Two factor authentication for SSH using PAM RADIUS module

sandbox-logintc.com/docs/connectors/ssh.html

Introduction

LoginTC makes it easy for administrators to add multi-factor to SSH on their Unix systems. This document shows how to configure SSH to require two factor authentication for remote access via Pluggable Authentication Module (PAM).

RADIUS Domain Creation

If you have already created a LoginTC Admin domain for your LoginTC RADIUS Connector, then you may skip this section and proceed to Installation.

1. Log in to LoginTC Admin
2. Click **Domains**:
3. Click **Add Domain**:

   
   Create Domain

4. Enter domain information:

   
   Create Domain Form

   Name
   Choose a name to identify your LoginTC Admin domain to you and your users

   Connector
   RADIUS

Installation

The LoginTC RADIUS Connector runs CentOS 6.8 with SELinux. A firewall runs with the following open ports:

Port	Protocol	Purpose
22	TCP	SSH access
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
8888	TCP	Web interface
443	TCP	Web interface

Port	Protocol	Purpose
80	TCP	Web interface
80	TCP	Package updates (outgoing)
123	UDP	NTP, Clock synchronization (outgoing)

Note: Username and Password

`logintc-user` is used for SSH and web access. The default password is `logintcradius`. You will be asked to change the default password on first boot of the appliance and will not be able to access the **web interface** unless it is changed.

The `logintc-user` has `sudo` privileges.

Configuration

Configuration describes how the appliance will authenticate your RADIUS-speaking device with an optional first factor and LoginTC as a second factor. Each configuration has **4 Sections**:

1. LoginTC

This section describes how the appliance itself authenticates against LoginTC Admin with your LoginTC organization and domain. Only users that are part of your organization and added to the domain configured will be able to authenticate.

2. First Factor

This section describes how the appliance will conduct an optional first factor. Either against an existing LDAP, Active Directory or RADIUS server. If no first factor is selected, then only LoginTC will be used for authentication (since there are 4-digit PIN and Passcode options that unlock the tokens to access your domains, LoginTC-only authentication this still provides two-factor authentication).

3. Passthrough

This section describes whether the appliance will perform a LoginTC challenge for an authenticating user. The default is to challenge all users. However with either a static list or Active Directory / LDAP Group you can control whom gets challenged to facilitate seamless testing and rollout.

4. Client and Encryption

This section describes which RADIUS-speaking device will be connecting to the appliance and whether to encrypt API Key, password and secret parameters.

Data Encryption

It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

The **web interface** makes setting up a configuration simple and straightforward. Each section has a **Test** feature, which validates each input value and reports all potential errors. Section specific validation simplifies troubleshooting and gets your infrastructure protected correctly faster.

First Configuration

Close the console and navigate to your appliance **web interface** URL. Use username `logintc-user` and the password you set upon initial launch of the appliance. You will now configure the LoginTC RADIUS Connector.

Create a new configuration file by clicking **+ Create your first configuration**:

Web Server

LoginTC Settings

Configure which LoginTC organization and domain to use:

Web Server

Configuration values:

Property	Explanation
`api_key`	The 64-character organization API key
`domain_id`	The 40-character domain ID

The API key is found on the LoginTC Admin Settings page. The Domain ID is found on your domain settings page.

Click **Test** to validate the values and then click **Next**:

Web Server

First Authentication Factor

Configure the first authentication factor to be used in conjunction with LoginTC. You may use Active Directory / LDAP or an existing RADIUS server. You may also opt not to use a first factor, in which case LoginTC will be the only authentication factor.

Web Server

Active Directory / LDAP Option

Select **Active Directory** if you have an AD Server. For all other LDAP-speaking directory services, such as OpenDJ or OpenLDAP, select **LDAP**:

Web Server

Configuration values:

Property	Explanation	Examples
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389` / `636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The password for the above bind_dn account	`password`
`base_dn`	The top-level DN that you wish to query from	`dc=example,dc=com`
`attr_username`	The attribute containing the user's username	`sAMAccountName` or `uid`
`attr_name`	The attribute containing the user's real name	`displayName` or `cn`
`attr_email`	The attribute containing the user's email address	`mail` or `email`
`Group Attribute` (optional)	Specify an additional user group attribute to be returned the authenticating server.	`4000`
`RADIUS Group Attribute` (optional)	Name of RADIUS attribute to send back	`Filter-Id`
`LDAP Group` (optional)	The name of the LDAP group to be sent back to the authenticating server.	`SSLVPN-Users`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

Click **Test** to validate the values and then click **Next**.

Existing RADIUS Server Option

If you want to use your existing RADIUS server, select **RADIUS**:

Web Server

Configuration values:

Property	Explanation	Examples
`host`	Host or IP address of the RADIUS server	`radius.example.com` or `192.168.1.43`
`port` (optional)	Port if the RADIUS server uses non-standard (i.e., `1812`)	`1812`

Property	Explanation	Examples
`secret`	The secret shared between the RADIUS server and the LoginTC RADIUS Connector	`testing123`

RADIUS Vendor-Specific Attributes

Common Vendor-Specific Attributes (VSAs) found in the FreeRADIUS dictionary files will be relayed.

Click **Test** to validate the values and then click **Next**.

Passthrough

Configure which users will be challenged with LoginTC. This allows you to control how LoginTC will be phased in for your users. This flexibility allows for seamless testing and roll out.

For example, with smaller or proof of concept deployments select the Static List option. Users on the static list will be challenged with LoginTC, while those not on the list will only be challenged with the configured First Authentication Factor. That means you will be able to test LoginTC without affecting existing users accessing your VPN.

For larger deployments you can elect to use the Active Directory or LDAP Group option. Only users part of a particular LDAP or Active Directory Group will be challenged with LoginTC. As your users are migrating to LoginTC your LDAP and Active Directory group policy will ensure that they will be challenged with LoginTC. Users not part of the group will only be challenged with the configured First Authentication Factor.

No Passthrough (default)

Select this option if you wish every user to be challenged with LoginTC.

Web Server

Static List

Select this option if you wish to have a static list of users that will be challenged with LoginTC. Good for small number of users.

Web Server

LoginTC challenge users: a new line separated list of usernames. For example:

```
jane.doe
jane.smith
john.doe
john.smith
```

Active Directory / LDAP Group

Select this option if you wish to have only users part of a particular Active Directory or LDAP group to be challenged with LoginTC. Good for medium and large number of users.

Web Server

Configuration values:

Property	Explanation	Examples
`LoginTC challenge auth groups`	Comma separated list of groups for which users will be challenged with LoginTC	`SSLVPN-Users` or `two-factor-users`
`host`	Host or IP address of the LDAP server	`ldap.example.com` or `192.168.1.42`
`port` (optional)	Port if LDAP server uses non-standard (i.e., `389` / `636`)	`4000`
`bind_dn`	DN of a user with read access to the directory	`cn=admin,dc=example,dc=com`
`bind_password`	The password for the above bind_dn account	`password`
`base_dn`	The top-level DN that you wish to query from	`dc=example,dc=com`
`attr_username`	The attribute containing the user's username	`sAMAccountName` or `uid`
`attr_name`	The attribute containing the user's real name	`displayName` or `cn`
`attr_email`	The attribute containing the user's email address	`mail` or `email`
`encryption` (optional)	Encryption mechanism	`ssl` or `startTLS`
`cacert` (optional)	CA certificate file (PEM format)	`/opt/logintc/cacert.pem`

Configuration Simplified

If Active Directory / LDAP Option was selected in First Authentication Factor the non-sensitive values will be pre-populated to avoid retyping and potential typos.

Click **Test** to validate the values and then click **Next**.

Client and Encryption

Configure RADIUS client (e.g. your RADIUS-speaking VPN):

Web Server

Client configuration values:

Property	Explanation	Examples
`name`	A unique identifier of your RADIUS client	`CorporateVPN`

Property	Explanation	Examples
`ip`	The IP address of your RADIUS client (e.g. your RADIUS-speaking VPN)	`192.168.1.44`
`secret`	The secret shared between the LoginTC RADIUS Connector and its client	`bigsecret`

Data Encryption

It is strongly recommended to enable encryption of all sensitive fields for both PCI compliance and as a general best practice.

Click **Test** to validate the values and then click **Save**.

Web Server

Testing

When you are ready to test your configuration, create a LoginTC user (if you haven't already done so). The username should match your existing user. Provision a token by following the steps:

When you have loaded a token for your new user and domain, navigate to your appliance**web interface** URL:

Web Server

Click **Test Configuration**:

Web Server

Enter a valid username and password; if there is no password leave it blank. A simulated authentication request will be sent to the mobile or desktop device with the user token loaded. Approve the request to continue:

Web Server

Congratulations! Your appliance can successfully broker first and second factor authentication. The only remaining step is to configure your RADIUS device!

If there was an error during testing, the following will appear:

Web Server

In this case, click **See logs** and then click the `/var/log/logintc/authenticate.log` tab to view the log file and troubleshoot:

Web Server

Install PAM RADIUS module

The PAM RADIUS module from FreeRADIUS allows the use of RADIUS to PAM authentication. It can be leverage for almost any service that supports PAM-based authentication. If your system does not have pam_radius_auth package installed you will need to do so. Below are instructions for CentOS. For more information on pam_radius_auth and installing it on your system please see: FreeRADIUS PAM Authentication and Accounting module.

Install PAM RADIUS on CentOS / RedHat

Step 1: Developer tools:

```
$ sudo yum install wget gcc pam pam-devel make -y
```

Step 2: Build PAM RADIUS module pre:

```
$ cd /tmp
$ sudo wget ftp://ftp.freeradius.org/pub/radius/pam_radius-1.4.0.tar.gz
$ sudo tar xvzf pam_radius-1.4.0.tar.gz
$ cd pam_radius-1.4.0
$ sudo ./configure
$ sudo make
```

Note: PAM RADIUS module version 1.4.0

At the time of this document being written **1.4.0** was the latest version of the PAM RADIUS module. For updates please see: FreeRADIUS PAM Authentication and Accounting module.

Step 3: Copy shared object library to appropriate folder

32-bit

```
$ sudo cp pam_radius_auth.so /lib/security/
```

64-bit

```
$ sudo cp pam_radius_auth.so /lib64/security/
```

The PAM RADIUS library is installed and ready to be configured.

Configure SSH

Step 1: Create or edit the `/etc/raddb/server` file to point to your LoginTC RADIUS Connector:

```
$ sudo mkdir -p /etc/raddb
$ sudo vi /etc/raddb/server
```

```
  # server[:port] shared_secret      timeout (s)
  # Example server (change to fit your needs):
  192.168.1.40    bigsecret          60
```

The `server` should match the IP Address of your LoginTC RADIUS Connector, while the `shared_secret` should match to one configured in the LoginTC RADIUS Connector. The corresponding settings are configured in Client and Encryption portion of the LoginTC RADIUS Connector.

Note: Timeout

We recommend the maximum timeout of 60 seconds allowed by the PAM RADIUS module.

Step 2: Edit `/etc/pam.d/sshd` :

```
$ sudo vi /etc/pam.d/sshd
```

Option 1: Use only LoginTC RADIUS Connector for authentication:

```
  #%PAM-1.0
  auth    required pam_sepermit.so
  auth       required     pam_radius_auth.so
  account    required     pam_nologin.so
  account    include      password-auth
  password   include      password-auth
  # pam_selinux.so close should be the first session rule
  session    required     pam_selinux.so close
  session    required     pam_loginuid.so
  # pam_selinux.so open should only be followed by sessions to be executed in the user
context
  session    required     pam_selinux.so open env_params
  session    required     pam_namespace.so
  session    optional     pam_keyinit.so force revoke
  session    include      password-auth
```

Option 2: Use local password authentication AND LoginTC RADIUS Connector for authentication:

```
  #%PAM-1.0
  auth    required pam_sepermit.so
  auth       required     pam_radius_auth.so skip_passwd
  auth       include      password-auth
  account    required     pam_nologin.so
  account    include      password-auth
  password   include      password-auth
  # pam_selinux.so close should be the first session rule
  session    required     pam_selinux.so close
  session    required     pam_loginuid.so
  # pam_selinux.so open should only be followed by sessions to be executed in the user
context
  session    required     pam_selinux.so open env_params
  session    required     pam_namespace.so
  session    optional     pam_keyinit.so force revoke
  session    include      password-auth
```

Option 2: Challenge Mode

First Factor Authentication should be set to **None**.

Web Server

Client Settings **Authentication Mode** should be set to **Challenge**.

Web Server

Challenge Message: `Press 1 to authenticate with LoginTC Push or enter an OTP or bypass code:`

Also ensure `/etc/ssh/sshd_config` has `ChallengeResponseAuthentication yes` set.

Step 4: Restart `sshd`:

```
$ sudo service sshd restart
```

You are now ready to test two-factor authentication with SSH.

Testing SSH

Test by accessing SSH. The username of the UNIX user must match the username of the user created in your organization and added to the domain you have configured to authenticate against.

```
$ ssh john.doe@192.168.0.30
```

You will be prompted for a password and then challenged with LoginTC.

Troubleshooting

PAM RADIUS Module

For troubleshooting related to the PAM RADIUS module please refer to: FreeRADIUS PAM Authentication and Accounting module.

Not Authenticating

If you are unable to authenticate, navigate to your appliance **web interface** URL and click **Status**:

Ensure that all the status checks pass. For additional troubleshooting, click **Logs**:

Also make sure to check the secure logs on the Linux machine hosting SSH (`/var/log/secure`).

Email Support

For any additional help please email support@cyphercor.com. Expect a speedy reply.