How to retrieve the Active Directory memberOf attribute from an RSA Authentication Manager identity source

Article Content

Article Number 000033639

Applies To

RSA Product Set: SecurID
RSA Product/Service Type: Authentication Manager
RSA Version/Condition: 3.0, 7.1, 8.0, 8.1

Issue

This article provides information on how to get the memberOf attribute from Active Directory and pass the group name to a NAS using RADIUS with either a custom configured RADIUS attribute or a standard RADIUS attribute like Class (25) or Filter-ID (11).

See Notes for prerequisites and other limitations regarding this process.

Resolution

Setting Attributes

Setting the identity attribute that is used in both custom RADIUS attribute and standard RADIUS attribute configuration

1. Login to the Operations Console.
2. Select **Deployment Configuration** > **Identity Sources** > **Manage Existing**.
3. For the identity source from which you are capturing the memberOf data, click on the context arrow and choose **Edit**.
4. Click on the **Map** tab.
5. Under *Directory Settings*, uncheck the option to **Validate identity attribute definition mappings against directory schema**.
6. When done, click **Save**.
7. Login to the Security Console.
8. Select **Identity** > **Identity Attribute Definitions** > **Add New**.
9. To configure a new attribute, give it a name.
10. For Category, select **Attributes**.
11. For Datatype, select **String**.
12. Under *Identity Source Mapping*, enter the name of the identity source.
13. In the text box, key in **memberOf** as the attribute name.
14. Leave all other options on the page as the default.
15. Click **Save**.

Configuring a Custom RADIUS Attribute

1. Login to the Security Console.
2. Select **RADIUS** > **RADIUS User Attribute Definitions** > **Add New**.

3. Select the **Custom Attributes** tab.
4. Select **Add New Custom Attribute**.
5. Configure a number; for example, 100.
6. Enter the RADIUS attribute name defined above.
7. Map to an Identity Attribute by selecting **Yes**.
8. To enable this attribute on the user, go to **Identity** > **Users** > **Manage Existing**.
9. Search for a user with whom to test.
10. Click on the context arrow next to the user ID and choose **Authentication Settings**.
11. Configure the user to use the mapped class attribute.
    a. Scroll to the RADIUS section.
    b. Under RADIUS User Attributes, select the **25 - Class** attribute, enter the value and click the **Add** button.
    c. Click **Save** when done.
12. Now edit the RADIUS dictionary file named radius.dct.
    a. From the Operations Console, select **Deployment Configuration** > **RADIUS Servers**.
    b. Click on the **Dictionary Files** tab.
    c. Click on the drop down arrow next to the name of the primary RADIUS server and select **Manager RADIUS Server Files**.
    d. Scroll to the radius.dct file, and choose **Edit** from the context menu.
    e. Search for **ATTRIBUTE Class**. The line will look like the example below, with the lower case **r** indicating only one single class attribute can be configured per profile.

```
ATTRIBUTE  Class                          25    string             r
```

    a. Change the r value to **R**, as below. Switching to an upper case **R** means multiple class attributes can be configured in a single profile.

```
ATTRIBUTE  Class                          25    string             R
```

    a. Click **Save & Restart RADIUS Server** when done. RADIUS must be restarted for the new value in the radius.dct file to be read into the system.

1. Repeat steps 12a - 12g on every replica in your deployment.
2. In order to prevent multiple class attributes from being sent, edit the vendor.ini file to add the **send-class-attribute = no** value..
    a. Login to the Operations Console as the Operations Console administrator.
    b. Select **Deployment Configuration** > **RADIUS Servers**.
    c. When prompted, enter your super admin credentials.
    d. Click on the drop down arrow next to the name of your primary Authentication Manager server and select **Manage Server Files**.
    e. Click on the drop down arrow next to the vendor.ini and choose **Edit**.
    f. Scroll to the bottom of the file and add the following text, shown here in bold font:

```
help-id              = 2000
vendor-product       = - Standard Radius -
dictionary           = Radius
ignore-ports         = no
help-id              = 2000
send-class-attribute = no
```

    a. When done, click **Save & Restart RADIUS Server**.
    b. Repeat steps 14a - 14g on each of the replicas in the deployment.

1. Finally test with NTRadPing.
    a. If you have not used NTRadPing, download it and extract the .dct and exe files to a computer.
    b. Create a RADIUS client and associated agent for the machine on which NTRadPing is installed.
    c. Enter the **FQDN or IP address** of the RADIUS server in the RADIUS Server/port text box.

   d. Make sure the correct **RADIUS port** is shown. Typically this is 1645 or 1812.
   e. Enter the **shared secret** defined when creating the RADIUS client.
   f. Enter the user name that was selected when editing the Authentication Settings. Ensure that the user is not in New PIN Mode with the token or fixed passcode that is being tested.
   g. Enter the **tokencode or passcode** shown on the token or the **fixed passcode** for the user.
   h. Do not choose CHAP.
   i. Press **Send**. You should see **Access-Accept** in the RADIUS Server reply box on the right.
   j. Under Attribute Dump will be the group information defined.

Configuring a Standard RADIUS Attribute to Pass Group Information

In this example, we will use class attribute 25.

Use the same attribute definition created above.

1. Login to the Security Console.
2. Select **RADIUS** > **RADIUS User Attribute Definitions** > **Add New**.
3. Select the **Standard Attributes** tab.
4. Click on the context arrow next to *Class* and choose **Edit**.
5. For *Map to an Identity Attribute*, select **Yes**.
6. From the combo box, select the identity attribute. Using the example from before, choose **Group**.
7. When done, click **Save**.
8. Now enable the attribute on the user.
9. Select **Identity** > **Users** > **Manage Existing**.
10. Search for a user with whom to test.
11. Click on the context arrow next to the user ID and choose **Authentication Settings**.
12. Configure the user to use the mapped class attribute.
    a. Scroll to the RADIUS section.
    b. Under RADIUS User Attributes, select the **25 - Class** attribute, enter the value and click the **Add** button.
    c. Click **Save** when done.

1. Now edit the RADIUS dictionary file named radius.dct.
   a. From the Operations Console, select **Deployment Configuration** > **RADIUS Servers**.
   b. Click on the **Dictionary Files** tab.
   c. Click on the drop down arrow next to the name of the primary RADIUS server and select **Manager RADIUS Server Files**.
   d. Scroll to the radius.dct file, and choose **Edit** from the context menu.
   e. Search for **ATTRIBUTE Class**. The line will look like the example below, with the lower case **r** indicating only one single class attribute can be configured per profile.

```
ATTRIBUTE  Class                         25    string             r
```

   a. Change the r value to **R**, as below. Switching to an upper case **R** means multiple class attributes can be configured in a single profile.

```
ATTRIBUTE  Class                         25    string             R
```

   a. Click **Save & Restart RADIUS Server** when done. RADIUS must be restarted for the new value in the radius.dct file to be read into the system.
   b. Repeat steps 13a - 13g on every replica in your deployment.

1. In order to prevent multiple class attributes from being sent, edit the vendor.ini file to add the send-class-attribute = no value..
   a. Login to the Operations Console as the Operations Console administrator.
   b. Select **Deployment Configuration** > **RADIUS Servers**.

c. When prompted, enter your super admin credentials.
d. Click on the drop down arrow next to the name of your primary Authentication Manager server and select **Manage Server Files**.
e. Click on the drop down arrow next to the vendor.ini and choose **Edit**.
f. Scroll to the bottom of the file and add the following text, shown here in bold font:

```
help-id              = 2000
vendor-product       = - Standard Radius -
dictionary           = Radius
ignore-ports         = no
help-id              = 2000
send-class-attribute = no
```

a. When done, click **Save & Restart RADIUS Server**.
b. Repeat steps a - g on each of the replicas in the deployment.

1. Finally test with NTRadPing.
   a. If you have not used NTRadPing, download it and extract the .dct and exe files to a computer.
   b. Create a RADIUS client and associated agent for the machine on which NTRadPing is installed.
   c. Enter the **FQDN or IP address** of the RADIUS server in the RADIUS Server/port text box.
   d. Make sure the correct **RADIUS port** is shown. Typically this is 1645 or 1812.
   e. Enter the **shared secret** defined when creating the RADIUS client.
   f. Enter the user name that was selected when editing the Authentication Settings. Ensure that the user is not in New PIN Mode with the token or fixed passcode that is being tested.
   g. Enter the **tokencode or passcode** shown on the token or the **fixed passcode** for the user.
   h. Do not choose CHAP.
   i. Press **Send**. You should see **Access-Accept** in the RADIUS Server reply box on the right.
   j. Under Attribute Dump will be the group information defined.

Notes

Prerequisites

- Identity sources must be correctly configured.

Limitations

- This solution does not work on a global catalog (GC) server. You must configure on administrative identity source if you are using GC server. See 000016865 - Cannot link the runtime identity source because no administrative identity sources reference this runtime source in RSA Authentication Manager for information on configuring both a GC and DC as external identity sources.
- There may be a limitation with this solution. If the user is a member of multiple groups, some RADIUS clients will only pick up the first group sent to it by Active Directory.

Patch Levels

The following patch levels are required:

- Authentication Manager 7.1 SP4 server,
- RSA SecurID Appliance 3.0.4 or later,
- Authentication Manager 8.0, or
- Authentication Manager 8.1.

Testing

Testing is done using NTRadPing, a free RADIUS test utility.