Dell™ One Identity Manager 7.1.3

LDAP Connector for IBM® RACF® Reference Guide

Legend

△ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

ⓘ **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

One Identity Manager LDAP Connector for IBM® RACF® Reference Guide
Updated - November 2017
Version - 7.1.3

Contents

1

Initializing and Configuring the LDAP Connector for IBM® RACF®

This document describes how to initialize and configure the RACF LDAP Connector into an existing One Identity Manager system. This enables a One Identity Manager system to access, read and update data stored in a RACF database on an IBM® mainframe.

Detailed information about this topic

Pre-requisites

- The IBM mainframe must have the IBM Tivoli Directory Server for z/OS installed and configured.
- An LDAP service account must be created in your RACF database with the appropriate permissions to administer users and groups on this platform. To be able to administer everything in the RACF database, the user will need the RACF 'special' privilege.

- If more than 4096 records need to be retrieved from the RACF database in any one search (e.g. if there are more than 4096 users defined on the system) then the Quest RACF TDS Exit must be installed and configured.
- If data set profile data is to be synchronized, then the Quest RACF TDS Exit must be installed and configured.

NOTE: Before attempting to connect to the Tivoli Directory Server with the One Identity Manager connector, it is recommended to first check that the LDAP server is running correctly. This can be tested with any LDAP browser for example the `LDP.exe` tool from Microsoft. For more information, see your LDAP browser documentation.

Platform Support

- The RACF LDAP connector has been verified for synchronization against the IBM® mainframe running z/OS 1.8 (and RACF® 1.8) or later.

Operating Constraints

- There is an eight character limit for user and group names on RACF.
- There is an eight character limit for passwords on RACF.
- If the Quest RACF TDS Exit has not been installed then there is a limit of 4096 records that can be read from the RACF system in any one search operation.
- If the Quest RACF TDS Exit has not been installed then the RACF dataset LDAP object will not be available to the connector.

Pre-installation Information

Read the information in this section before you install the RACF LDAP Connector.

Detailed information about this topic

- User and group identifier on page 6
- RACF system users on page 7

User and group identifier

The LDAP implementation for RACF uses the `racfid` attribute to store the user name in a user object and the group name in a group object. The object containing the attribute defines whether it is referring to a user or a group.

RACF system users

RACF creates three special or system users which can be listed with an LDAP call. They are called `iicerta`, `iimulti` and `iisitec`. These system users cannot (and must not) be altered by the connector through an LDAP call, so are filtered out by the connector, i.e. when returning a list of all users in the RACF database, these three users will not be listed.

How to initialize and configure the RACF LDAP connector

NOTE: The following sequence describes how you configure a synchronization project if the Synchronization Editor is in expert mode.

To set up initial synchronization project for RACF

1. Start the Synchronization Editor and log in.
2. From the start page, select **Start a new synchronization project**.

   This starts the Synchronization Editor's project wizard.
3. Select **RACF LDAP Connector** on the **Choose target system** page.
4. On the **System access** page, click **Next**.
5. On the **Create system connection** page, select **Create new system connection**.
6. On the system connection wizard start page, click **Next**.
7. On the **Network** page:
   a. In the **Server** field, enter the DNS name or IP address of your mainframe server.
   b. In the **Port** field, enter the port number.
   c. Click on the **Test** button to make sure the server is accessible.
   d. The Tivoli Directory Server for z/OS supports LDAP v3. Enter the number 3 in the **Protocol version**.
   e. If SSL is to be used, check the **Use SSL** box.
8. On the **Authentication** page:
   a. Set the **Authentication method** to "Basic".
   b. In the **Credentials** section, enter the full DN and password of the administrator account on your RACF system.
   c. Click **Test** to check that the credentials are valid.
9. The schema will be loaded from the RACF system.
10. On the **Search options** page:
    a. In the “Base DN for searches” drop-down list, select the correct base DN for your system.
    b. Uncheck the “Use paged search” check box.

a. In the **Base DN** drop-down list, select the correct base DN for your system.

b. Uncheck the **Use paged search** check box.

11. On the **System attributes** page, in the **Revision properties** section, deselect the "createTimestamp" and "modifyTimestamp" entries by double clicking on them.

26. Click **Finish**.

    This takes you back to the Synchronization Editor's project wizard.

27. Enter the database connection data on the **One Identity Manager connection** page.

28. This will load the RACF schema into your One Identity Manager. Wait for this to complete.

29. On the **Select project template** page, select **Create blank project**.

30. On the **General** page, enter a display name for your synchronization project and set a scripting language if required.

31. Click **Finish** to complete the project wizard.

32. Select **Activate project** to activate the project.

Related Topics

- Domain Filter Setting on page 9
- User Mapping Information on page 10
- Group Mapping Information on page 14
- Data Set Profile Mapping Information on page 19

System Variables

The following system variables need to be defined for the attribute mappings. For more detailed information about variables, see the Dell One Identity Manager Target System Synchronization Reference Guide.

Table 1: System variables

Name	Value
IdentDomain	The name of your RACF domain e.g. `RACF_DOMAIN`
UserLocation	Parent DN of your RACF user container, e.g. `profiletype=user,cn=mainframe1,o=mycompany,c=com`
GroupLocation	Parent DN of your RAF group container, e.g. `profiletype=group,cn=mainframe1,o=mycompany,c=com`
DatasetLocation	Parent DN of your RACF dataset container, e.g. `profiletype=dataset,cn=mainframe1,o=mycompany,c=com`

Related Topics

- Domain Filter Setting on page 9
- Property Mapping Rules on page 10

- Property Mapping Rules on page 15
- Property Mapping Rules on page 20

Domain Filter Setting

A domain filter needs to be created to identify information that has been retrieved from the RACF database to keep it separate from other imported data.

1. Update the One Identity Manager schema so that all entries are included.
    a. In the Synchronization Editor, open your RACF project.
    b. Select the category **Configuration | One Identity Manager connection**.
    c. Then in the "General" section on the right-hand side, click **Update schema**.
    d. Click on **Yes** in the next two dialog boxes.
    e. Click **Ok** when completed.
2. In the Manager
    a. Select the category **LDAP | Domains**.
    b. In the result list toolbar, click  .
    c. Enter at least the following general master data on the **General** tab.

    Table 2: Domain Master Data

Property	Description
Display name	Display name e.g. `RACF Domain`
Distinguished name	Distinguished name of the domain e.g. `cn=mainframe1,o=mycompany,c=com`
Domain	Domain name e.g. `RACF_DOMAIN`
Structural object class	Structural object class representing the object type, enter `DCOBJECT`

    d. Save the changes.
3. In the Synchronization Editor, open your RACF project.
    a. Select the category **Configuration | One Identity Manager connection**.
    b. Select the **Scope view** and click **Edit scope**.
    c. Select the object type `LDPDomain` in the **Scope hierarchy** list and set the **Object filter** to: `Ident_Domain ='$IdentDomain$'`.
    d. Save the changes.

For more detailed information about scopes, see the Dell One Identity Manager Target System Synchronization Reference Guide.

Related Topics

- System Variables on page 8

User Mapping Information

This section shows a possible mapping between a user account in RACF and the standard One Identity Manager database table called `LDAPAccount`.

- Set up a new mapping from `LDAPAccount(all)` to `racfUser(all)`.

For more detailed information about setting up mappings, see the Dell One Identity Manager Target System Synchronization Reference Guide.

Detailed information about this topic

- Mandatory RACF User Attributes on page 10
- Property Mapping Rules on page 10
- Object Matching Rules on page 13
- Sample User Mapping on page 14

Mandatory RACF User Attributes

When creating a user in the RACF database, the following LDAP attributes must be defined:

- objectclass
- racfid

Related Topics

- Property Mapping Rules on page 10
- Object Matching Rules on page 13

Property Mapping Rules

- CanonicalName ← vrtEntryCanonicalName

  `vrtEntryCanonicalName` is a virtual property, set to the canonical name of the object in the connector.

  Sample value:

  `COM/MYCOMPANY/MAINFRAME1/USER/USER1234`

- cn ←→ racfid

  On the RACF system, `racfid` is the user ID.

  Sample value:

  `USER1234`

- DistinguishedName ← vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector. Activate the check box **Force mapping against direction of synchronization**.

  Sample value:

racfid=USER1234,profiletype=user,cn=mainframe1,o=mycompany,c=com

- ObjectClass ←→ objectClass

  The objectClass attribute (multi-valued) on the RACF system. Activate the check box **Ignore case sensitivity**.

  Sample value:

  TOP;RACFBASECOMMON;RACFUSER

- StructuralObjectClass ← vrtStructuralObjectClass

  vrtStructuralObjectClass on the RACF system defines the single object class for the object type. Activate the check box **Ignore case sensitivity**.

  Sample value:

  RACFUSER

- UID_LDPDomain ← vrtIdentDomain

  Create a fixed value property variable on the RACF side called vrtIdentDomain that is set to the value $IdentDomain$. Map this to UID_LDPDomain. This will cause a conflict and the Property Mapping Rule Conflict Wizard opens automatically.

  To solve the conflict

  1. In the Property Mapping Rule Conflict Wizard, select the first option and click **OK**.
  2. On the **Select an element...** page, select **Ident_Domain** and click **OK**.
  3. Confirm the security prompt with **OK**.
  4. On the **Edit property...** page,
     a. Deactivate **Save unresolvable keys**.
     b. Activate **Handle failure to resolve as error**.
     c. To close the Property Mapping Rule Conflict Wizard, click **OK**.
  5. Activate the check box **Force mapping against direction of synchronization**.

  Sample value:

  RACF_DOMAIN

- vrtParentDN → vrtEntryParentDN

  Create a fixed value property variable on the One Identity Manager side called vrtParentDN equal to a fixed string with value $UserLocation$. Map this to vrtEntryParentDN on the RACF side.

  Sample value:

  profiletype=user,cn=mainframe1,o=mycompany,c=com

- vrtRDN → vrtEntryRDN

  Create a new variable on the One Identity Manager side of type "Script Property" with name vrtRDN and a data type of “string”. In the Scripts section, enter one of the he following scripts in the Read script section, depending on whether your project is configured for C# or Visual Basic.

  C# Script

  ```
  references VI.TSUtils.dll;
  ```

```
return (VI.TargetSystem.Base.Utils.LDAP.RDN.Create("cn", useOldValues ? $cn[o]$
: $cn$).ToString()).Replace("cn=","racfid=");
```

VB Script

```
References VI.TSUtils.dll

Imports VI.TargetSystem.Base.Utils.LDAP

Dim name as String = ""

If useOldValues Then

     name = $cn[o]$

Else

     name = $cn$

End If

return RDN.Create("cn",name).ToString().Replace("cn=","racfid=")
```

Then map this to `vrtEntryRDN` on the RACF side.

Sample value:

```
racfid=USER1234
```

- userPassword → racfPassword

  Used to change a user's RACF password. A condition needs to be set on this rule to map the password only when there is a value to be copied.

  ### *To add a condition*

  1. Create the mapping.
  2. Edit the property mapping rule.
  3. Expand the **Condition for execution** section at the bottom of the dialog.
  4. Click on **Add condition** and set the following condition (a blank password is indicated by using two apostrophe characters).

     ```
     Left.UserPassword<>''
     ```

- UID_LDAPContainer ← vrLDAPContainerDN

  This is a workaround needed to support group mappings. Create a new fixed value variable on the RACF side of type "String" with no value called `vrtLDAPContainerDN` with the value set to `$UserLocation$`. This generates a property mapping rule conflict.

  ### *To solve the conflict*

  1. In the Property Mapping Rule Conflict Wizard, select the first option and click **OK**.
  2. On the **Select an element...** page, select **DistinguishedName** and click **OK**.
  3. Confirm the security prompt with **OK**.
  4. On the **Edit property...** page,
     a. Deactivate **Save unresolvable keys**.
     b. Activate **Handle failure to resolve as error**.

c. Active **Ignore case**.

d. To close the Property Mapping Rule Conflict Wizard, click **OK**.

Related Topics

- Mandatory RACF User Attributes on page 10
- System Variables on page 8
- Object Matching Rules on page 13
- Sample User Mapping on page 14

Object Matching Rules

- DistinguishedName (primary rule) vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector. This forms a unique ID to distinguish individual user objects on the RACF system.

  To convert this mapping into an object matching rule

  1. Select the property mapping rule in the rule window.
  2. Click  in the rule view toolbar.

     A message appears.
  3. Click **Yes** to convert the property mapping rule into an object matching rule and save a copy of the property mapping rule.
  4. Edit the object mapping rule and ensure that the **Case sensitive** check box is not activated.

  Sample value:

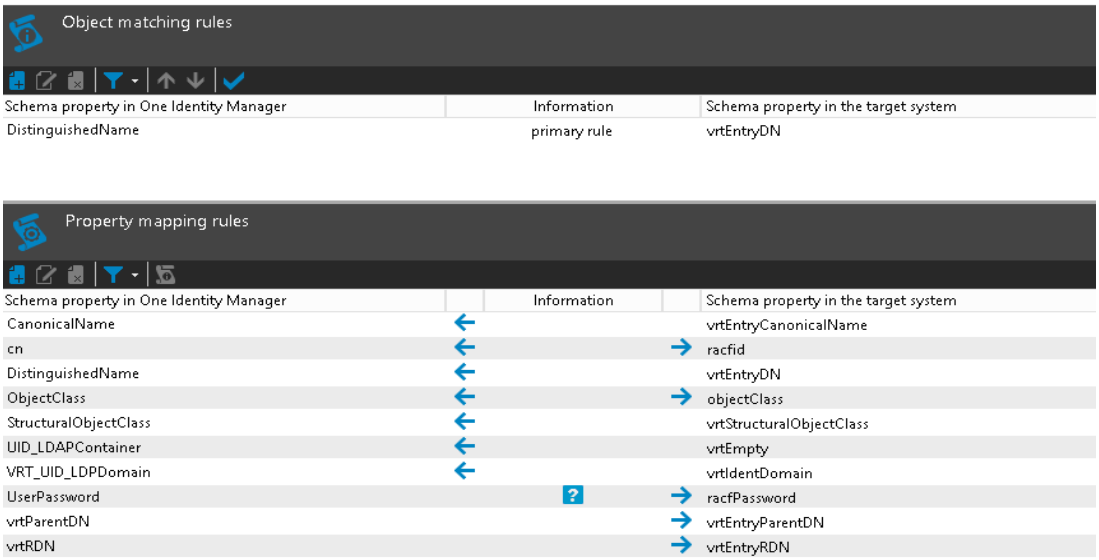
  `racfid=USER1234,profiletype=user,cn=mainframe1,o=mycompany,c=com`

Related Topics

- Mandatory RACF User Attributes on page 10
- Property Mapping Rules on page 10
- Sample User Mapping on page 14

Sample User Mapping

The following figure shows the above user mapping in operation.



Group Mapping Information

This section shows a possible mapping between a user account in RACF and the standard One Identity Manager database table called `LDAPGroup`. The data set profile mapping used later also maps to `LDAPGroup` so a filter needs to be applied in order to tell these apart.

- When creating the group mapping, add a new schema class as follows.

  Table 3: Schema class settings

Property	Value
Schema type	LDAPGroup
Display name	LDAPGroup (RACF Group)
Class name	LDAPGroup_racfgroup
Select objects: Condition	StructuralObjectClass='racfgroup'
Select objects: Ignore case	Activated

- Select this new schema class, `LDAPGroup (RACF Group)` for this mapping to `racfGroup(all)` on the RACF side.

For more detailed information about setting up mappings, see the Dell One Identity Manager Target System Synchronization Reference Guide.

Detailed information about this topic

- Mandatory RACF Group Attributes on page 15
- Property Mapping Rules on page 15
- Object Matching Rules on page 18
- Data Set Profile Mapping Information on page 19
- Sample Group Mapping on page 18

Mandatory RACF Group Attributes

When creating a group in the RACF database, the following LDAP attributes must be defined:

- objectclass
- racfid

Related Topics

- Property Mapping Rules on page 15
- Object Matching Rules on page 18

Property Mapping Rules

- CanonicalName ← vrtEntryCanonicalName

  `vrtEntryCanonicalName` is a virtual property, set to the canonical name of the object in the connector.

  Sample value:

  `COM/MYCOMPANY/MAINFRAME1/GROUP/USERGRP`

- cn ←→ racfid

  On the RACF system, `racfid` is the group ID.

  Sample value:

  `USERGRP`

- DistinguishedName ← vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector. Activate the check box **Force mapping against direction of synchronization**.

  Sample value:

  `racfid=USERGRP,profiletype=group,cn=mainframe1,o=mycompany,c=com`

- ObjectClass ←→ objectClass

  The `objectClass` attribute (multi-valued) on the RACF system. Activate the check box **Ignore case sensitivity**.

  Sample value:

  `TOP;RACFBASECOMMON;RACFGROUP`

- StructuralObjectClass ← vrtStructuralObjectClass

  `vrtStructuralObjectClass` on the RACF system defines the single object class for the object type.

  Sample value:

  `RACFGROUP`

- UID_LDPDomain ← vrtIdentDomain

  Create a fixed value property variable on the RACF side called `vrtIdentDomain` that is set to the value `$IdentDomain$`. Map this to `UID_LDPDomain`. This will cause a conflict and the Property Mapping Rule Conflict Wizard opens automatically.

  To solve the conflict

  1. In the Property Mapping Rule Conflict Wizard, select the first option and click **OK**.
  2. On the **Select an element...** page, select **Ident_Domain** and click **OK**.
  3. Confirm the security prompt with **OK**.
  4. On the Edit property... page,
     a. Deactivate **Save unresolvable keys**.
     b. Activate **Handle failure to resolve as error**.
     c. To close the Property Mapping Rule Conflict Wizard, click **OK**.
  5. Activate the check box **Force mapping against direction of synchronization**.

  Sample value:

  `RACF_DOMAIN`

- vrtParentDN → vrtEntryParentDN

  Create a fixed value property variable on the One Identity Manager side called `vrtParentDN` equal to a fixed string with value `$GroupLocation$`. Map this to `vrtEntryParentDN` on the RACF side. Activate the check box **Ignore case sensitivity**.

  Sample value:

  `profiletype=group,cn=mainframe1,o=mycompany,c=com`

- vrtRDN → vrtEntryRDN

  Create a new variable on the One Identity Manager side of type "Script Property" with name `vrtRDN` and a data type of “string”. In the Scripts section, enter one of the he following scripts in the Read script section, depending on whether your project is configured for C# or Visual Basic.

  C# Script

  ```
  references VI.TSUtils.dll;

  return (VI.TargetSystem.Base.Utils.LDAP.RDN.Create("cn", useOldValues ? $cn[o]$
  : $cn$).ToString()).Replace("cn=","racfid=");
  ```

  VB Script

  ```
  References VI.TSUtils.dll

  Imports VI.TargetSystem.Base.Utils.LDAP

  Dim name as String = ""
  ```

```
If useOldValues Then
      name = $cn[o]$
Else
      name = $cn$
End If
return RDN.Create("cn",name).ToString().Replace("cn=","racfid=")
```

Then map this to `vrtEntryRDN` on the RACF side.

Sample value:

```
USERGRP
```

- UID_LDAPContainer ← vrLDAPContainerDN

  This is a workaround needed to support group mappings. Create a new fixed value variable on the RACF side of type "String" with no value called `vrtLDAPContainerDN` with the value set to `$GroupLocation$`. This generates a property mapping rule conflict.

  To solve the conflict

  1. In the Property Mapping Rule Conflict Wizard, select the first option and click **OK**.
  2. On the **Select an element...** page, select **DistinguishedName** and click **OK**.
  3. Confirm the security prompt with **OK**.
  4. On the **Edit property...** page,
     a. Deactivate **Save unresolvable keys**.
     b. Activate **Handle failure to resolve as error**.
     c. Active **Ignore case**.
     d. To close the Property Mapping Rule Conflict Wizard, click **OK**.

- vrtMember ←→ racfGroupUserids

  This mapping is used to synchronize group membership information.

  1. Create a new virtual entry on the One Identity Manager side of type "Members of M:N schema types" with name `vrtMember`. Activate the boxes to **Ignore case** and **Enable relative component handling**.
  2. Add the following M:N schema types:
     a. Add an entry for `LDAPAccountInLDAPGroup`. Set the left box to `UID_LDAPGroup` and the right box to `UID_LDAPAccount`. Set the **Primary Key Property** to `DistinguishedName`.
     b. Add an entry for `LDAPGroupInLDAPGroup`. Set the left box to `UID_LDAPGroupParent` and the right box to `UID_LDAPGroupChild`. Set the **Primary Key Property** to `DistinguishedName`.
  3. Create a new mapping rule of type "Multi-reference mapping rule". Set the rule name to "Member" and the mapping direction to "Both directions". Set the One Identity Manager schema property to `vrtMember` and the RACF schema property to `racfGroupUserids`.

Related Topics

- Mandatory RACF Group Attributes on page 15
- System Variables on page 8
- Object Matching Rules on page 18
- Sample Group Mapping on page 18

Object Matching Rules

- DistinguishedName (primary rule) vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector. This forms a unique ID to distinguish individual group objects on the RACF system.

  To convert this mapping into an object matching rule

  1. Select the property mapping rule in the rule window.
  2. Click  in the rule view toolbar.

     A message appears.
  3. Click **Yes** to convert the property mapping rule into an object matching rule and save a copy of the property mapping rule.
  4. Edit the object mapping rule and activate the **Case sensitive** check box.

  Sample value:

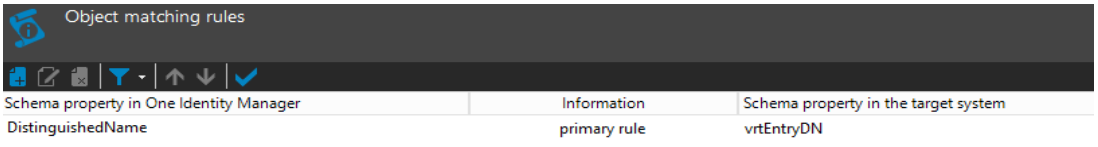
  `racfid=USERGRP,profiletype=group,cn=mainframe1,o=mycompany,c=com`

Related Topics

- Mandatory RACF Group Attributes on page 15
- Property Mapping Rules on page 15
- Sample Group Mapping on page 18

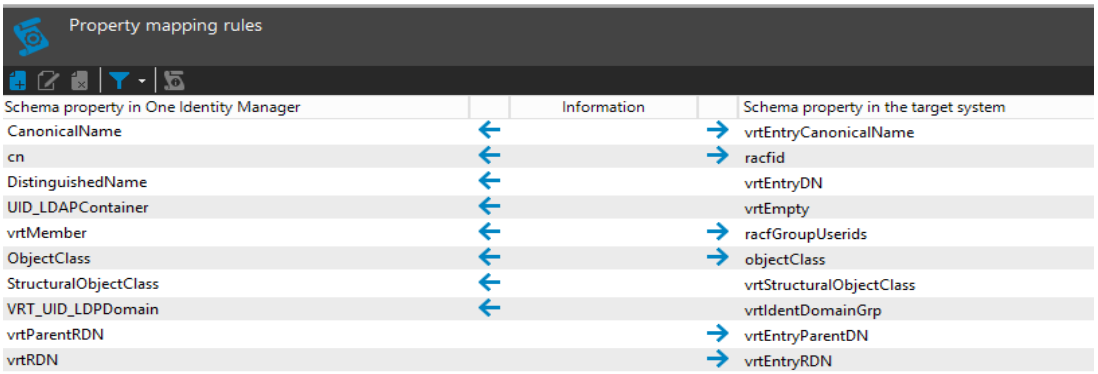
Sample Group Mapping

The following figure shows the above group mapping in operation.



Object matching rules

Schema property in One Identity Manager	Information	Schema property in the target system
DistinguishedName	primary rule	vrtEntryDN



Property mapping rules

Schema property in One Identity Manager		Information		Schema property in the target system
CanonicalName	←		→	vrtEntryCanonicalName
cn	←		→	racfid
DistinguishedName	←			vrtEntryDN
UID_LDAPContainer	←			vrtEmpty
vrtMember	←		→	racfGroupUserids
ObjectClass	←		→	objectClass
StructuralObjectClass	←			vrtStructuralObjectClass
VRT_UID_LDPDomain	←			vrtIdentDomainGrp
vrtParentRDN			→	vrtEntryParentDN
vrtRDN			→	vrtEntryRDN

System Filtering on Users and Groups

The IBM® Tivoli Directory Server does not support standard LDAP filtering but a limited level of functionality is supported. The only attribute that can be filtered is `racfid` which can apply to both user and group names. This means that it is possible to filter on the names of both users and groups.

This is done by applying a system filter to either the `racfuser` or `racfgroup` objects of the form `(racfid=<variable>*)` where `<variable>` applies to a common prefix.

For example, to import only the users that start with "ABC" the following system filter should be applied to the `racfuser` object:

```
(racfid=ABC*)
```

To import only the groups beginning with "#1" the following system filter should be applied to the `racfgroup` object:

```
(racfid=#1*)
```

Data Set Profile Mapping Information

This section shows a possible mapping between a user account in RACF and the standard One Identity Manager database table called `LDAPGroup` (a group is the closest equivalent in One Identity Manager to a data set profile). A mapping for RACF group already exists, so a filter needs to be applied in order to tell these apart.

- When creating the data set profile mapping, add a new schema class as follows.

  Table 4: Schema class settings

Property	Value
Schema type	LDAPGroup
Display name	LDAPGroup (Data set profile)
Class name	LDAPGroup_datasetprofile
Select objects: Condition	StructuralObjectClass='RACFDATASET'
Select objects: Ignore case	Activated

- Select this new schema class, `LDAPGroup (Data set profile)` for this mapping to `racfDataset (all)` on the RACF side.

For more detailed information about setting up mappings, see the Dell One Identity Manager Target System Synchronization Reference Guide.

Detailed information about this topic

- Mandatory RACF Data Set Profile Attributes on page 20
- Property Mapping Rules on page 20
- Object Matching Rules on page 23
- Group Mapping Information on page 14
- Sample Data Set Profile Mapping on page 23

Mandatory RACF Data Set Profile Attributes

When creating a data set profile in the RACF database, the following LDAP attributes must be defined:

- objectclass
- racfDataset

Related Topics

- Property Mapping Rules on page 20
- Object Matching Rules on page 23

Property Mapping Rules

- CanonicalName ← vrtEntryCanonicalName

  `vrtEntryCanonicalName` is a virtual property, set to the canonical name of the object in the connector.

  Sample value:

  `COM/MYCOMPANY/MAINFRAME1/DATASET/ABCDB.*.**`

- cn ←→ racfDataset

  On the RACF system, this refers to the dataset profile ID.

  Sample value:

  `ABCDB.*.**`

- DistinguishedName ← vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector.

  Sample value:

  `racfdataset=ABCDB.*.**,profiletype=dataset,cn=mainframe1,o=mycompany,c=com`

- ObjectClass ←→ objectClass

  The `objectClass` attribute (multi-valued) on the RACF system. Activate the check box **Ignore case sensitivity**.

  Sample value:

  `TOP;RACFBASECOMMON;RACFDATASET`

- StructuralObjectClass ← vrtStructuralObjectClass

  `vrtStructuralObjectClass` on the RACF system defines the single object class for the object type.

  Sample value:

  `RACFDATASET`

- VRT_UID_LDPDomain ← vrtIdentDomain

  Create a fixed value property variable on the RACF side called `vrtIdentDomain` that is set to the value `$IdentDomain$`. Map this to V`RT_UID_LDPDomain`, the attribute created by One Identity Manager when this step was performed for a group mapping above.

  Sample value:

  `RACF_DOMAIN`

- vrtDatasetParentDN → vrtEntryParentDN

  Create a fixed value property variable on the One Identity Manager side called `vrtDatasetParentDN` equal to a fixed string with value `$DatasetLocation$`. Map this to `vrtEntryParentDN` on the RACF side.

  Sample value:

  `profiletype=dataset,cn=mainframe1,o=mycompany,c=com`

- vrtDatasetRDN → vrtEntryRDN

  Create a new variable on the One Identity Manager side of type "Script Property" with name `vrtDatasetRDN` and a data type of “string”. In the Scripts section, enter one of the he following scripts in the Read script section, depending on whether your project is configured for C# or Visual Basic.

  C# Script

  ```
  references VI.TSUtils.dll;

  return (VI.TargetSystem.Base.Utils.LDAP.RDN.Create("cn", useOldValues ? $cn[o]$
  : $cn$).ToString()).Replace("cn=","racfDataset=");
  ```

  VB Script

```
References VI.TSUtils.dll

Imports VI.TargetSystem.Base.Utils.LDAP

Dim name as String = ""

If useOldValues Then

     name = $cn[o]$

Else

     name = $cn$

End If

return RDN.Create("cn",name).ToString().Replace("cn=","racfDataset=")
```

Then map this to `vrtEntryRDN` on the RACF side.

Sample value:

```
ABCDB.*.**
```

- BusinessCategory ←→ uid

  This is a multi-valued string that contains the RACF user IDs and the rights they have been granted for a particular data set profile. Changes to this list on the RACF side can be performed by synchronizing the necessary changes from the One Identity Manager side. `BusinessCategory` was chosen for the mapping as it was a pre-existing multi-valued string.

  Sample value:

  ```
  USER001(READ); USER002(ALTER); USER003(READ)
  ```

- vrtDatasetMember ←→ racfPermitId

  This mapping is used to synchronize data set membership information.

  1. Create a new virtual entry on the One Identity Manager side of type "Members of M:N schema types" with name `vrtDatasetMember`. Activate the check boxes to **Ignore case** and **Enable relative component handling**.
  2. Add the following M:N schema types:
     a. Add an entry for `LDAPAccountInLDAPGroup`. Set the left box to `UID_LDAPGroup` and the right box to `UID_LDAPAccount`. Set the **Primary Key Property** to `DistinguishedName`.
     b. Add an entry for `LDAPGroupInLDAPGroup`. Set the left box to `UID_LDAPGroupParent` and the right box to `UID_LDAPGroupChild`. Set the **Primary Key Property** to `DistinguishedName`.
  3. Create a new mapping rule of type "Multi-reference mapping rule". Set the rule name to "Member" and the mapping direction to "Both directions". Set the One Identity Manager schema property to `vrtDatasetMember` and the RACF schema property to `racfPermitId`.

     NOTE: When this membership mapping has been set up at the same time as that for groups (vrtMember <-> racfGroupUserids in the group mapping) the data set synchronization will populate both the `vrtDatasetMember` and `vrtMember` attributes with the same values. The values stored in `vrtMember` can be ignored.

Related Topics

- Mandatory RACF Data Set Profile Attributes on page 20
- System Variables on page 8
- Object Matching Rules on page 23
- Sample Data Set Profile Mapping on page 23

Object Matching Rules

- DistinguishedName (primary rule) vrtEntryDN

  `vrtEntryDN` is a virtual property, set to the DN of the object in the connector. This forms a unique ID to distinguish individual dataset objects on the RACF system.

  To convert this mapping into an object matching rule

  1. Select the property mapping rule in the rule window.
  2. Click  in the rule view toolbar.

     A message appears.
  3. Click **Yes** to convert the property mapping rule into an object matching rule and save a copy of the property mapping rule.

  Sample value:

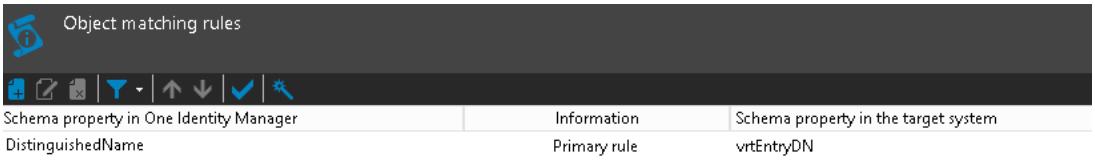
  ```
  racfdataset=ABCDB.*.**,profileType=dataset,cn=mainframe1,o=mycompany,c=com
  ```

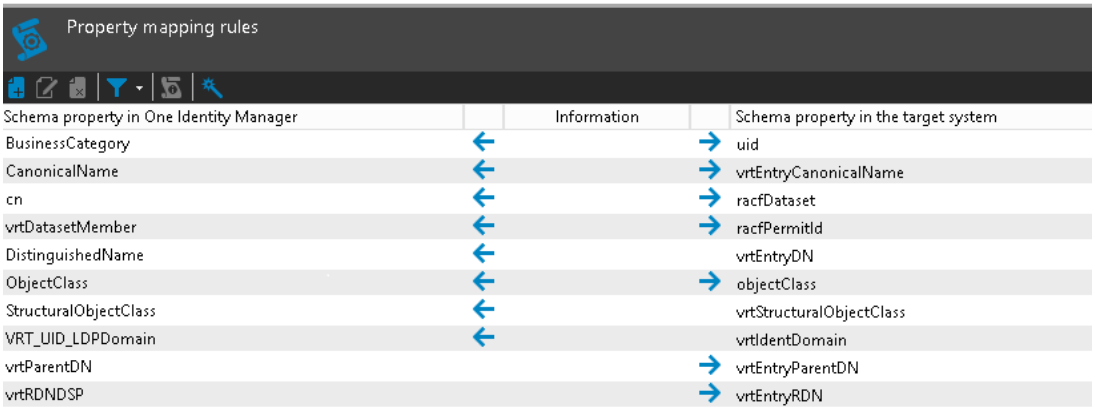
Related Topics

- Mandatory RACF Data Set Profile Attributes on page 20
- Property Mapping Rules on page 20
- Sample Data Set Profile Mapping on page 23

Sample Data Set Profile Mapping

The following figure shows the above data set profile mapping in operation.





TSO Command Execution

The RACF LDAP Connector can be used to execute any TSO command on the connected system if the Quest RACF TDS Exit has been installed and configured. This TSO command execution needs to be configured manually for the connector made available with One Identity Manager 7.1.3.

The required steps are:

1. Adding the component definition
2. Creating a process

   For more detailed information, see the Dell One Identity Manager Configuration Guide.

Detailed information about this topic

- Pre-requisites on page 24
- Component definition setup on page 25

Pre-requisites

The file called `VI.Projector.MFRJobComponent.dll` needs to be present in One Identity Manager installation directory. The file needs to be copied from the installation source to here:

```
<root drive>\Program Files\Dell\One Identity Manager
```

Component definition setup

The following steps should be followed to set up a component definition to run TSO commands that can be called from other parts of One Identity Manager.

To set up the component definition

1. Select the category **Process Orchestration | Process components** in the Designer.
2. In the Process Component Editor, select the menu item **Objects | New process component**.
3. Enter the following values.

   Table 5: Process Component Properties

Property	Value
Display name	MFRComponent
Component class	VI.Projector.MFR.JobComponent.MFRComponent
Version	1.0
Assembly Name	VI.Projector.MFR.JobComponent

4. In the Process Component Editor, select the newly created `MFRComponent` and select **New process task** in the context menu.
5. On the **Properties** tab, enter the following values.

   Table 6: Process Task Properties

Property	Value
Name	RacfRunTSOCommand
Operating system class	WIN32
Execution type	EXTERNAL

6. In the Process Component Editor, select the newly created task called `RacfRunTSOCommand`.
7. Select **New parameter** in the context menu.
8. Enter the process parameter values in the **Properties** tab.
9. Repeat the steps for every required parameter.
10. To commit your changes, select menu item **Database | Commit to database...**.

The following six parameters need to be set up; these are performed one at a time.

- CommandLine

  Enter your required TSO command where it says `Your TSO command here`.

Table 7: Process parameter CommandLine

Property	Value
Name	CommandLine
Value template	Value="Your TSO command here"
Value template (example)	Value="Your TSO command here", e.g. Value="TIME"

- ConnectionProvider

Table 8: Process Parameter ConnectionProvider

Property	Value
Name	ConnectionProvider
Value template	Value=ConnectionInfo.ConnectionProvider
Value template (example)	Value=ConnectionInfo.ConnectionProvider

- ConnectionString

Table 9: Process Parameter ConnectionString

Property	Value
Name	ConnectionString
Value template	Value=ConnectionInfo.ConnectionString
Value template (example)	Value=ConnectionInfo.ConnectionString
Hidden	True
Encrypted	True

- UID_DPRShell

Table 10: Process Parameter UID_DPRShell

Property	Value
Name	UID_DPRShell
Value template	Value="UID of shell here"
Value template (example)	Value="UID of shell here"

- UID_DPRSystemVariableSet

Table 11: Process Parameter UID_DPRSystemVariableSet

Property	Value
Name	UID_DPRSystemVariableSet
Value template	Value="UID of DPRSystemVariableSet here"
Value template (example)	Value="UID of DPRSystemVariableSet here"

- OutputParamater

Table 12: Process Parameter OutputParameter

Property	Value
Name	OutputParameter
Value template	Value="Output"
Value template (example)	Value="Output"
Optional	True

Auxiliary Classes

The RACF user and group objects have a number of auxiliary classes available to add extra attributes. There are 12 of these auxiliary classes in total.

Auxiliary classes that can extend the RACF user object:

- SAFTSOSegment
- SAFDfpSegment
- racfCicsSegment
- racfLanguageSegment
- racfOperparmSegment
- racfWorkAttrSegment
- racfUserOmvsSegment
- racfUserOvmSegment
- racfNetviewSegment
- racfDCESegment

Auxiliary classes that can extend the RACF group object:

- racfGroupOmvsSegment
- racfGroupOvmSegment
- SAFDfpSegment

The list of the additional attributes that each of these makes available is given in Appendix: Auxiliary Classes on page 33.

When the RACF user or group object is viewed in the Synchronization Editor, all of the attributes made available by all of the above auxiliary classes are listed by default and can be used in user or group mappings. In order to make use of the additional attributes during a synchronization to RACF, the user or group object must contain the corresponding object class for each additional attribute, otherwise the attribute will be discarded. The object class attribute for a user is multi-valued and must contain the full list of all object classes needed for the user.

For example, the auxiliary class `racfUserOvmSegment` contains an attribute called `racfOvmUid`.

To successfully synchronize a value to this attribute for a user, the user object must contain the value `racfUserOvmSegment` in its object class attribute.

RACF Groups and RACF Universal Groups

A standard RACF group keeps track of its members in an attribute called `racfGroupUserIds`. This imposes a limit on the number of members a group can have because there is a fixed amount of space in a group's profile to store this information. The limit is approximately 6,000 users.

To get around this, IBM® introduced universal groups. Universal group profiles do not list user members whose group authority is set to `USE` and since most users will have this as their group authority, the number of possible user members is increased well over the 6,000 limit.

Creating a Universal Group

A universal group is created the same as standard group except that the `racfAttributes` attribute for the group must be set to `UNIVERSAL` when the group is created. This must be done when the group is created; a standard group cannot be converted to a universal group after it has been created.

Group Authority

When a user is connected to a group, the user's group authority level needs to be specified. The default level is `USE` but it is possible to set this to a different value. In order to do this, a virtual attribute called `vrtGroupPermission` needs to be enabled for user mappings. This is done in the RACF connection configuration wizard on the "Search Options" panel. Check the box next to **Use vrtGroupPermission** to enable this virtual attribute in user searches and mappings.

Synchronizing Group Members

There are a number of ways to synchronize group memberships. The method used will depend on whether the group is a universal group and whether the group authority level needs to be a value different from the default of `USE`. There are three options available; but note that only one of the three options should be used with any one group:

- Standard Group and all Users have Default Authority

  In this case, the list of group members should be synchronized to the group attribute `racfGroupUserIds`. Entries to be synchronized take the form of the DN of each user member. For more information, see Sample Group Mapping on page 18.

- Universal Group and all Users have Default Authority

  In this case, the group memberships need to be synchronized on a per-user basis using the user attribute `racfConnectGroupName`. Entries to be synchronized take the form of the DN of each of the groups that the user is to be connected to.

- Any Group Type and some Users have non-Default Authority

  In this case, the group memberships need to be synchronized on a per-user basis using the virtual user attribute `vrtGroupPermission`. The values to be synchronized must take the form

  ```
  <group ID> (<Authority level>)
  ```

A

Appendix: RACF User Attributes

The following table lists the RACF user attributes that are made available to One Identity Manager by the RACF LDAP Connector.

Table 13: List of RACF User Attributes

Attribute Name
racfAttributes
racfAuthorizationDate
racfClassName
racfConnectGroupAuthority
racfConnectGroupName
racfConnectGroupUACC
racfDatasetModel
racfDefaultGroup
racfHavePassPhraseEnvelope
racfHavePasswordEnvelope
racfid
racfInstallationData
racfLastAccess
racfLogonDays
racfLogonTime
racfOwner
racfPassPhrase
racfPassPhraseChangeDate
racfPassPhraseEnvelope
racfPassword
racfPasswordChangeDate
racfPasswordEnvelope

Attribute Name
racfPasswordInterval
racfProgrammerName
racfResumeDate
racfRevokeDate
racfSecurityLabel
racfSecurityLevel

B

Appendix: RACF Group Attributes

The following table lists the RACF group attributes that are made available to One Identity Manager by the RACF LDAP Connector.

Table 14: List of RACF Group Attributes

Attribute Name
racfAuthorizationDate
racfDatasetModel
racfGroupNoTermUAC
racfGroupUniversal
racfGroupUserids
racfid
racfInstallationData
racfOwner
racfSubGroupName
racfSuperiorGroup

C

Appendix: RACF Data Set Profile Attributes

If the Quest RACF TDS Exit has been installed and enabled, the following RACF data set profile attributes will be made available to Dell One Identity Manager by the RACF LDAP Connector.

Table 15: List of RACF Data Set Profile Attributes

Attribute Name
racfAccess
racfAudit
racfCreateGroup
racfDataset
racfErase
racfGlobalAudit
racfNotify
racfOwner
racfPermitid
racfUacc
racfWarning
uid

D

Appendix: Auxiliary Classes

The following list defines all of the auxiliary classes for RACF user and group classes, along with their associated attributes.

Auxiliary class `SAFDfpSegment` for RACF user and RACF group

- SAFDfpDataApplication
- SAFDfpDataClass
- SAFDfpManagementClass
- SAFDfpStorageClass

Auxiliary class `racfGroupOmvsSegment` for RACF group

- racfOmvsGroupId

Auxiliary class `racfGroupOvmSegment` for RACF group

- racfOvmUserId

Auxiliary class `SAFTsoSegment` for RACF user

- SAFAccountNumber
- SAFDefaultCommand
- SAFDestination
- SAFHoldClass
- SAFJobClass
- SAFMessageClass
- SAFDefaultLoginProc
- SAFLogonSize
- SAFMaximumRegionSize
- SAFDefaultSysoutClass
- SAFUserdata
- SAFDefaultUnit
- SAFTsoSecurityLabel

Auxiliary class `racfCicsSegment` for RACF user

- racfOperatorIdentification
- racfOperatorClass

- racfOperatorPriority
- racfOperatorReSignon
- racfTerminalTimeout

Auxiliary class `racfLanguageSegment` for RACF user

- racfPrimaryLanguage
- racfSecondaryLanguage

Auxiliary class `racfOperparmSegment` for RACF user

- racfStorageKeyword
- racfAuthKeyword
- racfMformKeyword
- racfLevelKeyword
- racfMonitorKeyword
- racfRoutcodeKeyword
- racfLogCommandResponseKeyword
- racfMGIDKeyword
- racfDOMKeyword
- racfKEYKeyword
- racfCMDSYSKeyword
- racfUDKeyword
- racfMscopeSystems
- racfAltGroupKeyword
- racfAutoKeyword

Auxiliary class `racfWorkAttrSegment` for RACF user

- racfWorkAttrUserName
- racfBuilding
- racfDepartment
- racfRoom
- racfAddressLine1
- racfAddressLine2
- racfAddressLine3
- racfAddressLine4
- racfWorkAttrAccountNumber

Auxiliary class `racfUserOmvsSegment` for RACF user

- racfOmvsUid
- racfOmvsHome
- racfOmvsInitialProgram

Auxiliary class `racfNetviewSegment` for RACF user

- racfNetviewInitialCommand
- racfDefaultConsoleName
- racfCTLKeyword
- racfMSGRCVRKeyword
- racfNetviewOperatorClass
- racfDomains
- racfNGMFADMKeyword

Auxiliary class `racfDCESegment` for RACF user

- racfDCEUUID
- racfDCEPrincipal
- racfDCEHomeCell
- racfDCEHomeCellUUID
- racfDCEAutoLogin

Auxiliary class `racfUserOvmSegment` for RACF user

- racfOvmUid
- racfOvmHome
- racfOvmInitialProgram
- racfOvmFileSystemRoot
- racfOvmHomeUUID

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.quest.com.

Contacting Dell

For sales or other inquiries, visit http://quest.com/company/contact-us.aspx or call +1 949 754-8000.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.quest.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to http://quest.com/trials.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer