```
*--host*:
```

updates the hostname of the appliance. If you performed this step using the console and made the necessary updates made to **`/etc/hosts`** if DNS is not properly configured, you can omit the **`--host`** option.

```
*--iparealm*:
```

if omitted, the **`iparealm`** is based on the domain name of the**`ipaserver`**.

```
*--ipaprincipal*:
```

if omitted, defaults to admin.

Example 4.1. Configuring External Authentication

```
$ ssh root@appliance.test.company.com
[appliance]# /bin/appliance_console_cli --host
appliance.test.company.com \
                                      --ipaserver
ipaserver.test.company.com \
                                      --iparealm TEST.COMPANY.COM
\
                                      --ipaprincipal admin \
                                      --ipapassword smartvm1
```

Example 4.2. Reverting to Internal Database Authentication

```
$ ssh root@appliance.test.company.com
[appliance]# /bin/appliance_console_cli --uninstall-ipa
```

4.1.4.2.9. Configuring External Authentication Using SAML

This procedure outlines how to manually configure an appliance to use SAML external authentication. While other SAML identity providers can be used with Red Hat CloudForms, this procedure covers using Red Hat Single Sign-On (SSO) 7.0, which is implemented using the Apache HTTP server's **`mod_auth_mellon`** module.

To enable external authentication using SAML, complete the following steps to configure your HTTP server, then your Red Hat CloudForms appliance.

Note

The current SAML implementation only secures the Red Hat CloudForms appliance's web administrative user interface with SAML. The REST API and self service user interface do not currently support SAML.

Requirements

The following is required in order to enable SAML authentication to the appliance:

- A CloudForms 4.1 appliance
- A SAML identity provider (e.g. Red Hat Single Sign-On (SSO) 7.0 or later)

Configuring the HTTP Server for SAML

The Apache HTTP server first must be configured to work with SAML authentication. All SAML-related certificates and keys are accessed from **`/etc/httpd/saml2/`**.

1. Log into the Red Hat CloudForms appliance as root using SSH, and create the **`/etc/httpd/saml2/`** directory:

   ```
   # mkdir -p /etc/httpd/saml2
   ```

2. Copy the **`httpd`** remote user and SAML template configuration files to the appliance:

   ```
   # TEMPLATE_DIR="/opt/rh/cfme-appliance/TEMPLATE"
   # cp ${TEMPLATE_DIR}/etc/httpd/conf.d/manageiq-remote-user.conf
   /etc/httpd/conf.d/
   # cp ${TEMPLATE_DIR}/etc/httpd/conf.d/manageiq-external-auth-
   saml.conf /etc/httpd/conf.d/
   ```

   Note

   The following are notable SAML configuration defaults in the **`manageiq-external-auth-saml.conf`** file:

   - Identity Provider Files (i.e. Red Hat SSO)
     - Metadata File: **`/etc/httpd/saml2/idp-metadata.xml`**
   - Service Provider Files (i.e. **`mod_auth_mellon`**)
     - Private Key File: **`/etc/httpd/saml2/miqsp-key.key`**
     - Certificate File: **`/etc/httpd/saml2/miqsp-cert.cert`**
     - Metadata File: **`/etc/httpd/saml2/miqsp-metadata.xml`**

   Other **`mod_auth_mellon`** parameters, such as endpoints and protected URLs, must not be modified as the appliance expects them to be defined as such.

3. Generate the service provider files on the appliance using the Apache HTTP server's **`mod_auth_mellon`** command **`mellon_create_metadata.sh`**:

   ```
   # cd /etc/httpd/saml2
   # /usr/libexec/mod_auth_mellon/mellon_create_metadata.sh
   https://<miq-appliance> https://<miq-appliance>/saml2
   ```

   The **`mellon_create_metadata.sh`** script creates file names based on the appliance URL.

4. Rename the files created by the **mellon_create_metadata.sh** script to match the expected file names from the **manageiq-external-auth-saml.conf** file:

   ```
   # mv https_<miq-appliance>.key  miqsp-key.key
   # mv https_<miq-appliance>.cert miqsp-cert.cert
   # mv https_<miq-appliance>.xml  miqsp-metadata.xml
   ```

5. Now that the service provider’s **metadata.xml** file has been generated, the service provider definition can be defined in the SAML identity provider. For Red Hat SSO, a realm can be created for one or more appliances with individual clients defined one per appliance, where the client ID is specified as the URL of the appliance.

   To add a client in the Red Hat SSO Red Hat CloudForms realm:

   a. Select and import the **miqsp-metadata.xml** file created for **mod_auth_mellon**.

   b. Set the client ID as **https://<miq-appliance>**.

   c. Set the client protocol as **saml**.

6. Update the client definition for the appliance in Red Hat SSO with the following:

Setting	Value
Name ID Format	username
Valid Redirect URIs	https://<miq-appliance>/saml2/postResponse
Master SAML Processing URL	https://<miq-appliance>/saml2
Assertion Consumer Service POST Binding URL	https://<miq-appliance>/saml2/postResponse
Logout Service Redirect Binding URL	https://<miq-appliance>/saml2/logout

7. Obtain the identity provider’s **idp-metadata.xml** metadata file as follows:

   ```
   # cd /etc/httpd/saml2
   # curl -s -o idp-metadata.xml \
     http://<redhatSSO-server>:8080/auth/realms/<miq-
   realm>/protocol/saml/descriptor
   ```

8. In CloudForms 4.1, the following change is necessary to the **idp-metadata.xml** file for SAML logout to work between **mod_auth_mellon** and Red Hat SSO:

```
# vi idp-metadata.xml

  ...
  <SingleLogoutService
<   Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
---
>   Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
    Location=
  ...
```

9. Restart the HTTP server on the appliance:

```
# systemctl restart httpd
```

Configuring the Appliance Administrative User Interface

After configuring the HTTP server for SAML, update the Red Hat CloudForms appliance so that the administrative user interface works with SAML authentication.

1. Login to the appliance as **`admin`**, and navigate to **Settings** → **Configuration** → **Authentication**.
2. Set the mode to **External (httpd)**.
3. Check **Enable SAML**. This enables the SAML login button on the appliance login screen, then redirects to the SAML protected page for authentication, and supports the SAML logout process.
4. Check **Enable Single Signon**. With this option enabled, initial access to the appliance's administrative user interface redirects to the SAML identity provider authentication screen. Logging out from the appliance returns the user to the appliance login screen, allowing them to log in as **`admin`** unless **Disable Local Login** is also checked.
5. Optional: Check **Disable Local Login** to disable the **`admin`** login to appliance and only allow SAML based authentication. Note that if there are issues with the identity provider or you require **`admin`** access to the appliance, you cannot log in through the appliance login screen until you re-enable local login as described in Section 4.1.4.2.9, "Configuring External Authentication Using SAML".
6. Check **Get User Groups from External Authentication (httpd)**
7. Click **Save**.

Important

Ensure the user’s groups are created on the appliance and appropriate roles are assigned to those groups. See *SAML Assertions* in Section 4.1.4.2.9, “Configuring External Authentication Using SAML” for more information on the parameters used by the Red Hat CloudForms appliance.

For example, to configure user groups from your SAML identity provider to work with Red Hat CloudForms:

1. In your SAML identity provider, specify your existing user groups in similar format to the following:
   `REMOTE_USER_GROUPS=Administrators;CloudAdministrators;Users`

2. On your Red Hat CloudForms appliance, create the equivalent groups. See *Creating a User Group* in Section 4.2.8, “Creating a User Group”.

3. On your Red Hat CloudForms appliance, assign EVM roles to the groups. See *Creating a Role* in Section 4.2.14, “Creating a Role”.

Complete the above steps on each appliance in **Settings** → **Configuration** → **Access Control**.

You can now log into your Red Hat CloudForms appliance using your SAML credentials.

SAML Assertions

To authenticate to the Red Hat CloudForms appliance using SAML, the following remote user parameters are looked at by the appliance upon a successful login and redirect from the identity provider. These parameters are used by the appliance to obtain group authentication information.

HTTP Environment	SAML Assertion
REMOTE_USER	username
REMOTE_USER_EMAIL	email
REMOTE_USER_FIRSTNAME	firstname
REMOTE_USER_LASTNAME	lastname
REMOTE_USER_FULLNAME	fullname
REMOTE_USER_GROUPS	groups

For Red Hat SSO, the above SAML assertions can be defined for the appliance client in Red Hat SSO as mappers.

Name	Category	Type	Property
username	AttributeStatement Mapper	User Property	username
email	AttributeStatement Mapper	User Property	email
firstname	AttributeStatement Mapper	User Property	firstName
lastname	AttributeStatement Mapper	User Property	lastName
fullname	AttributeStatement Mapper	User Attribute	fullName
groups	Group Mapper	Group List	groups

Important

The **`fullName`** attribute was not available in the default database as of this writing and was added as a user attribute.

Re-enabling Local Login (Optional)

If you disabled local login in the administrative user interface but need the ability to log in as **`admin`**, local login can be re-enabled using one of the following methods:

Re-enabling Local Login from the Appliance Administrative User Interface

This method requires the identity provider to be available, and the ability to login as a user with enough administrative privileges to update Red Hat CloudForms authentication settings.

1. Log in to the appliance user interface as the administrative user.
2. Navigate to **Settings** → **Configuration** → **Authentication**.
3. Uncheck **Disable Local Login**.
4. Click **Save**.

Re-enabling Local Login from the Appliance Console:

1. Use SSH to log into the appliance as **`root`**.

2. Run the **`appliance_console`** command.

3. Select **Update External Authentication Options**.

4. Select **Enable Local Login**.

5. Apply the updates.

Alternatively, log into the appliance as root using SSH, and run the following command:

```
# appliance_console_cli --extauth-opts local_login_disabled=false
```

4.1.4.3. Workers

Use the Workers page to specify the number of workers and amount of memory allowed to be used for each type.

Note

Only make these changes when directed to by Red Hat Support.

4.1.4.3.1. Changing Settings for a Worker

To change the settings for a worker (except replication worker)

1. Navigate to **Settings** → **Configuration**.

2. Click on the **Settings** accordion, then click **Zones**.

3. Click the zone where the server is located.

4. Click on the server.

5. Click **Workers**.

6. Go to the type of worker you have been directed to change.

7. If applicable, change Count or Memory Threshold using the dropdown boxes.

8. Click **Save**.

4.1.4.4. Database

Use the Database page to specify the location of your Virtual Machine Database (VMDB) and its login credentials. By default, the type is PostgreSQL on the Server.

Note

The server may not start if the database settings are changed. Be sure to validate your new settings before restarting the server.

4.1.4.4.1. Changing a Database Setting