Technical Guide:

Canadian Access Federation Identity Provider (IdP) Installer

Software Version: 3.0.1

Revision Date: June 22, 2017

Technical Support: tickets@canarie.ca

canarie.ca | @canarie_inc

Table of Contents

1. Using This Guide

1.1. Preface

The Identity Provider (IdP) Installer is a tool to rapidly deploy services offered through the Canadian Access Federation (CAF), namely eduroam (federated RADIUS) and Federated Identity Management or FIM (SAML2). Both services connect to your existing authentication and access management environment, allowing users to login securely using their existing credentials.

The IdP Installer reduces the installation and configuration time for CAF services to a matter of minutes.

eduroam and FIM can be installed independently or together depending on a participant's needs. We recommend you build a test instance for your service(s) using IdP Installer before installing CAF services in a production environment.

1.2. Who Should Read This Guide

This guide is intended for person(s) responsible for the planning, preparation, installation and administration of CAF services at their institution.

1.3. Skill and Knowledge Expectation of Installation Personnel

Although the installation tools and process are intended to minimize the required depth of knowledge across all the required components, the following skills and knowledge would be helpful for planners and or installers:

1.3.1. Required Operational Institutional Knowledge

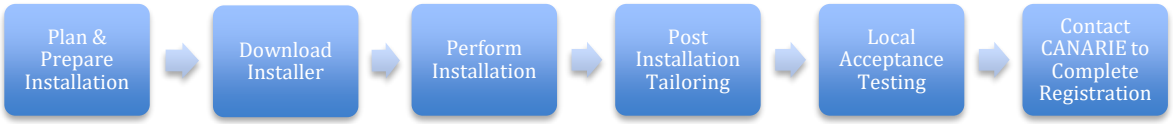
- Sign-on systems for wireless (for eduroam installs)
- Web-based sign-on (for FIM installs)
- Testing or change control practices
- Service and deployment management strategy
- Active Directory and/or LDAP infrastructure
- Firewall configuration, management, and/or ability to request updates

1.3.2. Recommended Skills and Technology Familiarity

- Web sign-on strategies and techniques
- Ability to navigate, configure and manage within a Linux operating system (start/stop services, reboot, review logs, edit files etc.)
- Web application structures and their design (HTML and applications creating dynamic HTML)

2. Installation Overview

The following steps will be followed in order to successfully complete installation, configuration and verification of CAF services to a test and/or production environment as depicted in Figure 1 below.



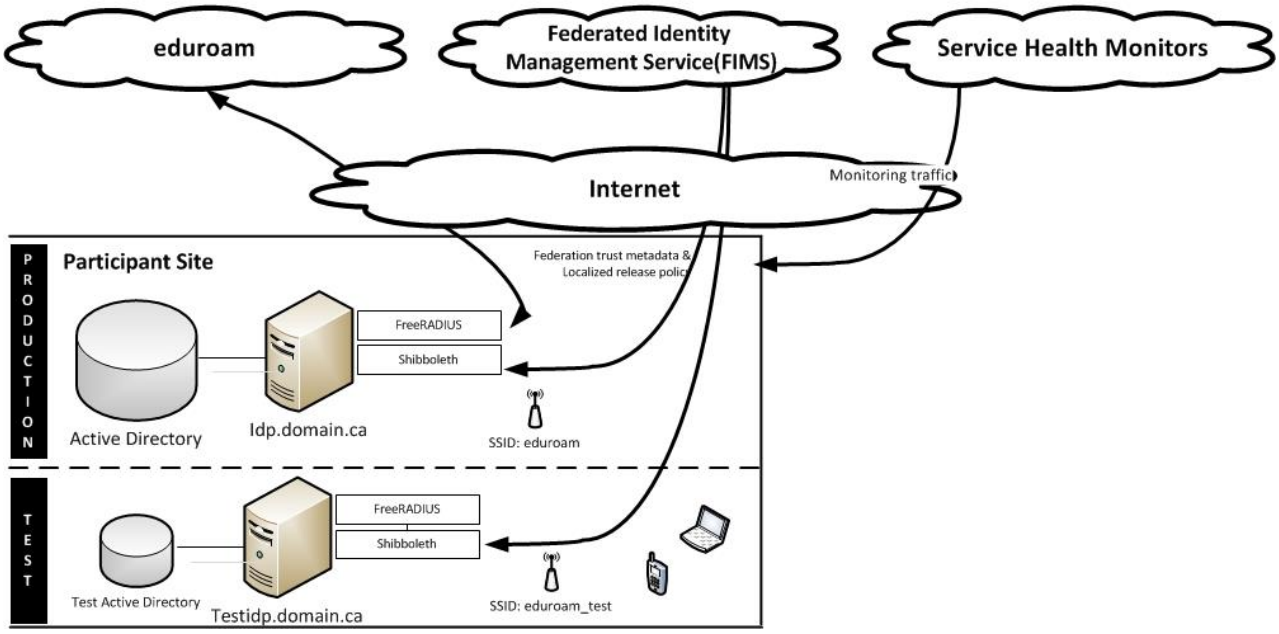


Figure 1. Typical Site Deployment with Test and Production Servers

3. Planning Your Installation

3.1. System Requirements

Both eduroam and FIM services can be installed on either the same server or separate servers (recommended) using the same IdP Installer tool. The physical requirements for an eduroam or FIM server are the same for simplicity.

3.1.1. Server OS

The IdP Server OS can be one of:

- CentOS 6.5 'or higher'
- CentOS 7.2 'or higher'
- Ubuntu 14.04 LTS
- RedHat 7.2
- Debian 8.3

3.1.2. Physical or Virtual Servers

We strongly recommend that virtualization technology be used to host the CAF services. Virtualization technology has many benefits that can be leveraged, such as the ability to perform system snapshots, clone instances, and execute full VM backups while the instance remains in service.

3.1.3. IPv4 and IPv6 Support

CAF services are operationally intended to be available over IPv4 end-to-end.

IPv6 support is available in certain portions of CAF infrastructure, but is not operationally available end-to-end and is not yet a required element.

3.1.4. Resource Requirements

Whether the installation is a pre-production (test) or production installation, the following are the recommendations for server/VM resources:

Resource	Amount
System Memory	Minimum 6 Gb RAM
System Total Swap (/tmp)	12 Gb
System Disk with 1 Partition (/)	20 Gb

3.2. Preparing Your Network

See the table below for the IP addresses and ports associated with the CAF services for both eduroam and FIM that you will be connecting your site IdP server to. CANARIE operates additional monitoring and operational tools for CAF services that participants are encouraged to use and permit access to CANARIE on the listed ports below. The list of IPs, protocols and ports below should be made accessible through provisioning of your site firewall rules.

Location	DNS CNAME	IPv4 Address	IPv6 Address	CAF Participant Site Ports Required	Ports Accepted by This Host
Kelowna BC	prod1-west.eduroam.ca	128.189.5.5		icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Vancouver BC	Prod2-west.eduroam.ca	142.231.112.1		icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Ottawa, ON	prod1-east.eduroam.ca	205.189.33.100	2001:410:102:1::100	icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Ottawa, ON	prod2-east.eduroam.ca	205.189.33.101	2001:410:102:1::101	icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Ottawa, ON	monitor.canarie.ca	205.189.33.55	2001:410:102:1::55	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	UDP: 1812, 1813
Ottawa, ON	amidala.canarie.ca	205.189.33.75	2001:410:102:1::75	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	UDP: 1812, 1813
Ottawa, ON	tools.canarie.ca	205.189.33.111	2001:410:102:1::111	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	TCP: 443, 80
Ottawa, ON	logger.canarie.ca	205.189.33.23	2001:410:102:1::23	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443	UDP: 514, TCP: 514
Toronto, ON	caf-shib2ops.ca	128.100.132.106			UDP:ping TCP: 443, 80

Table 1: CAF Operational Server IP Addresses and Ports

Service	Transport/Port	Visibility
eduroam	UDP/1812,1813	Your network, CANARIE Federations servers
FIM	TCP/443	Your Network, the internet
SSH	TCP/22	Administrative use on your network only
Mysql	TCP/3306	Localhost and standby host if advanced model used

Table 2: Key Ports for Your IdP

3.3. Preparing Your Environment

3.3.1. Connecting to Your Directory Service

The IdP Installer requires directory connectivity for:

- the validation of userid and passwords
- the ability to retrieve and populate attributes as needed

The IdP Installer can connect to Microsoft Active Directory or any directory presenting an LDAP v3 compliant interface. The IdP Installer will perform runtime adjustments for specific fields used to authenticate and find users in the directory.

3.3.2. Service Specific Limitations on Directories

3.3.2.1. For eduroam

Sites are strongly encouraged to support the MS-CHAPv2 protocol for eduroam RADIUS. For MS-CHAPv2 to work, the IdP host MUST use an Active Directory instance as the LDAP server and be joined to the AD domain via the command line in order for MS-CHAPv2 password validation to function.

Alternatives exist with other LDAP directories but require advanced configuration. This advanced configuration requires manual adjustments after the IdP Installer has completed its run.

3.3.2.2. For FIM

FIM has no limitations on which directory to connect to but does require a TLS connection over port 636 for a secure communications channel.

If your directory is not able to offer TLS over port 636 you may elect to install stunnel[1] to create a secure connection for the IdP Installer.

3.3.2.3. Test Directories

Non-production (or test) environments are strongly recommended as a proving ground for CAF services setup and configuration. Non-production environments should be completely isolated from production systems.

3.3.3. Transport Layer Security (TLS) Certificates

TLS certificates play a large role in protecting information in transit in both eduroam and FIM.

[1] https://www.stunnel.org

The default behaviour of the Installer is to use self-signed certificates and in the case of eduroam, a Certificate Authority (CA) will be automatically created based on the information collected by the IdP Installer.

3.3.3.1. Certificates that End Users will Experience

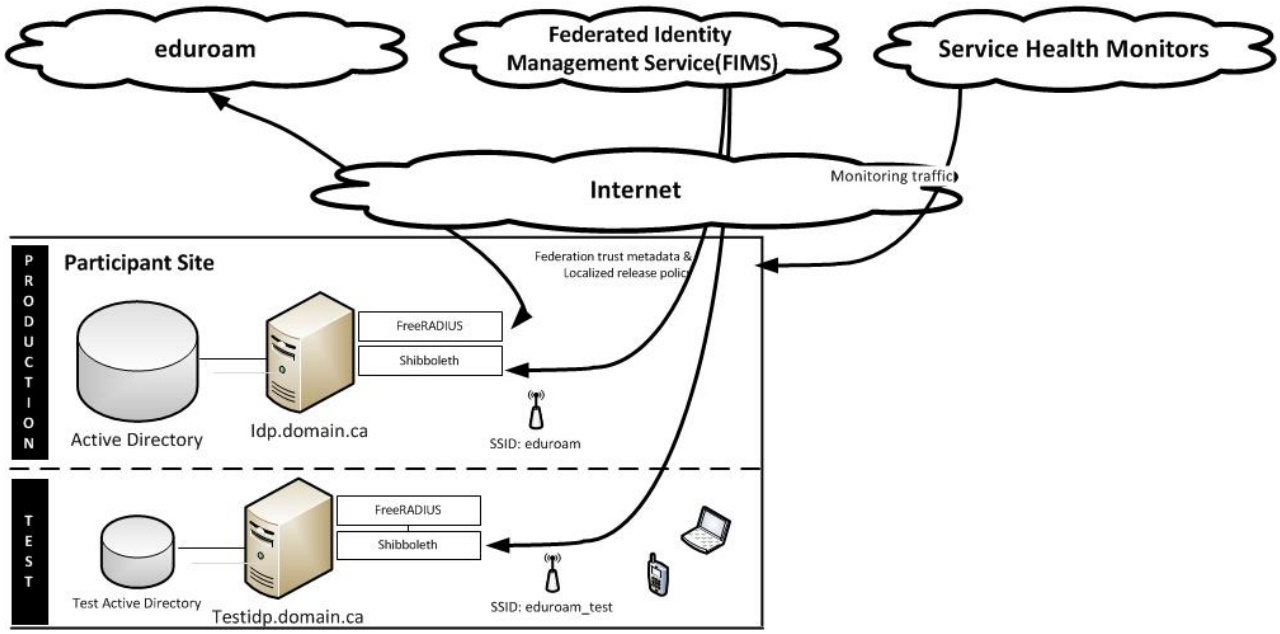
For eduroam, the certificate that FreeRADIUS employs is one that the end user must accept as proof that the RADIUS authentication server is truly that server. This certificate will be presented to a mobile device once, when configuring Wi-Fi on the device using the eduroam SSID.

3.3.3.2. Other Certificates

FIM uses the Shibboleth software that in turn creates a long-lived (10 years) certificate that is self-signed and used in the SAML2 metadata. This certificate should not be changed or modified.

3.4. Deployment Approaches

3.4.1. Recommended Deployment Approach



The recommended deployment approach can serve organizations with a medium set of users (i.e. 10-20,000 FTEs) and services and can be easily configured to have two production servers: one active and one standby, in addition to the test server that is representational of the production environment.

The test server should be installed first to exercise the build process for your production environment. Working through the deployment on the test server will highlight additional deployment steps and customizations of the environment when the production server is installed.

3.4.2. Advanced Deployment Approaches

Advanced deployments are typically driven by these main drivers:

- Business continuity needs (fault tolerance and failover)
- High availability (HA) needs
- Special feature needs

When working through an advanced deployment, it is important to consider the business continuity needs and adjustments that would be required over and above the recommended deployment.

It is recommended you leverage the IdP Installer's existing deployment approach and then apply the additional settings to the environment in order to achieve your desired outcome.

This will minimize the amount of manual manipulation of an IdP installation and can be automated to some degree.

3.4.2.1. FIM High Availability Configurations

It is not uncommon to see production installations having two IdP instances in production. One active, one standby with the same configuration shared between them but not clustered. IdP clustering[2] is not necessary if it is sufficient to have a new IdP takeover activity while one is being worked on, but it does provide an enhanced level of HA.

If IdP clustering is desired, it is recommended to be configured post installation using IdP Installer.

3.4.2.2. FIM Special Feature Configurations

The FIM (Shibboleth) Server is deployed along with a way to cache persistent identifiers for services. If there is a service that requires a special identifier that you must transmit in order to use that service (e.g. Office365 UniqueId or a special SAML2 persistent NameID), you need to decide how that value is created and managed. The IdP's database can store such attributes which can be retrieved locally by the IdP. A high availability configuration must take this into consideration with the attribute data being present in all instances of the database. More details about advanced topics can be found at:

https://collaboration.canarie.ca/elgg/file/view/3164/idp-task-cheat-sheet

3.5. Availability and Reliability Considerations

A number of factors should be considered as you plan for your deployment. The default out-of-the-box behaviour of the IDP Installer is to install a base as a test server. As you plan taking this base installation to production, some things to consider in your deployment are:

[2] https://wiki.shibboleth.net/confluence/display/IDP30/Clustering

3.5.1. Aspects of Reliability in the Services

Different strategies exist to increase the reliability of a service and usually involve a load balancer to manage a pool of servers.

An alternative ad-hoc method is to identify an IP address that floats between servers and have a heartbeat process to monitor server health. If the service is up initially but suddenly goes down (detected by the heartbeat process), you can switch over to the standby server. It is possible to use this method with the services installed using the IdP Installer, but it is up to the technician to install and reliably configure them.

Use of multiple DNS entries and round robin techniques has not proven to increase reliability and is therefore not recommended.

3.5.1.1. eduroam Reliability Aspects

eduroam uses the RADIUS protocol, which is a stateless protocol. It uses UDP over ports 1812 and 1813 as network transport and is designed with the ability to work with failover servers. The IdP Installer only installs a single instance of FreeRADIUS directed to a pool of upstream Federation Lever RADIUS servers (FLRs) for Canada.

Clients that communicate with the locally deployed FreeRADIUS server do so by DNS lookup. Clients are defined as smartphones, laptops, access points, and other RADIUS servers.

3.5.1.2. FIM Reliability Aspects

FIM uses the Shibboleth software to implement the SAML protocol, which travels over a secure channel (HTTPS port 443). Shibboleth authentication and the population of attributes in the assertion response do not require statefulness. In a single request, the end user's browser handles the delivery of the authentication assertion to the service provider in the SAML2 assertion over HTTPS. Subsequent visits to a FIM IdP will link you to the in-memory record of your session. If the session is terminated, the user is forced to re-authenticate again. Managing the session across more than one server is an advanced option in Shibboleth and is not supported by the IdP Installer at this time.

If the Shibboleth server is restarted all user sessions are lost. The impact is not a service outage but triggers the user to authenticate once again to re-create their session.

3.5.1.3. FIM and eduPersonTargetedID and persistentID

The Shibboleth server uses a MySQL database as a local cache to store the calculated eduPersonTargetedID[3] and persistentID values used in the SAML2 NameID identifier.

If a load-balanced model of two production servers is used in an active-standby strategy, the MySQL database may be replicated to the standby server.

[3] http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html#eduPersonTargetedID

4. Installation Procedure

4.1. How the Installer Works

Using the IdP Installer has three key parts:

- A Configuration Builder that runs on the user's desktop (HTML form that generates the configuration file)
- An installer process that runs on the IdP server, reading the configuration file and updating and doing the necessary customizations based on the configuration
- Post-installation steps to tailor the installation for advanced/custom configuration

All components are bundled in the Installer ZIP file and should be copied to both the user's desktop and the target IdP server. The Installer ZIP file can be retrieved from:

http://bit.ly/idpinstaller300zip

4.2. Assumptions for the Installation Process to be Successful

- The user performing the installation will use either Firefox, Google Chrome, or Safari on their desktop to open the Configuration Builder (URL) locally on their machine
- Server(s) are provisioned with appropriate resource levels (see 3.1.4)
- Necessary network configurations are complete (see 3.2)
- A deployment approach and target configuration have been chosen (see Error! Reference source not found.)

4.3. Building your configuration

Open the Configuration Builder in your browser by opening the URL:

file:///<location_of_unzipped_installer>/idp-installer-CAF/www/appconfig/CAF/index.html

Once you have answered all the questions on the form, click on 'Generate Configuration File'.

Additional information about the key configuration elements are embedded in the Configuration Builder. You may require the assistance of your Active Directory admin or firewall admin for some answers to the questions.

4.3.1. Loading a Pre-existing Configuration

In order to quickly re-build or replicate one of your IdP Server instances, you can import a previously saved configuration. This will save you the time of manually entering fields on the form presented in the Configuration Builder. To do this, click on 'Import an Existing Configuration' in the top right of the Configuration Builder, cut and paste contents from your existing configuration file into the text area presented on the page, and click 'Import My Existing Config From Below'.

4.4. Deployment on the IdP Server

On the target IdP Server, sign on as a root and perform these steps in order:

1) Ensure your host has accurate DNS and network configurations in /etc/resolv.conf and /etc/hosts
2) Copy the idp-installer-<version>.zip to a temp directory (i.e. /tmp) on the IdP server
3) If required, install the "unzip" utility with either 'yum -y install unzip' or 'apt-get –y install unzip' depending on your server OS
4) cd /tmp
5) unzip idp-installer-<version>.zip
6) cd into the idp-installer-<version> sub-directory
7) copy or cut-and-paste your configuration (created in Section 4.3), by editing the file 'config' and then saving it
8) run the script ./deploy_idp.sh as root
9) perform any post installation steps

5. Post Installation Steps

5.1. eduroam-Specific Post Installation

5.1.1. Testing the Default eduroam Installation (local site)

By connecting the RADIUS instance to your access point or controller, you can test the default installation using a client (smartphone or laptop) to authenticate to the SSID you have configured.

The wireless access point configuration can be quite detailed but minimally WPA2, 802.1x authentication would point to this RADIUS instance.

The chosen test client will then need to submit a userid of 'some_id@yourdomain.ca' and the appropriate password.

Windows clients may require additional configuration to trust the certificate (self-signed) and likely the certificate authority as well.

The ability to validate or test eduroam transit from end-to-end is not possible until your production server is connected to the top level Federation Level RADIUS servers.

5.1.2. Starting and Stopping the eduroam Service

The freeRADIUS service uses the standard start/stop methodology in Linux and should be configured to automatically start on server reboot.

Manually starting the service: *service radiusd start*

Manually stopping the service: *service radiusd stop*

Note: In order to start/stop the service, you must be logged into the server as "root"

5.1.3. Replacing Auto-generated Self-signed Certificate (Optional)

The IdP Installer auto-generates TLS certificates from the freeRADIUS cert bootstrap process. If you wish to update/replace the certificate with a commercial one you will need to:

- Sign into the machine as root
- cd /etc/raddb/certs
- Choose to generate a new Certificate Signing Request (CSR) or use the existing one
    - Ensure the extended key usage aspects of the TLS certificate are present for RADIUS usage
- Replace server.crt with the relevant certificate
- Restart the freeRADIUS service by entering 'service radius restart'

5.2. FIM Specific Post Installation

5.2.1. Testing the Default FIM Installation

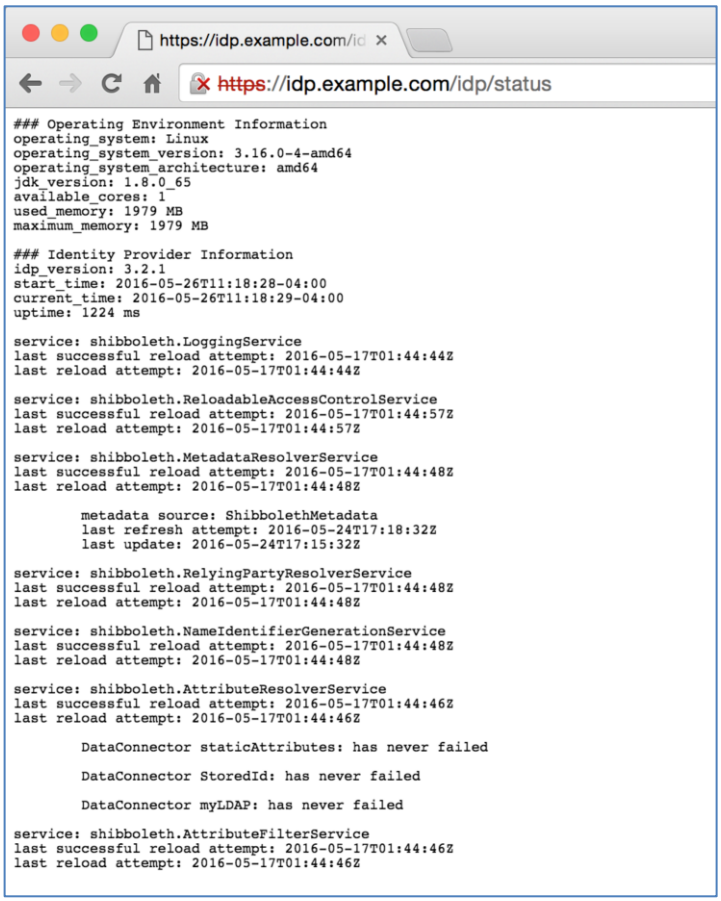
A very simple test is to invoke the URL of:

https://<yourserverFQDN>/idp/status

which, when all is in order, should render the status of the server.

This simple test validates that:

- the web server and certificate are operational and properly configured
- IPTables is doing the proper thing
- there are no syntactical errors in the configuration
- the directory connection works for the attribute resolver
- the directory connection for authentication works (they use the same credentials, but different configuration locations)



5.2.2. Optional Additional Testing

5.2.2.1. Testing Using testshib.org

The public test service called testshib.org operates a simple open IdP and SP that you can test against for end-to-end testing on your own. To test, uncomment the relevant section in metadata-providers.xml and restart your IdP and follow the instructions on the testshib.org site.

5.2.2.2. Testing with CAF Test Federation

CAF has a test federation that CAF participants can use. This test federation has its own discovery service and a test service provider that can be used to test your IdP installation. To join the test federation, send a request to tickets@canarie.ca and include your metadata if it has not already been sent.

5.2.3. Starting and Stopping the FIM Service

The FIM service uses Tomcat as its container to run in, the standard start/stop methodology, and should automatically start on server reboot.

Manually starting the service: */etc/init.d/jetty start*

Manually stopping the service: */etc/init.d/jetty stop*

Note: In order to start/stop the service, you must be logged into the server as "root"

5.2.4. Replacing Webserver Certificate with a Commercial Certificate (Optional)

The IdP Installer auto-generates TLS certificates from openSSL for the Shibboleth software for:

- The Java Key Store (JKS) for the Tomcat webserver
- The JKS for the Shibboleth software

The Tomcat webserver CSR is the only certificate needing replacement if it is to transition from self-signed to a commercial certificate.

A regular CSR may be generated and if both eduroam and FIM are used, the SAME CSR could be used as the host will be the same name.

For more details please see our FAQ:

https://tts.canarie.ca/otrs/public.pl?Action=PublicFAQZoom;ItemID=83

5.2.5. Customizing the Login Page for FIM / Shibboleth

The IdP Installer uses Shibboleth out-of-the-box for the FIM service and does not tailor the login page to reflect the look and feel of the organization. For details about how to customize the look and feel, please see these two references:

- CAF-specific:
  - https://tts.canarie.ca/otrs/public.pl?Action=PublicFAQZoom;ItemID=79
- Full reference from Shibboleth Consortium:

- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAuthUserPassLoginPage

5.3. Backup and Change Management Practices

The IDP Installer is designed to be able to re-use configuration files it generates, which allows for rapid rebuilding of the environment. However, it is not intended as a substitute for backups or retaining logging or debugging data that may have been generated by the use of the services. Rebuilding of a service will erase historical logs and any customizations. To this end, regular backups of server instances and on-demand snapshots are recommended.

It is strongly recommended that some form of change management practices are applied to these services and align with your IT department polices. It is also recommended you document any site-specific customizations performed during installation.

5.4. Connecting your FIM or eduroam Server to CAF Production

Once you have fully completed verifying your installation, please contact CANARIE at tickets@canarie.ca indicating that you are ready to connect your site to the CAF FIM. This should be done by your authorized CAF technical contact (identified in the application to join CAF).

For eduroam, you need to supply the IP address(es) of your server(s) and CANARIE in return will provide you with a "shared secret" used for secure connectivity between sites.

To connect your Shibboleth IdP to CAF FIM you need to supply the following information (attached in your email to tickets@canarie.ca):

- Your entityid
  - usually 'https://idp.yourschoolname.ca/idp'
- The name of your organization or institution
- The display name for your organization
  - This will be how your institution is seen in pick lists for discovery purposes
- A short description of your organization
- A URL for the logo of your organization
  - URL should be served via SSL, usually from your IdP itself
  - image size should be 100x100 pixels
- The domain for which you are authoritative
  - this will be your official scope in CAF metadata
- Your entity metadata url to retrieve your metadata
  - https://your_server.ca/idp/shibboleth will be presumed otherwise
    - this URL retrieves the file in /opt/shibboleth/idp/metadata/idp-metadata.xml
- Appropriate contact information for:
  - one role-based help desk account with
    - a phone number
    - an email
  - one or more personal technical contacts with
    - a phone number
    - an email

6. Appendix

6.1. Installed Software and Related Directories

Software installed specifically by the IdP Installer is listed below. Many packages have dependencies automatically installed so this list is not exhaustive of all the discrete Linux packages installed. Using RPM (or similar utility) prior to installation, it is possible to count the packages and then compare the list after installation.

- FIM-Related:
    - jetty
        - **Installed by:** download of the package
        - **Install dir:** /opt/jetty
        - **Log dir:** /opt/jetty/jetty-base/
    - shibboleth-identityprovider-3.2.1
        - **Installed by:** extracting tar of package
        - **Install dir:** /opt/shibboleth/idp
        - **Log dir:** /opt/shibboleth-idp/logs
    - cas-client-3.3.3-release
        - **Installed by:** extracting tar of package plugin to Tomcat
        - **Install dir:** /opt/cas-client-3.3.3
        - **Log dir:**
    - mysql-connector-java-5.1.35 (for EPTID and persistentID)
        - **Installed by:** IdP Installer extracting it from its zip file
        - **Install dir:** /opt/shibboleth-idp/edit-webapp/WEB-INF/lib/
        - **Log dir:** n/a
    - MySQL Community Service 5.6 (for EPTID and persistentID)
        - **Installed by:** extracting tar of package
        - **Install dir:** /usr/sbin
        - **Log dir:**/var/log/mysql/
- eduroam-Related:
    - freeRADIUS-2.1.12
        - **Installed by:** rpm installation of package
        - **Install dir:** /usr/sbin, /etc/raddb
        - **Log dir:** /var/log/radiusd
    - samba-3.6.9 (to connect to AD for MS-CHAPv2)
        - **Installed by:** rpm install of package
        - **Install dir:** /usr/bin, /etc/samba/
        - **Log dir:** /var/log/syslog