

Assigning a User collection to an Administrative Security Role

Here are the basic steps we will complete in this lecture

1. From the Domain Controller, using ADUC we will create users, create a security group, add members to the group.
 2. Then using configuration manager we will create a user collection, and assign a security role to that collection.
- From our Domain Controller **SADC01**, open Server Manager, tools, Active Directory Users and Computers.
 - Double click the **ServerAcademy.com** domain. In case you have never created a user, I will show you how, then you'll go ahead and stop the video and **create two more users**.
 - Right click on Users, click new user
For first name type Mike
Tab down to last name and type Sims
Tab down to user logon name and type msims, then click next
Then type a password twice.
 - For this lab we will uncheck user must change password at next logon and check password never expires, click next, then finish.
 - Now go ahead and stop the video and create the other two users.
 - Now that you have created three users, right click on **users** then New, then click **Group**
For **Group Name** type **SCCM Admin Users**, click ok. **(Cancel)**
 - Double click the SCCM Admin Users group, then click members. Then click add, type Mike, then click check names, then click Ok.
 - Now add the other two users that you just created to the SCCM Admin users group.
These three users will be my administrator's, and will also be members of a User collection assigned to the Full Administrator security roll.
 - **Stop the video while you do this. Then click ok**

Now let's Create a User Collection

- From the SCCM server, open Configuration Manager, from the Workspace click Assets and Compliance, from the Navigation Pane right click **User Collections**, click **Create User Collection**.
- For Name type **SCCM Admin Users**, then click **Browse**, and select **All User Groups**, click ok. **Then click next**
- Click **Add Rule**, then select **Direct Rule**, then click next

- From Resource Class, select **User Group Resource**, for Attribute Name, Select **Active Directory Container Name**, For Value, type %, wildcard variable (this will display all the groups) then click **next**.
- Now, SCCM displays a list of all the groups from Active Directory. Scroll down and Click SERVERACADEMY\SCCM Admin Users, then click **next**, then click **next** again, then click **close**.
- Click next, then next again. Then click close

2. Now that we have created our collection, let's assign a security Role to the SCCM Admin Users Collection.

- From the Workspace, click Administration, from the Navigation Pane, click **Security**, then right click **Administrative Users**, click **add user or group**.
From User or group name, click **Browse**, type **SCCM Admin Users** then click **check names**, click **ok**.
- Click Add – Here is where we choose the Administrative Security Role, **Click Full Administrator**, click **ok**
Click Add, then click **collection**, click **SCCM Admin Users**, click ok, then click ok again
- **For verification**, click monitoring, click reporting, click the **Report Manager server/Reports**, Click Administrative Security, Security Roles Summary, scroll down, you will see the security Roll named Full Administrator and the SCCM Admin users group.

Verifying Security Roles

If you recall msims was one of the users that we created and added to the SCCM Admin users group, now we will check and see if msims has full admin rights to the console.

Now let's logout of SCCM and log back in as msims.

Go ahead and open the console. msims should have full administrator rights to the console. Go ahead and checkout the Administration workspace.

From Administration, servers and site system Roles, if I right click on the site, we see that msims can add site system roles which only an admin can configure.

Experimenting with Security Roles

- If you want to **experiment with security rolls**, try this.
From the workspace select Administration, from the Navigation Pane, click Security, then click on Administrative Users, then right click on SCCM Admin Users, click properties.

- Select security Rolls, Click add, check Read-only Analyst, click ok. Click Full Administrator, click remove, click apply, then click ok.
Log out and log back into configuration manager as msims, notice the difference in what Jobs can be performed.
- Read-only Analyst has very limited capability. all msims can accomplish is to view the console and send feedback to Microsoft.

Here is a quick review of what we accomplished in this lecture:

- First, we created three users in Active Directory, then we created a security group and added the three users to that group.
- Then from Configuration Manager we created a collection, then we assigned the “Full Administrator” security roll to the collection. Logged in as msims and demonstrated the result.
- Then we changed the security roll to Read-only Analyst using the same collection and demonstrated the results of that change.

Thanks for watching and we will see you in the next lecture.