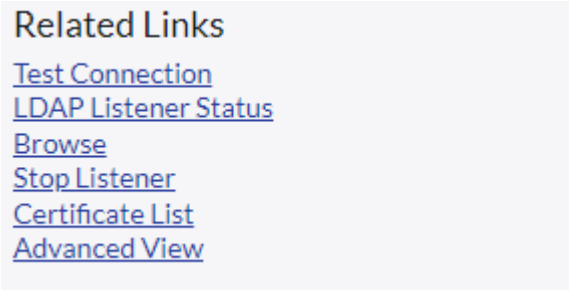


- For this we need to go to our FORUM SYSTEMS website and Copy Bind Distinguished Name (DN) and Password *(*Bind DN: *cn=read-only-admin,dc=example,dc=com* Bind Password: *password)*
- Now right click on the LDAP Server header and hit Save.

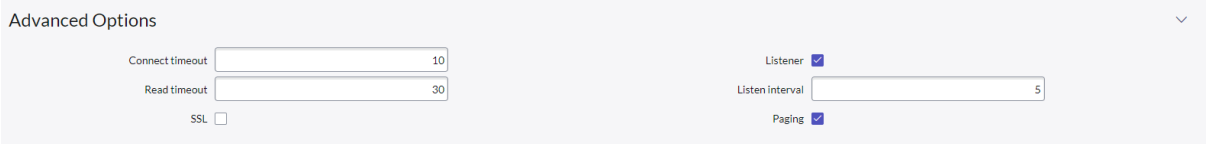


- Now we can see connected successfully prompt on the top.

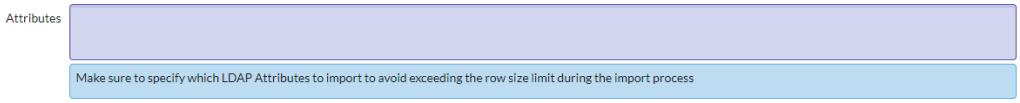
- If we need to test the connection again, just scroll little bit down and we can see Test Connection option under related links.



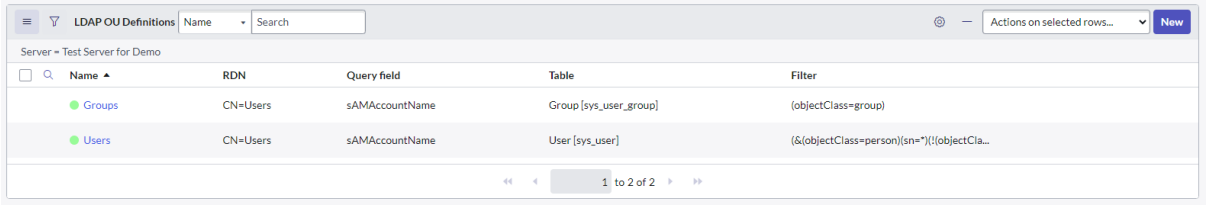
- We have configured our LDAP Server. Now if we can see, it also updated few settings under Advanced Options like connect timeout, Read timeout, Listen interval, Listener and paging.
- Listener option monitors LDAP server for changes and updates the ServiceNow user and group tables accordingly.
- Paging option allows ServiceNow to import large numbers of LDAP users and groups in manageable chunks.



- LDAP, basically has lot of attributes that means it has lot of columns like email, userid, account status etc.,



- We can mention what ever fields we want to import.
- If we can see, it automatically created 2 OU Definitions. One is for Groups and one is for Users.



- If we go to our LDAP Server on FORUM SYSTEMS, this particular website provided us these user details.

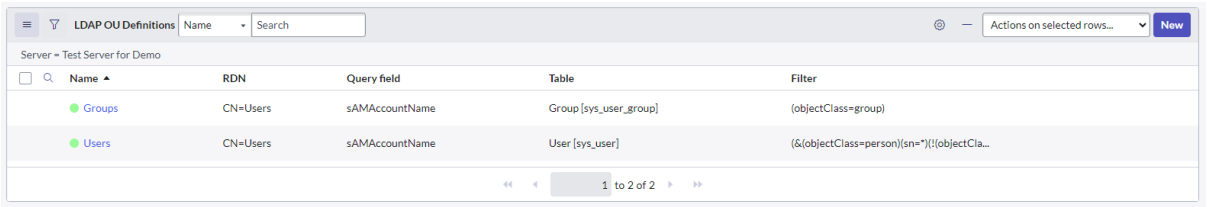
ou=mathematicians,dc=example,dc=com

- *riemann*
- *gauss*
- *euler*
- *euclid*

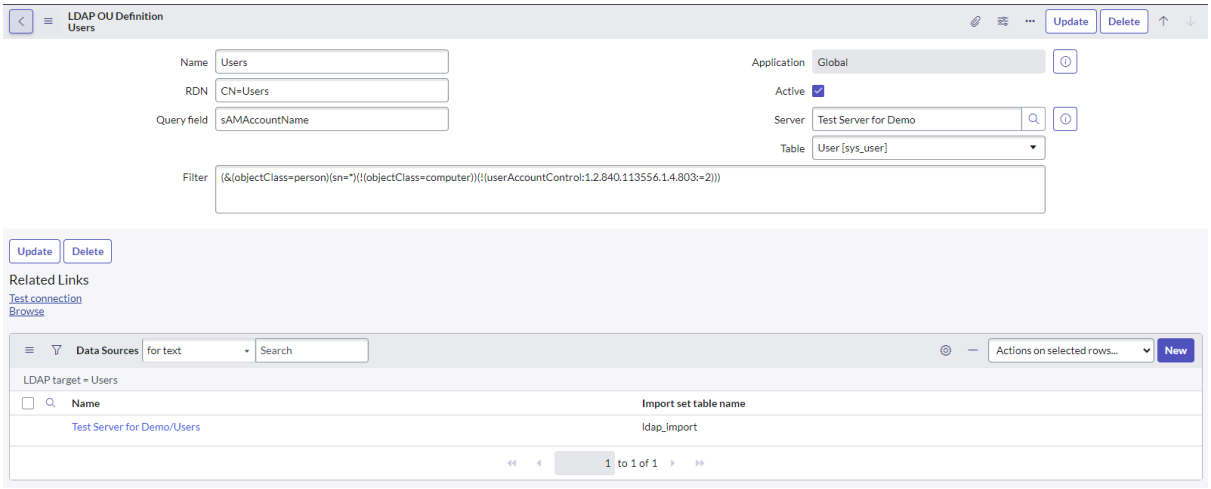
ou=scientists,dc=example,dc=com

- *einstein*
- *newton*
- *galieleo*
- *tesla*

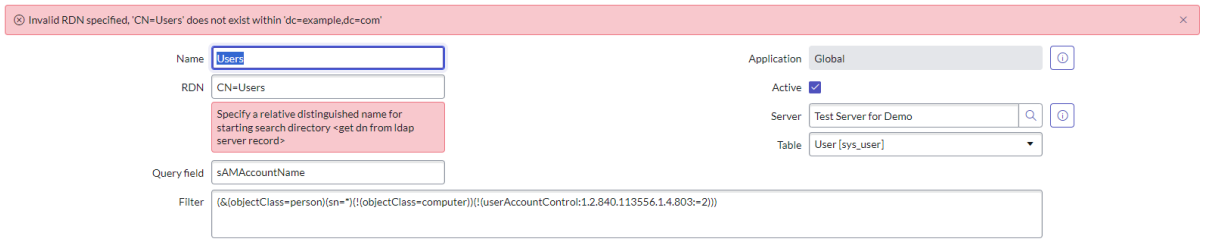
- If we can see the above image, these are the list of users present in this particular organizational unit (FORUM SYSTEMS).
- Here in our FORUM SYSTEMS, we have 2 OUs. One OU is for mathematicians and one is for scientists.
- Now let's check whether we are able to see all of these Users (mathematicians and scientists)



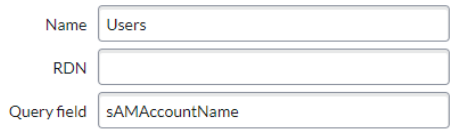
- Click on Users under LDAP OU Definitions,



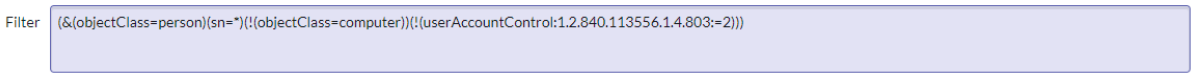
- Now, let's test the connection again in our LDAP OU definition Users record. We can see a prompt saying Invalid RDN specified. 'CN=Users' does not exist within 'dc=example,dc=com'



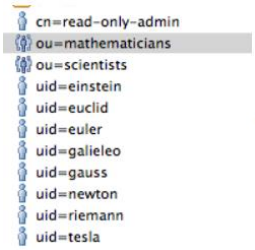
- Basically, it is saying that this CN=User, RDN doesn't exists. For now, let's make RDN column as blank.



- These are the configuration details, which we need to confirm with our AD Team.
- Because in LDAP, we have different directories. So, we have to confirm with our AD Team like what kind of distinguished name, we have to mention or what kind of RDN we have to mention.
- This is LDAP filter, it will decide what users you need to pick and put it into your ServiceNow.



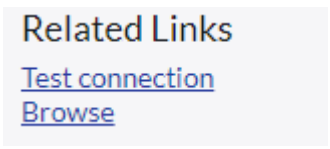
- In LDAP, you might find different kinds of user may be a user who is a just a computer account or user which is a real user. This is the reason why we need to use the filter.
- As we are using Public LDAP Server, it already mentioned the list of uid's and ou's list in Online LDAP Test Server website.



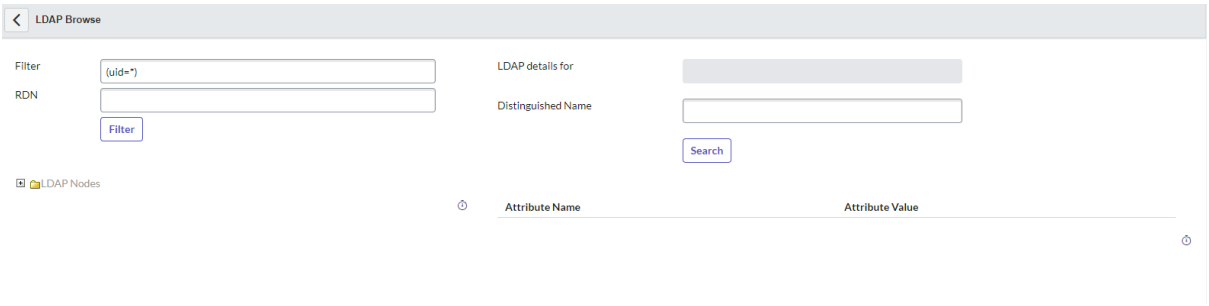
- For now, let's update uid in the filter column like (uid=*)

- Now if we can see, it says connected successful prompt on top.

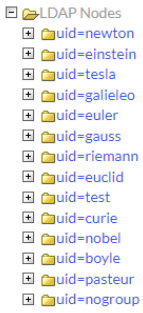
- That means, now our filter and RDN is working.
- Let click on browser under related links in LDAP OU Definition Users



- Let's go to Browse,



- This is really helpful during troubleshooting LDAP, now let's click on LDAP Nodes.



- We can see the list of uid's under LDAP Nodes. If can compare both of the uid's in FORUM SYSTEMS and LDAP Nodes in Services both are same.

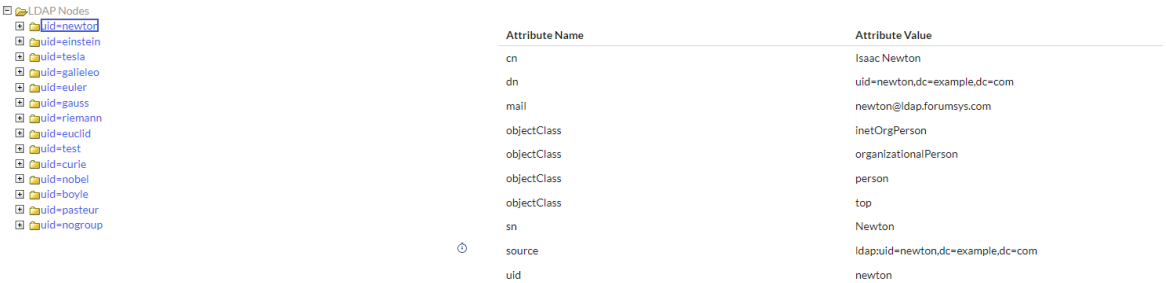
ou=mathematicians,dc=example,dc=com

- *riemann*
- *gauss*
- *euler*
- *euclid*

ou=scientists,dc=example,dc=com

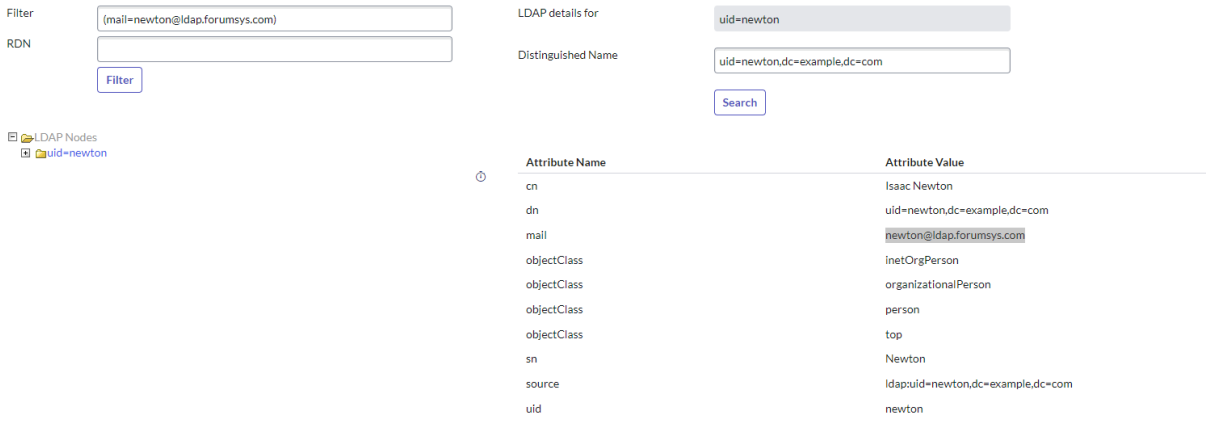
- *einstein*
- *newton*
- *galieleo*
- *tesla*

- Now, let's click on uid=newton under LDAP Nodes. We can see all the information regarding newton.

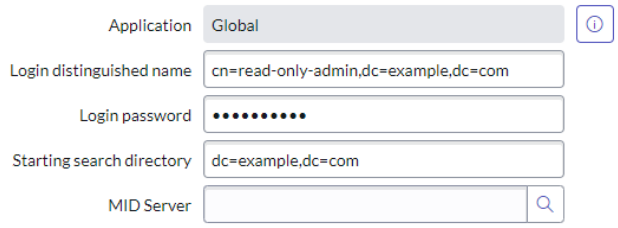


- Let's troubleshoot, copy the email id from the attribute value, which is newton@ldap.forumsys.com
- Let's compose a filter with the email id as (mail=newton@ldap.forumsys.com)

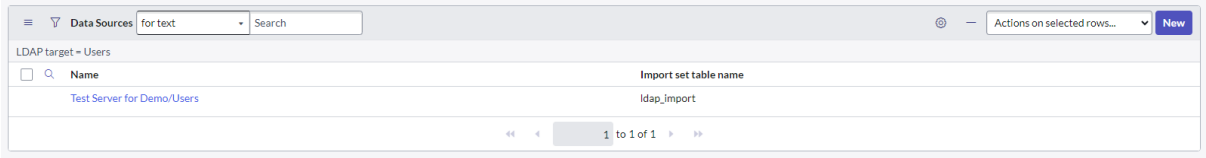
- Make sure the attribute name is same as mentioned in Attribute Naming convention.



- Now click Filter, and in the LDAP Nodes we can see uid=newton gets populated.
- This is because the filter that we mention is related to this user(uid=newton)
- We can troubleshoot our LDAP server like this using filters.
- Let's go to LDAP Server Test Server for Demo record
- In order to import our users using MID server. We need to select our MID Server.

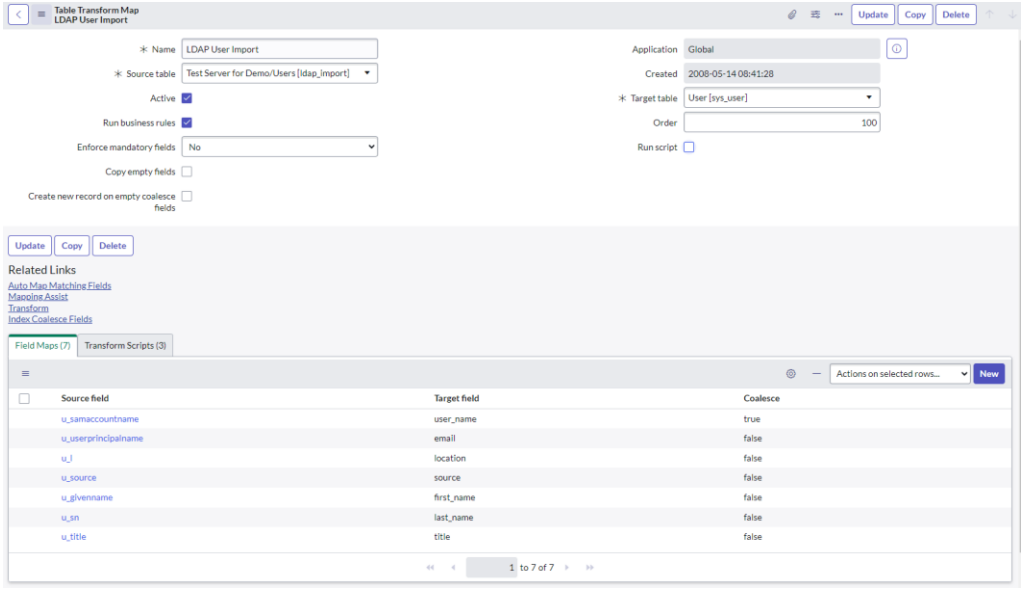


- We do not need to have a MID server to import users using LDAP. However, using a MID server can offer some advantages like Improved security, performance and simplified configuration.
- As of now, I don't have any MID server Installed on my Instance. So, I cannot select it.
- Now, let's go to our Test Server for Demo/Users record under Data Sources in LDAP OU Definition Users.



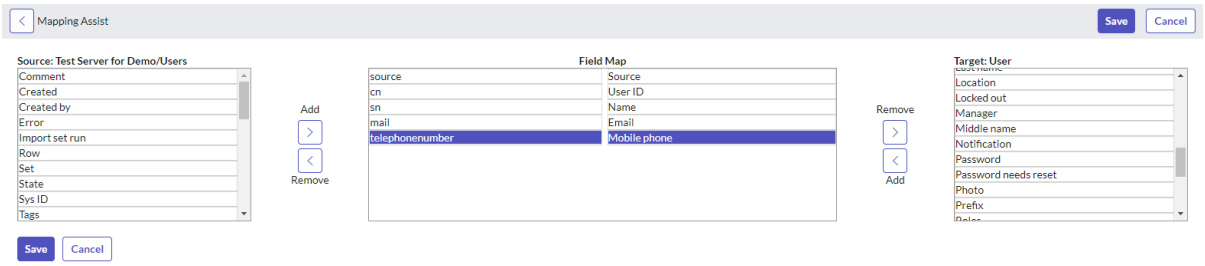
- We can also get this Data Source for Test Server for Demo/Users record from System LDAP module.

- Now click on Test Server for Demo/Users, we can see our Test Server for Demo/Users record here.
- Let's click Test Server for Demo record under Transforms table.
- Now we will be redirected to Table Transform Map LDAP User Import record.

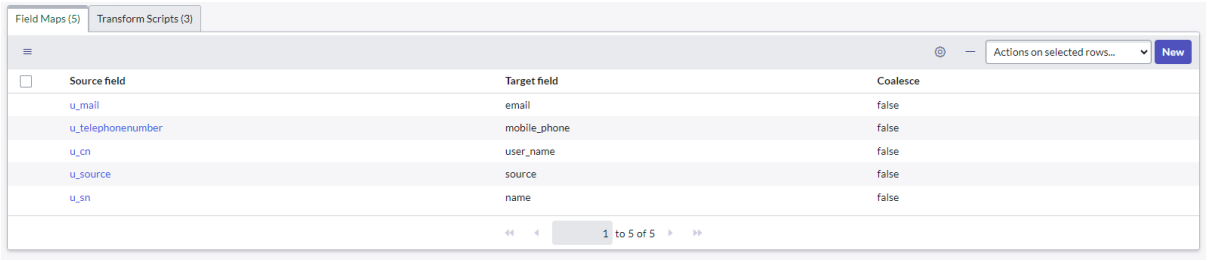


- Make sure Target table field is set to User [sys_user]
- As we can see, under the Field Maps. All the Source fields and Target fields are not mapped correctly in Field Map.
- Let's map them using Mapping Assist under Related Links.

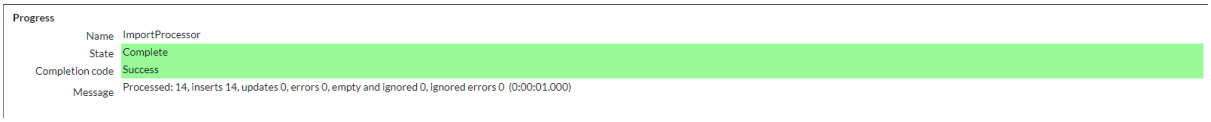
- Map the source field and target field data correctly and dump them in Field Map column.



- Now click on Save.
- Now, if we can see. All of our Source Field and Target Field under Field Maps got loaded correctly and successfully.



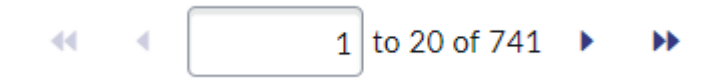
- Now let's click Transform under Related Links.
- Now we will be redirected to Specify Import Set and Transform map.
- Under Specify Import Set and Transform map, click Transform.
- Now we can see the records got successfully inserted in our sys_user table.



- Message is showing Processed:14, Inserts: 14, Updates: 0, errors 0, empty and ignored errors 0 (0:00:01.000)
- Now, Let go to our sys_user.list table and let's verify the count under sys_user table before and now.

BEFORE:

AFTER:



NEWLY LOADED USERS:

User ID	Name	First name	Email	Active
Albert Einstein	einstein	einstein	einstein@ldap.forumsys.com	true
Carl Friedrich Gauss	gauss	gauss	gauss@ldap.forumsys.com	true
Marie Curie	curie	curie	curie@ldap.forumsys.com	true
No Group	nogroup	nogroup	nogroup@ldap.forumsys.com	true
Bernhard Riemann	riemann	riemann	riemann@ldap.forumsys.com	true
Alfred Nobel	nobel	nobel	nobel@ldap.forumsys.com	true
Nikola Tesla	tesla	tesla	tesla@ldap.forumsys.com	true
Robert Boyle	boyle	boyle	boyle@ldap.forumsys.com	true
Galileo Galilei	galieleo	galieleo	galieleo@ldap.forumsys.com	true
Euclid	euclid	euclid	euclid@ldap.forumsys.com	true
Isaac Newton	newton	newton	newton@ldap.forumsys.com	true
Leonhard Euler	euler	euler	euler@ldap.forumsys.com	true
Test	test	test		true
Louis Pasteur	pasteur	pasteur	pasteur@ldap.forumsys.com	true