So you want to do some logging. . . (PT. 3 Adding Central Authentication)

blog.iso365down.com/so-you-want-to-do-some-logging-pt-3-adding-central-authentication-34831fd66a87

HanSolo71 December 6, 2023

You want to know who has been using the logging server

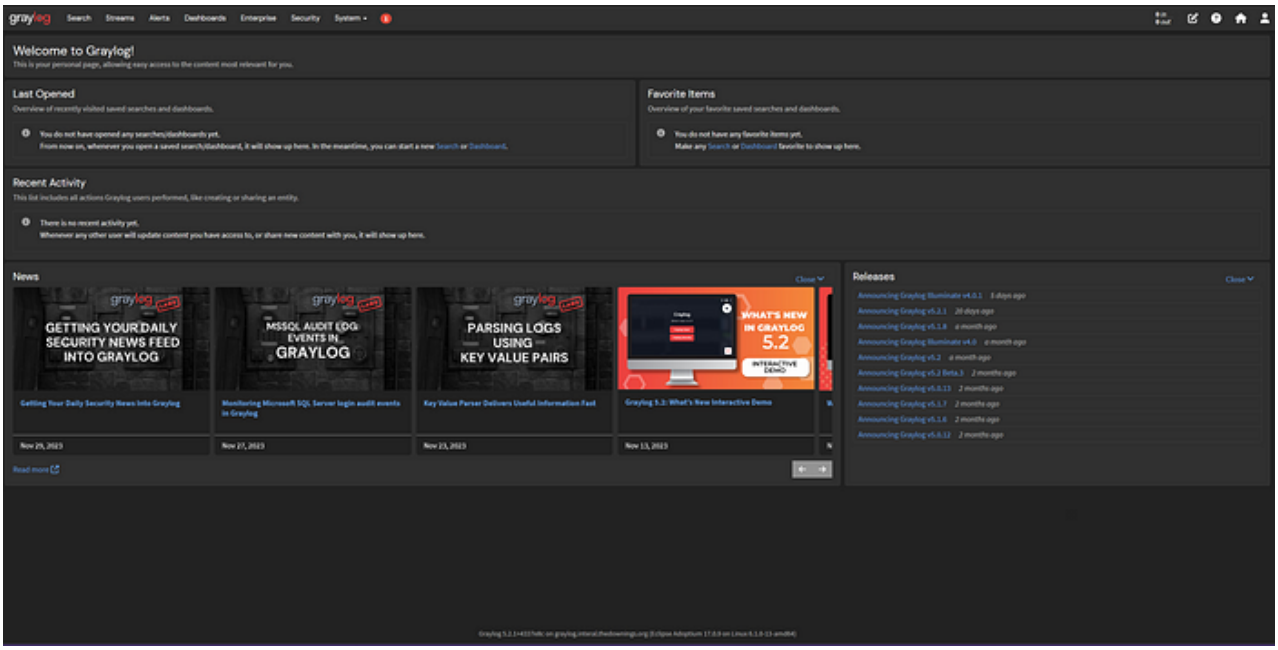
Adding Active Directory Authentication

Now that we have a Graylog server running and the web interface and API protected by a HTTPS its time to start configuring Graylog. The first thing we will be configuring is adding central authentication for our users in the form of Active Directory.

Login to the web interface of your Graylog server at https://servername.domain.com. The username is admin and the password is the password we created in Part 1 with this command.

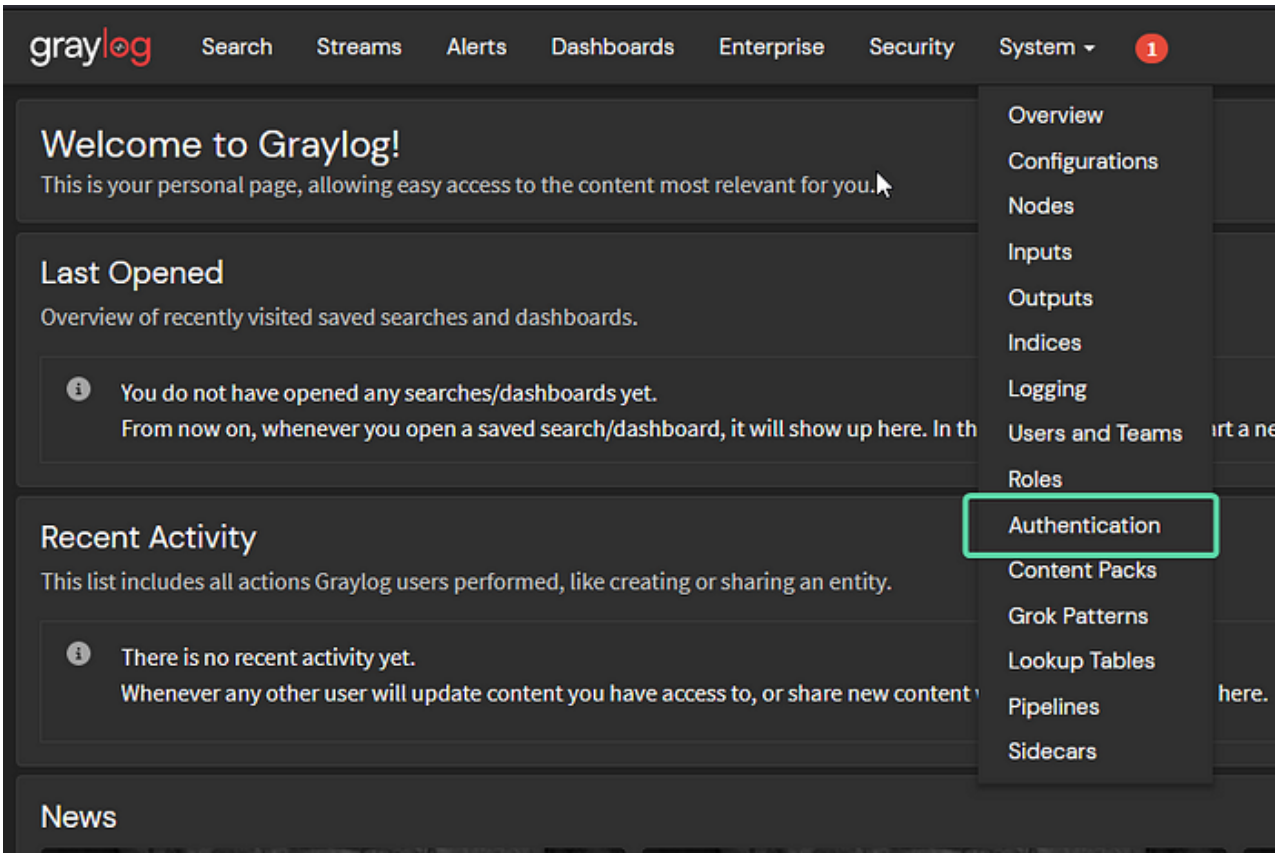
```
-n  &&  -1 </dev/stdin |  -d  |  |  -d -f1
```

If everything is working you should be presented with a page similar to this.



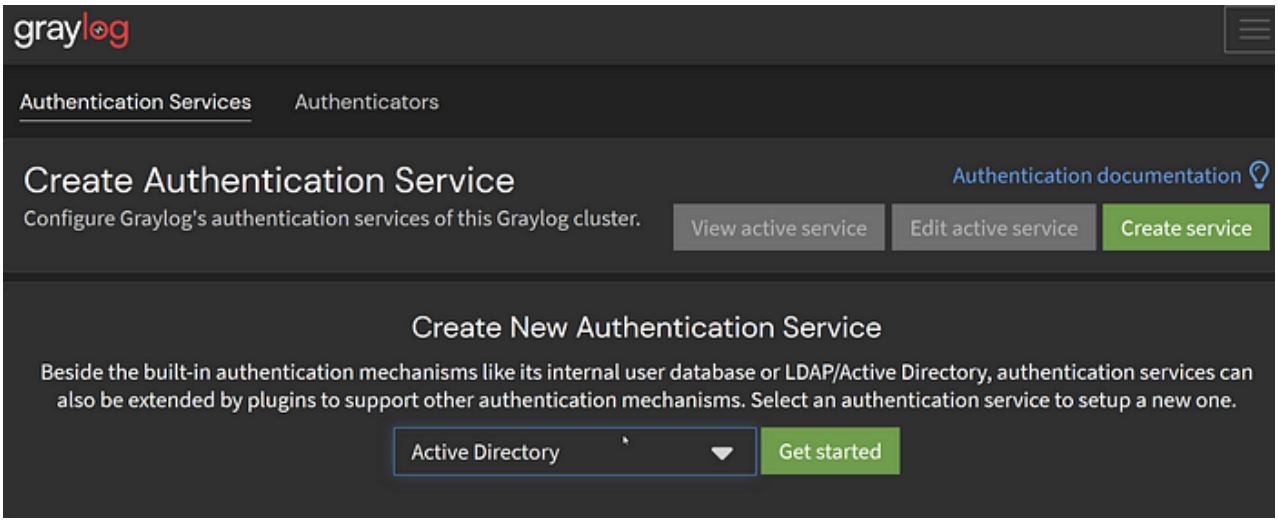
Graylog in all its default glory

Using the top menu lets browse to System > Authentication.

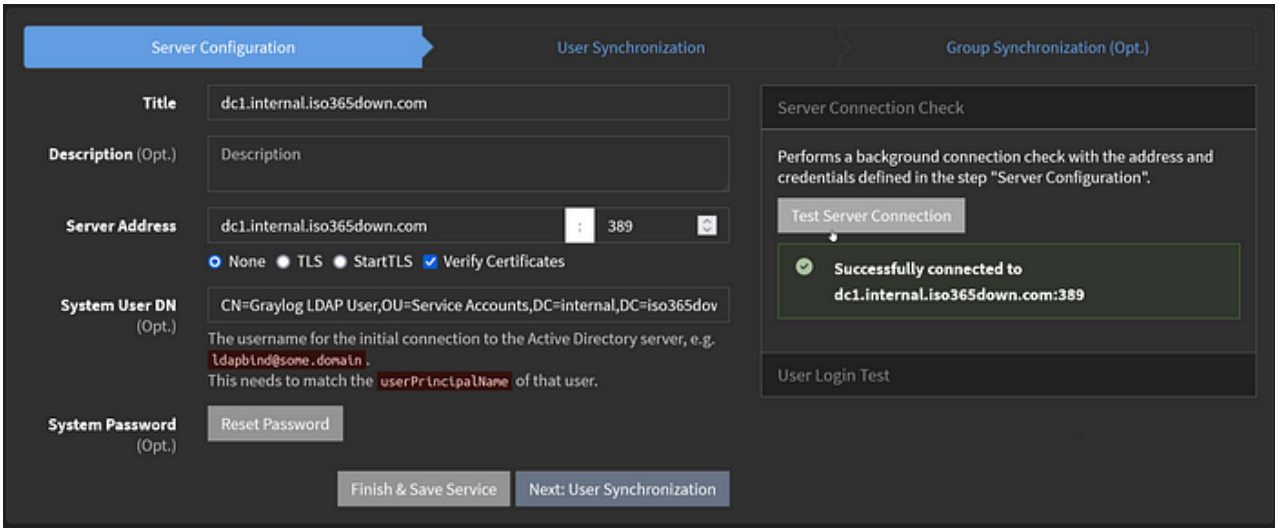


System > Authentication

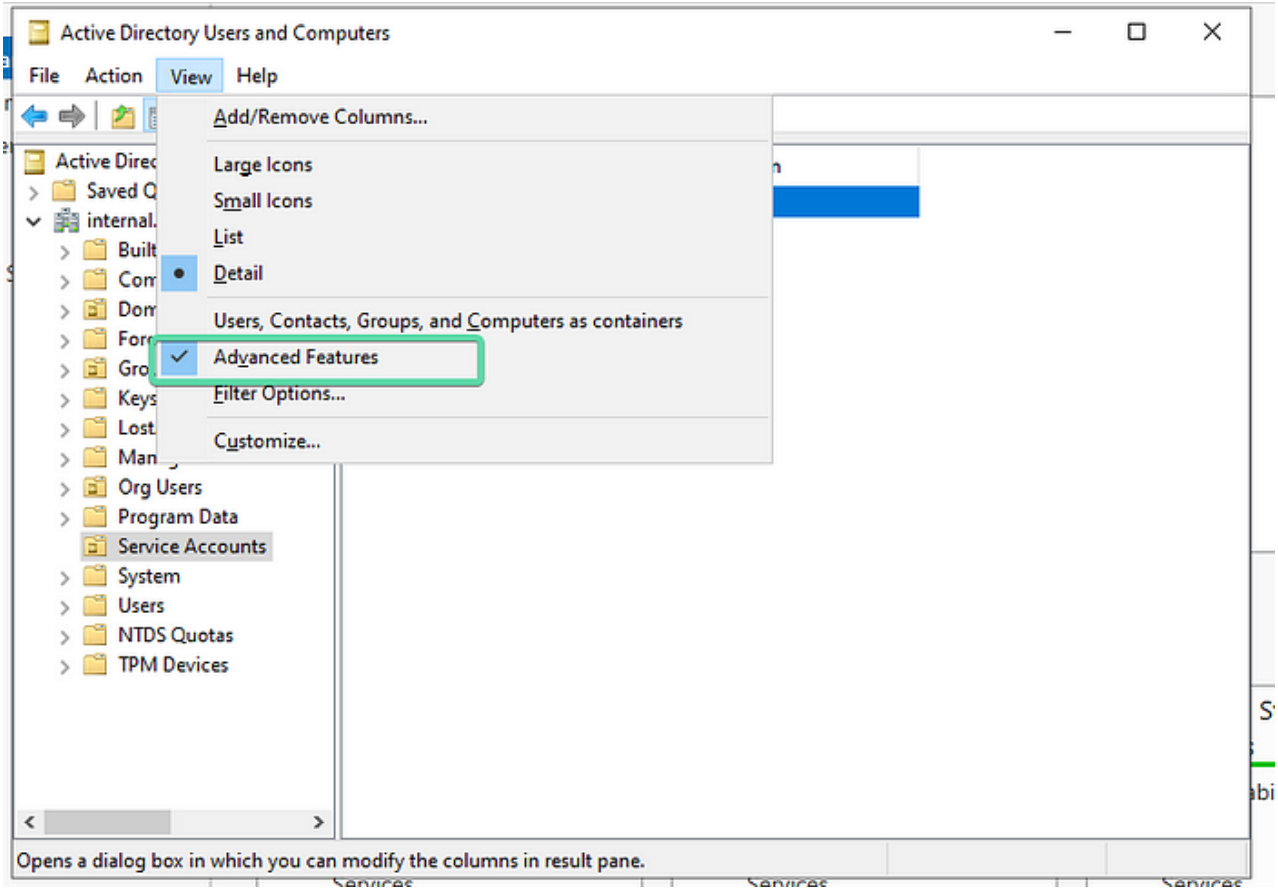
For this demo we will be configuring our central authentication to use active directory.



For this demo we will not be setting up LDAPS. In production do no pass credentials over a unencrypted connection.

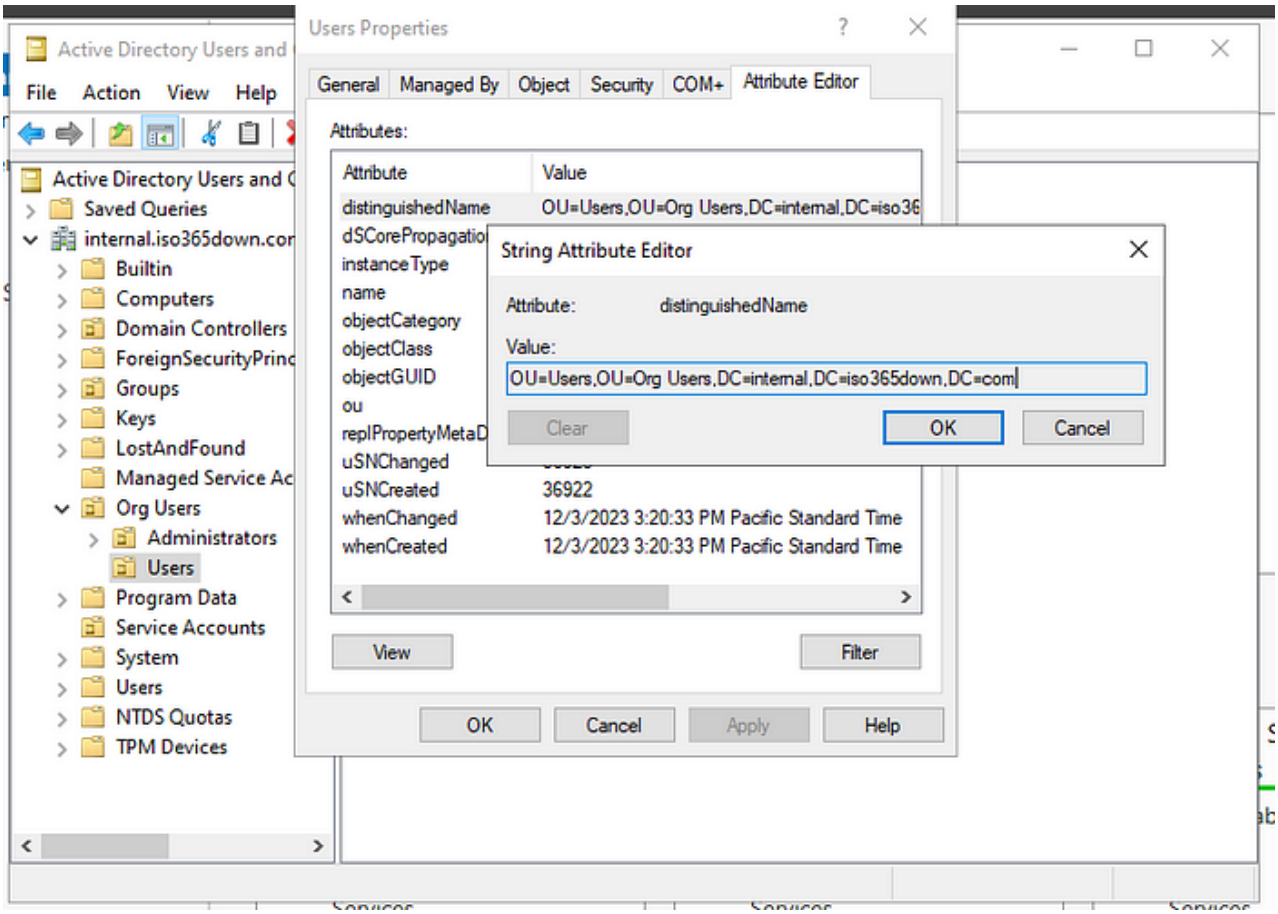


After we have made a connection to our domain controller we will want to configure the “Search Base DN”. In active directory this can easily be found by opening “Active Directory Users and Computers > View > Advanced Features” and enabling “Advanced Features”.



Enabling Advance Features

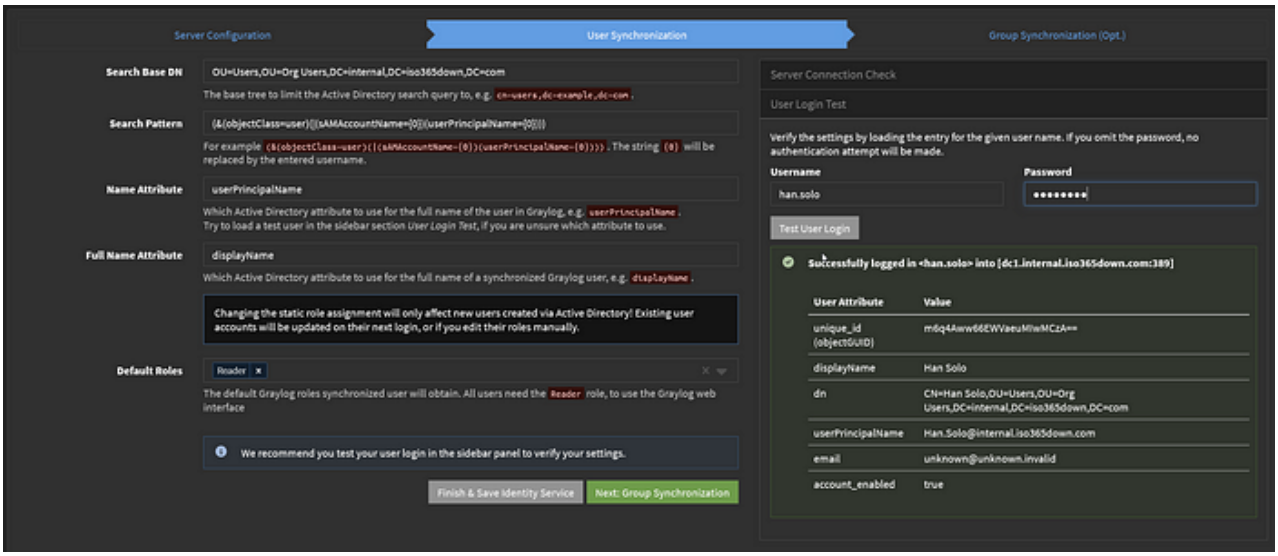
Then right click on the OU that contains your users and select “Properties”. Inside of the OU properties select “Attribute Editor”. Find the attribute *distinguishedName.* It should looke like the following string. I recommend leaving the default role as reader to ensure no user starts with excessive permissions.



Its easy to find the Base DN of OU in Active Directory

```
OU=Users,OU=Org Users,DC=internal,DC=iso365down,DC=com
```

Test with a user to validate we can authenticate.

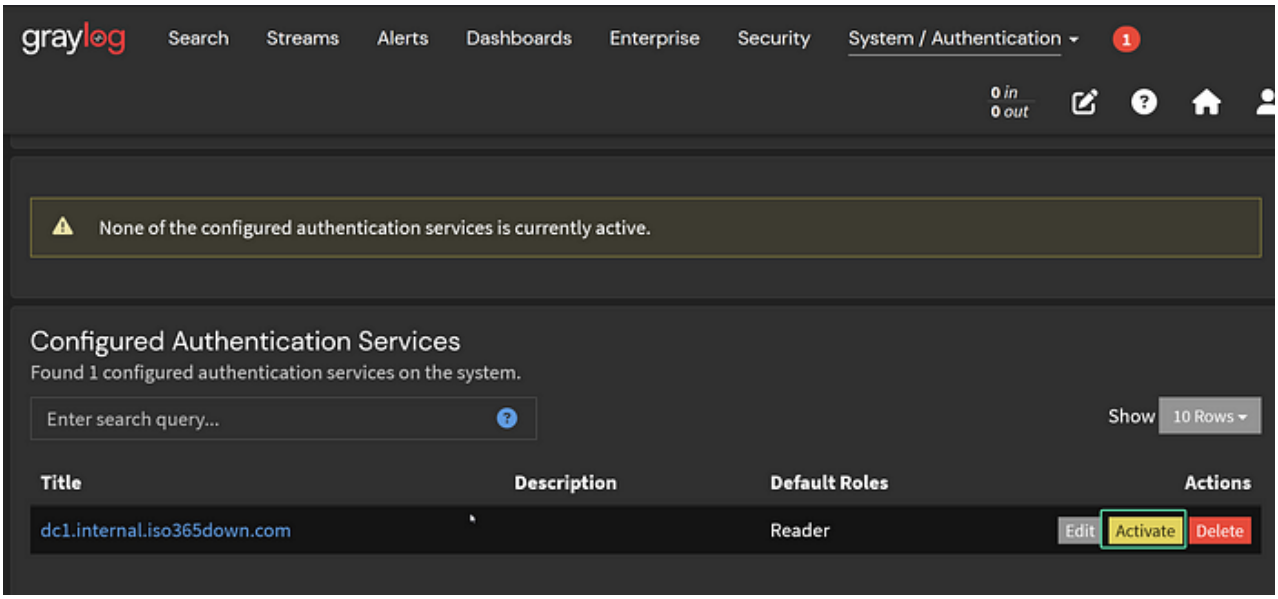


Make sure you test a few users

Because the non-enterprise version of Graylog can't sync groups (I have strong feelings about this and they aren't good feelings) I highly recommend limiting the Base Search DN to OU with a subset of users who you trust with access to Graylog.

This feature wasn't always locked behind enterprise

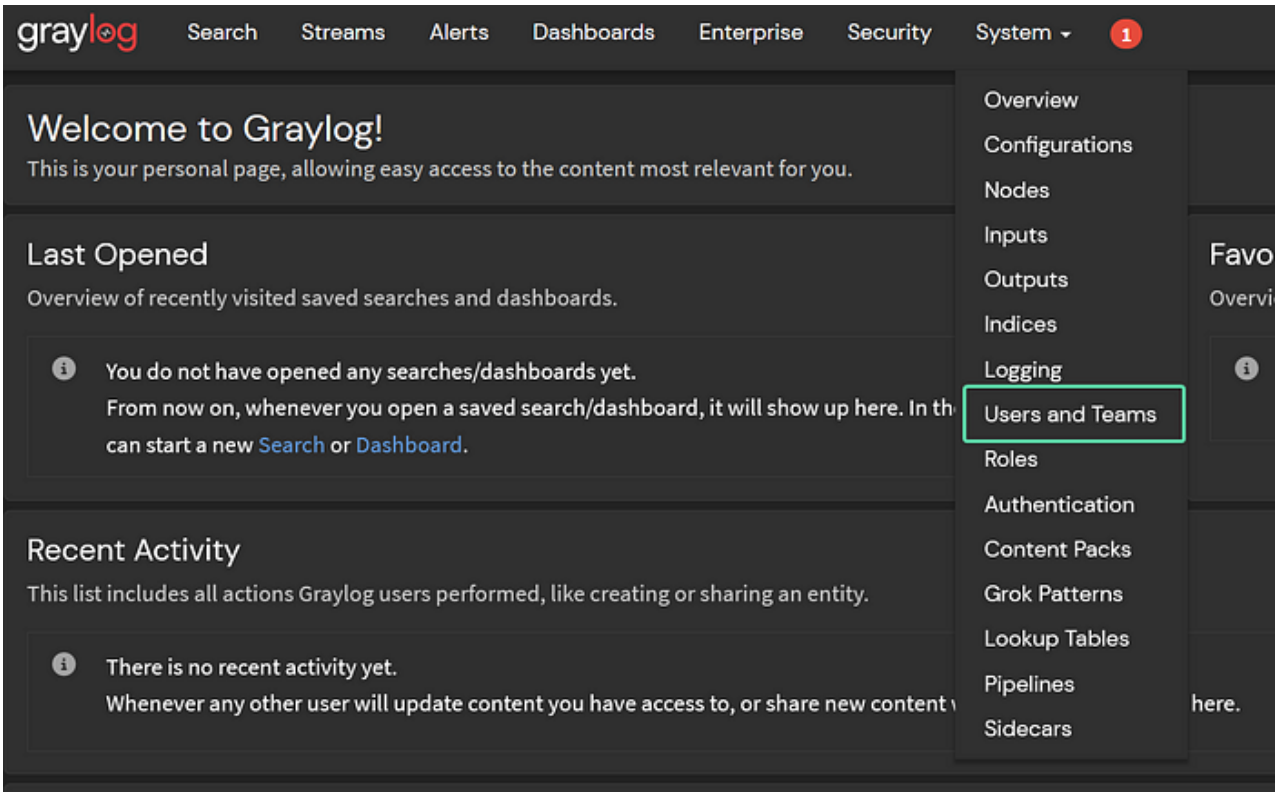
Go ahead and select "Finish and Save Service" and you should be back at the main "All Authentication Services" screen. Before going on we need to activate our new authentication server.



Make sure to active your new authentication server

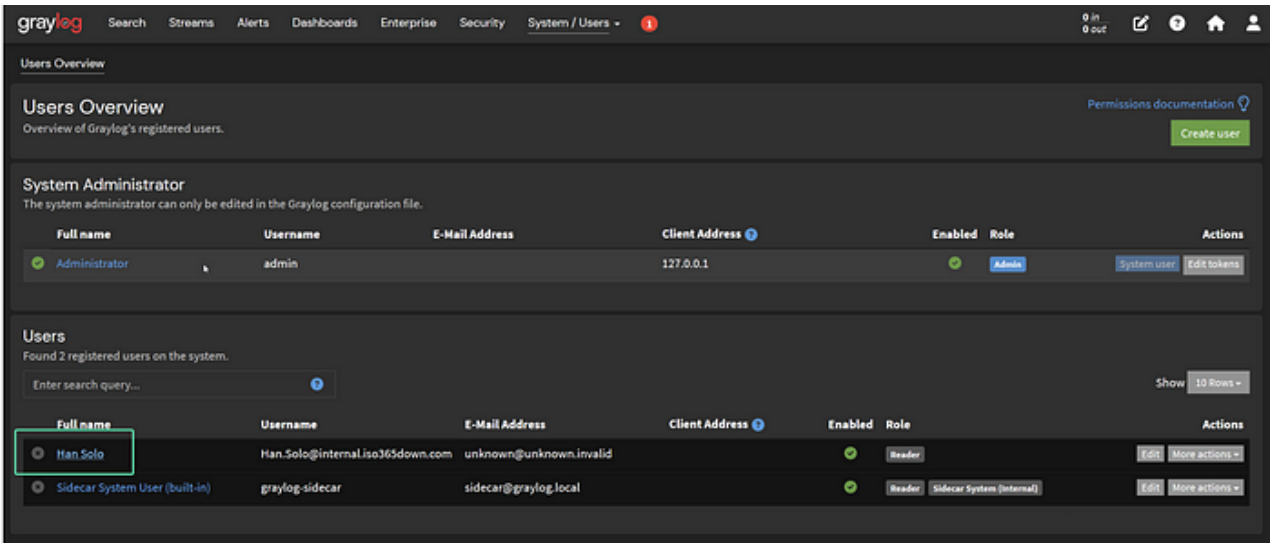
Once a user logs in, we will want to update their permissions to allow them to do work on the system. Each user by default only has *reader* access.

Once again using the top menu select "System > Users and Teams".



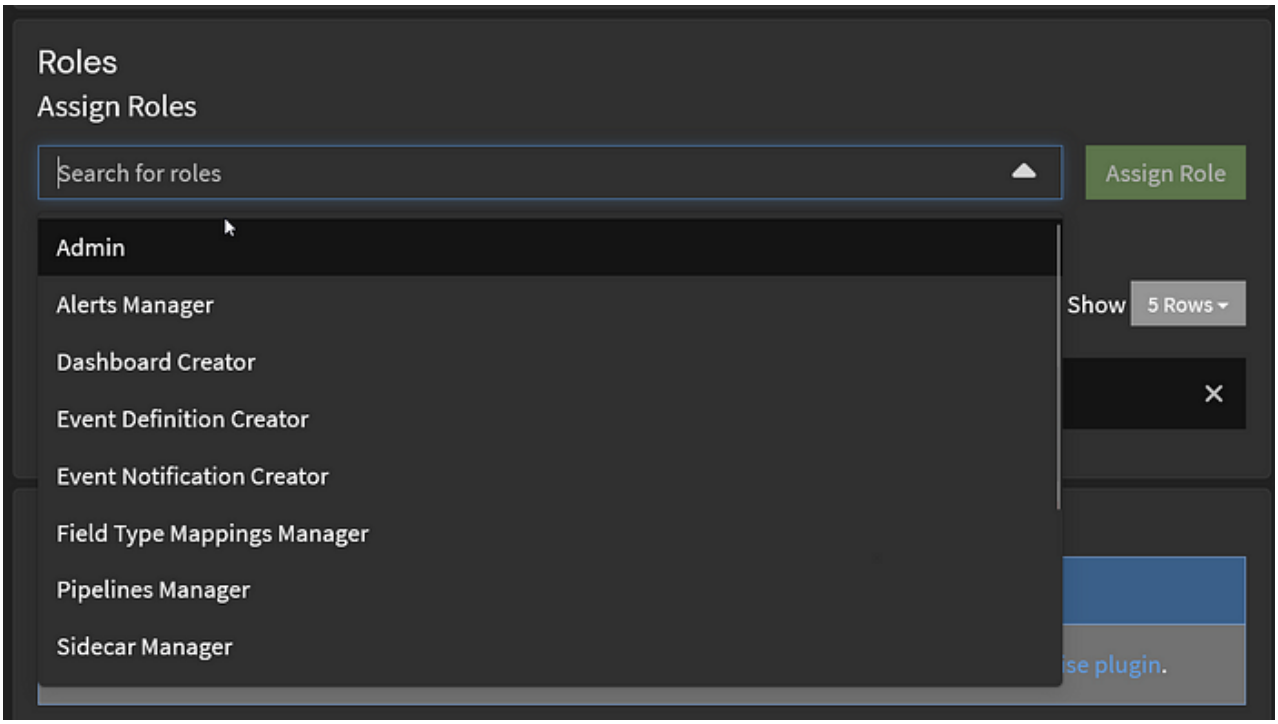
Now to find our user who just logged in

Select a user you would like to modify and edit that user.



Select the user you would like modify

Find the area named roles and assign the role you would like the user to have.



Assign the role needed.

With that we have enabled central authentication for Graylog.