Linux Console

The Linux Console is the text-based interface to a Linux system.

Contents

Moonshot-enabling the Linux Console requires the use of pam_gss, a PAM module that brings Moonshot compatibility to PAM. Unfortunately, pam_gss necessarily has to work in a way that is not generally recommended with Moonshot - the client device is not under the direct control of the user, and with pam_gss the device is both the client *and* the server. The consequence of this is that the user's credentials (NAI and password) are exposed directly to a device which is not the user's. Thus, this should only be deployed where the implications and the risk are fully understood:

- Deployers should understand that the credentials of users using the device could be exposed on that device.
- Users should understand that their credential could be exposed and should thus do it only on devices managed by organisations they trust.

Due to the severity of this problem, the Moonshot project does not officially distribute pam_gss packages. Members of the community have made them available, however. The instructions on this page walk you through configuring GNOME using this community-provided code, but again - **only do so if you understand the consequences.**

1. Overview

Moonshot-enabling the Linux console is achieved through the use of a PAM module.

2. Compatibility

2.1. Key

In the tables below, the following icons have the following meanings:

- ✓ - This version of the software has been tested and verified as supporting Moonshot.
- ✗ - This version of the software has been tested and verified as **not** supporting Moonshot.
- ? - This version of the software has not yet been tested thoroughly and its status is not known. Let us know if you have tried it and whether it worked or not!

2.2. Compatibility List

Any versions not listed below have not yet been tested. If you do so, please let us know!

OS version	Compatible?	Notes
CentOS 6	✓	
RHEL 6	✓	
Scientific Linux 6	✓	

3. Installation & Configuration

How you set up a Moonshot-enabled version of the Linux Console will differ depending on your OS. See the relevant pages for your particular distribution:

- CentOS 6
- RHEL 6
- Scientific Linux 6

4. Next Steps

4.1. Account Mapping

Read our General account mapping advice page before you go any further to get an overview of the general options available for mapping federation provided identities to local accounts.

Moonshot by default uses Shibboleth libraries to parse RADIUS and SAML attributes.

SAML assertions can be embedded inside RADIUS responses by the IdP, allowing an IdP to exercise a very fine-grained authorisation policy. One potential use of this is to allow the Moonshot IdP to specify which account the user should log in to your Linux console as. RADIUS attributes, such as the `User-Name` attribute, are simply mapped with a special type of Shibboleth attribute. To do this, enable the functionality in Shibboleth as follows.

Edit `/etc/shibboleth/shibboleth2.xml` and modify the lines after the opening `<SPConfig ... clockSkew="180">` stanza:

Shibboleth 2.x only

Insert these lines immediately after the opening stanza:

```
    <OutOfProcess tranLogFormat="%u|%s|%IDP|%i|%ac|%t|%attr|%n|%b|%E|%S|%SS|%L|%UA|%a">
        <Extensions>
                <Library path="plugins.so" fatal="true" />
        </Extensions>
    </OutOfProcess>
```

Shibboleth 3.x only

Modify the `OutOfProcess` stanza as follows:

```
    <OutOfProcess tranLogFormat="%u|%s|%IDP|%i|%ac|%t|%attr|%n|%b|%E|%S|%SS|%L|%UA|%a">
        <Extensions>
                <Library path="plugins.so" fatal="true" />
        </Extensions>
    </OutOfProcess>
```

4.1.1. Mapping to an account specified in a SAML attribute

To map an attribute in a SAML assertion embedded in a RADIUS response, your Linux console maps that to a local user account (via `local-login-user`) as follows:

1. Edit `/etc/shibboleth/attribute-map.xml` and find the SAML attribute that the Moonshot IdP will be sending you that contains the username.

   Example

   We want to map from the incoming SAML2 representation of "eduPersonEntitlement"

   ```
   <Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" id="entitlement"/>
   ```

2. Change the id of the attribute to "local-login-user".

Example

We change the attribute defining the SAML2 representation of "eduPersonEntitlement" such that its id becomes "local-login-user"

```
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7" id="local-login-user"/>
```

In the standard Moonshot distribution, SSH will look for local-login-user to determine who to authenticate the user as. This attribute mapping will be managed by the XML assertion in the FreeRADIUS reply for a successful authentication.

4.1.2. Further mapping options

To Come!

4.2. Logging into the Linux Console using Moonshot

The user experience of logging into the Linux Console is different to the usual experience when using moonshot (see the warning at the start of this page).

To do so, do the following:

1. At the Linux console login prompt, enter the full NAI of your username (e.g. johnsmith@example.com). Hit return.
2. A Password: prompt will show. Enter the password associated with the account. Hit return.
3. If successful, you should be logged into the Linux Console as the local user that your account is mapped to (see next section).

Ensure that the account that the user is being mapped to (via whatever method) actually exists beforehand!