SecurID

RSA® Authentication Manager 8.6

RSA RADIUS Migration

RSA Authentication Manager 8.6 RSA RADIUS Pre-Migration Script

SecurID provides an RSA RADIUS pre-migration script that locates any RSA RADIUS issues that need to be corrected before upgrading from RSA Authentication Manager 8.5 to RSA Authentication Manager 8.6.

The script generates an HTML report. You must manually resolve any issues that are identified. After you resolve any issues, run the script again.

When there are no more issues, you can upgrade to version 8.6.

If you are not using RSA RADIUS, you can upgrade without running the script.

Note: SecurID strongly recommends backing up your deployment before upgrading Authentication Manager.

Run the Script

Before upgrading to RSA Authentication Manager 8.6, run the RSA RADIUS pre-migration script on the primary instance.

Before you begin

- You must have the **rsaadmin** operating system password to log on to the primary instance.
- The script prompts you for Operations Console administrator credentials.
- Running the script restarts the RADIUS service.

Procedure

1. Download **rsa-am-pre-upgrade-check-2.1.zip** from RSA Link (sign on required).
2. Move **rsa-am-pre-upgrade-check-2.1.zip** into the **/opt/rsa/am/utils/** directory on the RSA Authentication Manager primary instance.
3. Change the directory to **/opt/rsa/am/utils**, and unzip **rsa-am-pre-upgrade-check-2.1.zip**.
4. Change the directory to **/opt/rsa/am/utils/rsa-am-pre-upgrade-check-2.1**, and provide executable permission for the file **rsa_am_preupgrade_check-2.1.sh**. For example,

   ```
   chmod 777 rsa_am_preupgrade_check-2.1.sh
   ```

5. Execute the file:

   ```
   ./rsa_am_preupgrade_check-2.1.sh
   ```

   The script restarts the RADIUS service.

6. After the script completes, check the HTML report. The report path is specified in the console script output:

```
/opt/rsa/am/radius-migration/<report_date_timestamp>
```

7. Resolve any issues that are listed in the report. For information on how to resolve RADIUS client IP address conflicts, RADIUS dictionary file issues, and RADIUS profiles with unknown attributes, see Resolving RSA RADIUS Issues below.

FAILURES	
WARNINGS	Apr 27, 2022 9:09:10 AM | Changing SBR attribute named EAP-Message from octets to octets concat Apr 27, 2022 9:09:10 AM | Changing SBR attribute named state from string to octets
ADDITIONAL FAILURES	Radius Client IP Conflict click here for more details Radius Clients with Empty Shared Secret click here for more details

8. After resolving any issues, run the script again.

   When the HTML report shows success, you can upgrade to RSA Authentication Manager 8.6.

RSA RADIUS Migration Report_020922_0629AM_UTC

This report summarizes the results of migrating RSA RADIUS to RSA Authentication Manager 8.6. For troubleshooting instructions and additional details, see the RSA Authentication Manager 8.6 Setup and Configuration Guide.

Pre-Migration Report	
Pre-Migration Results	Success
Total Vendors (Make and Model) Found	131
Total Vendors (Make and Model) Considered for Migration	2
Vendors (Make and Model) Considered for Migration	- Standard Radius -
Total Vendors (Make and Model) Migrated Successfully	2
Total Vendors (Make and Model) that Failed to Migrate	0

After you finish

After successfully upgrading to RSA Authentication Manager 8.6, you can delete the zip file and the folder:

1. Change the directory to **/opt/rsa/am/utils/**.
2. Run the following commands:

```
rm rsa-am-pre-upgrade-check-2.1.zip
```

```
rm rsa-am-pre-upgrade-check-2.1
```

Resolving RSA RADIUS Issues

You can choose how to resolve any RSA RADIUS issues that are listed in the pre-migration HTML report:

- RADIUS Client IP Address Conflicts
- RADIUS Dictionary File Issues on page 5
- RADIUS Profiles with Unknown Attributes on page 6
- Invalid Radius Client Name on page 7
- Invalid Radius IP Address on page 7

RADIUS Client IP Address Conflicts

Resolve any RADIUS client IP address conflicts that are displayed in the HTML report. The report displays a resolution number for different types of IP address conflicts. You can sometimes choose from several approaches for resolving IP address conflicts.

HTML Report also displays the conflicts between the Radius client IP and the IP Address of the Authentication Manager.

Example: Radius client IP Address same as Host IP Address.

To resolve this issue, perform the following:

Procedure

1. Navigate to **/opt/rsa/am/radius-migration/<report_date_timestamp>**.
2. Open the **rsa_am_preupgrade_check_<report_date_timestamp>.log**.
3. Check for the error message **"Radius client IP Address same as Host IP Address"**.
4. Below the error message, RADIUS client names with Incorrect IP addresses are listed.

   Example: The Radius Client IP is same as the Host IP in Radius Client Name : RADCLINT1.
5. Next, log in to the **Security Console** as admin.
6. Navigate to **RADIUS** > **RADIUS Clients** > **Manage Existing**.
7. Search for the clients displayed in the log.
8. Update the RADIUS clients with a valid IP address and then click **Save**.

Resolution No 1: Conflict with Agent(s) Primary IP

To resolve this issue, choose one of the following options.

Option A: Make the IP address the Same for the RADIUS Client and its Associated Agent

Procedure

1. Update the agent with the IP address conflict:
   a. In the Security Console, click **Access > Authentication Agents > Manage Existing**.
   b. Search for the agent.
   c. Update the Primary IP address with a unique IP address.
2. Update the primary IP address of the RADIUS Client:
   a. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
   b. Search for the RADIUS client.
   c. Edit the RADIUS client. Update the RADIUS client IP address with its current IP address or with the IP address used by its associated Agent.
3. Verify that RADIUS authentication and agent authentication is working normally.

Option B: Update the RADIUS Client with a Unique IP Address

Procedure

1. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
2. Search for the RADIUS client
3. Update the client IP address with a unique IP address.
4. Verify that RADIUS authentication and agent authentication is working normally.

Resolution No 2: Conflict with Agent's Alternate IP

To resolve this issue, choose one of the following options.

Option A: Make the IP address the Same for the RADIUS client and its Associated Agent

Procedure

1. Update the agent with the IP address conflict:
    a. In the Security Console, click **Access > Authentication Agents > Manage Existing**.
    b. Search for the agent with the IP address conflict.
    c. Update the Alternate IP address with a unique IP address or remove the Alternate IP address.
2. Update the primary IP address of the RADIUS Client:
    a. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
    b. Search for the RADIUS client.
    c. Edit the RADIUS client. Update the RADIUS client with its current IP address or the IP address used by its associated agent.
3. Verify that RADIUS authentication and agent authentication is working normally.

Option B: Update the RADIUS Client with a Unique IP Address

Procedure

1. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
2. Search for the RADIUS client
3. Update the client IP address with a unique IP address.
4. Verify that RADIUS authentication and agent authentication is working normally.

Resolution No 3: Conflict with Radius Client(s)

To resolve this issue, choose one of the following options.

Option A: Make the IP address the Same for the RADIUS Client and its Associated Agent

Procedure

1. Update or remove the Alternate IP address of the RADIUS client with the IP address conflict
    a. In the Security Console, click **Access > Authentication Agents > Manage Existing**.
    b. Search for the agent with the IP address conflict.

c. Update the Alternate IP address with a unique IP address or remove the Alternate IP address.

2. Update the primary IP address of the RADIUS Client:
    a. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
    b. Search for the RADIUS client.
    c. Edit the RADIUS client. Update the RADIUS client with its current IP address or the IP address used by its associated agent.
3. Verify that RADIUS authentication is working normally.

Option B: Update the RADIUS Client with a Unique IP Address

Procedure

1. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
2. Search for the RADIUS client
3. Update the client IP address with a unique IP address.
4. Verify that RADIUS authentication is working normally.

RADIUS Dictionary File Issues

Resolve any RADIUS dictionary file issues that are displayed in the HTML report.

Make and Model Entry Missing in Vendor.ini

When a make and model entry is missing in **vendor.ini**, the following message displays:

```
<date-timestamp>| The vendor model named ***** of radius client ***** does not exist in the vendor.ini file and will not be considered for migration.
```

For example,

```
Feb 03, 2022 5:02:35 PM | The vendor model named "ACC Tigris and Amazon Servers" of radius client "RADIUS_APC_CLIENT" does not exist in the vendor.ini file and will not be considered for migration.
```

You can either add the make and model to a RADIUS dictionary or delete any RADIUS clients that use the missing information.

Option A: Add the Missing Make and Model

You can add the missing make and model if RADIUS client require this information.

Procedure

1. In the Operations Console, click **Deployment Configuration > Radius Server > Manage Server Files > Configuration Files**.
2. Select the **vendor.ini** file.
3. Click **Edit**, and add or update the missing vendor model.
4. Save your changes.
5. Log on to the appliance operating system, and verify that the associated dictionary file is available in the directory **/opt/rsa/am/radius**. Restore the file if it is missing.
6. Restart the RADIUS server. For example, type:

cd /opt/rsa/am/server

./rsaserv restart radius.

7. Verify that RADIUS authentication is normal.

Option B: Delete the RADIUS Clients that Use the Missing Make and Model

You can delete any RADIUS clients that are not used for authentication.

Procedure

1. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
2. Click the client that you want to delete.
3. From the context menu, click **Delete**.

RADIUS Dictionary File Missing

When a RADIUS Dictionary file is missing, the following message displays:

```
<date-timestamp>| The vendor model named ***** of radius client ***** does not have a valid dictionary file ***** in path /opt/rsa/am/radius and will not be considered for migration.
```

For example:

```
Feb 03, 2022 5:02:35 PM | The vendor model named "APC MODEL" of radius client "DJS-Client" does not have a valid dictionary file "apc.dct" in path /opt/rsa/am/radius and will not be considered for migration.
```

You can either restore the missing dictionary file or delete any RADIUS clients that are not used for authentication.

Option A: Restore a Missing Dictionary File

Procedure

1. In the Operations Console, click **Deployment Configuration > RADIUS Servers > Manage Server Files > Dictionary Files**.
2. Click **Add New**, select the dictionary file, and click Submit.
3. Restart the RADIUS server.
4. Verify that RADIUS authentication is normal.

Option B: Delete the RADIUS Clients that Use the Missing Dictionary File

You can delete any RADIUS clients that are not used for authentication.

Procedure

1. In the Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
2. Click the client that you want to delete.
3. From the context menu, click **Delete**.

RADIUS Profiles with Unknown Attributes

When RADIUS profiles have unknown attributes, the following message displays:

```
Failed to check profile attribute :****** for profile: ******
```

For example:

```
Failed to check profile attribute :SonicWall-User-Privilege for profile:
Sonic-Profile
```

This message has two causes:

1. No RADIUS clients use a make and model that corresponds to the RADIUS profile attributes.

   You can either add a RADIUS client that uses the RADIUS profile, for example, a fake RADIUS client with a fake IP address, or you can verify that the RADIUS profile is not needed and delete it. Use the Security Console to verify that the RADIUS profile does not have any associated agents, users, user aliases, or trusted users.

2. The dictionary file in the make and model of the RADIUS client was changed, and this caused the RADIUS profile attributes to disappear from the RADIUS dictionary file.

   Most likely the RADIUS profile is not in use. You can either add the profile attributes back to the corresponding RADIUS dictionary file, or you can verify that the RADIUS profile is not needed and delete it. Use the Security Console to verify that the RADIUS profile does not have any associated agents, users, user aliases, or trusted users.

Invalid Radius Client Name

Resolve any RADIUS client name with an invalid special character or length greater than 50 character.

Caution: Do not use the following special characters ~ ` ! @ # $ % ^ & * ( ) = + [ ] { } \ | ; : ' " , < > / ? in client name. If used these special characters will be considered as invalid.

Procedure

1. Navigate to **/opt/rsa/am/radius-migration/<report_date_timestamp>**.
2. Open the **rsa_am_preupgrade_check_<report_date_timestamp>.log**.
3. Check for the error message "Radius Client With Invalid Name" from the log.
4. Below the error message from step 3, Invalid RADIUS client names are listed.
   For example: Invalid Radius Client Name: RADCLISP/14
5. Log in to **Security Console** as admin.
6. Navigate to **RADIUS** > **RADIUS Clients** > **Manage Existing**.
7. Search for the clients displayed in the log.
8. Delete the existing client.
9. Create a client again with a valid name.

Invalid Radius IP Address

Resolve any RADIUS client that has an invalid IP Address.

Procedure

1. Navigate to **/opt/rsa/am/radius-migration/<report_date_timestamp>**.
2. Open the **rsa_am_preupgrade_check_<report_date_timestamp>.log**.
3. Check for error message "Radius client with Invalid IP Address" from the log.
4. Below this error message from step 3, RADIUS client names which are having invalid IP address are listed.
   For example: Invalid Radius Client IP in Radius Client Name: RADCLISP13.
5. Log in to **Security Console** as admin.
6. Navigate to **RADIUS** > **RADIUS Clients** > **Manage Existing**.

7. Search for the clients displayed in the log.
8. Update the RADIUS clients with a valid IP address and then click **Save**.

Warnings

RADIUS Client missing in the RADIUS server

This warning displays the list of RADIUS clients missing in the RADIUS Server database.

Procedure

1. Log in to **Security Console** as admin.
2. Navigate to **RADIUS** > **RADIUS Clients** > **Manage Existing**.
3. Search for the clients one by one listed on the HTML report.
4. Delete the clients.

RADIUS Client missing in Authentication Manager

This warning displays the list of RADIUS clients that are missing in Authentication Manager, but available in the RADIUS server.

1. In the HTML report, check for the error message "*The number of RADIUS clients that need to be synched from SBR to AM database is: <NUMBER>*".
2. In the log file, verify the following messages to know the status of the client:
    - Added the RADIUS client from SBR database to AM database:<CLIENT_NAME>
    - Deleted RADIUS client from SBR database: <CLIENT_NAME>.

These issues will get resolved during data sync automatically. To verify, run the tool again and check the HTML report not showing the warning for missing clients in Authentication Manager.

Radius Client Associated Agent with Sub Domain

To resolve Radius Client associated agent with sub domain, either upgrade the environment to 8.6Patch4 or perform the following:

Procedure

1. Navigate to **/opt/rsa/am/radius-migration/<report_date_timestamp>**.
2. Open the **rsa_am_preupgrade_check_<report_date_timestamp>.log**.
3. Check for the error message **"Radius Client Associated Agent With Sub Domain"**.
4. Below the error message, you can view the Agent names that have a sub domain.

    Example: Radius Client Associated Agent with sub domain: TESTSUBRADCLINET
5. Next, log in to the **Security Console** as admin.
6. Navigate to **Access** > **Authentication Agents** > **Manage Existing**.
7. Search for the Agent displayed in the log.
8. Delete the existing agent and recreate a new one with the system domain and the same IP address.

RADIUS Client Profile Check list Attribute (User-Name):

To resolve the User-Name attribute issue, either upgrade the environment to 8.6Patch4 or perform the following:

Procedure

1. Log in to **Security Console** as admin.
2. Navigate to **RADIUS** > **RADIUS Profiles**> **Manage Existing**.
3. Search the name of the RADIUS profile displayed on the HTML page.
4. Edit the profile and remove **User-Name** attribute from check list and click **Save.**

RADIUS Client with Invalid Shared Secret

Resolve any RADIUS client with invalid shared secret that are displayed in the HTML report. Invalid shared secret refers to empty shared secret or special characters in shared secret.

- RADIUS clients with empty shared secret will result in 8.6 upgrade failures.
- RADIUS clients with special characters will not cause any upgrade failures but authentication will fail after successful upgrade.

  Caution: Do not use the following special characters ****, **`**, **'**, and **’**, in Shared Secret. If used, these special characters may cause authentication failures in AM 8.6. Special charters will work after the environment is upgraded to 8.6Patch4. However, certain combination with backslash (\) will not function accurately. Refer to the known issues to understand the limitation of special characters.

Procedure

1. Navigate to **/opt/rsa/am/radius-migration/<report_date_timestamp>**.
2. Open the **rsa_am_preupgrade_check_<report_date_timestamp>.log**.
3. To identify the type of invalid shared secret, check for the "Radius Client with empty shared secret" or "Radius Client with invalid special character in shared secret" message in the log.
   For example: Radius Client with empty shared secret: SDKCLIN5
   Radius Client with invalid special character in shared secret: TESTCLIENT
4. Log in to **Security Console** as admin.
5. In Security Console, click **RADIUS > RADIUS Clients > Manage Existing**.
6. Search for the clients one by one listed on the HTML report for **Radius Clients** with **Invalid Shared Secret**.
7. Edit the **Radius Clients** and update the **Shared Secret**.
8. Click **Save**.

Known Issues

This section lists known issues and workarounds.

RADIUS authentication failures were reported after the upgrade to 8.6Patch4. This was caused because the RADIUS client had a backslash (\) in the shared secret.

Tracking Number: **AM-46616** and **AM-46592**.

Problem: After an upgrade to AM 8.6Patch4, if the radius client shared secret has a backslash, then the RADIUS authentication fails.

Workaround: Update the shared secret with proper value.

Support and Service

You can access community and support information on RSA Link at https://community.rsa.com. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at https://community.securid.com/t5/securid-integrations/tkb-p/securid-access-integrations provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

January 2021

Intellectual Property Notice

Open Source License