

CAF IdP Installer Guide

CANARIE Inc.

Canadian Access Federation

SOFTWARE VERSION: 3.0.0	REVISION DATE: June 6,2016
---------------------------------------	--

Table of Contents

1. USING THIS GUIDE	3
1.1. PREFACE	3
1.2. WHO SHOULD READ THIS GUIDE	3
1.3. SKILL AND KNOWLEDGE EXPECTATION OF INSTALLATION PERSONNEL	3
1.3.1. <i>Required Operational Institutional Knowledge</i>	3
1.3.2. <i>Recommended Skills and Technology Familiarity</i>	3
2. INSTALLATION OVERVIEW	4
3. PLANNING YOUR INSTALLATION	5
3.1. SYSTEM REQUIREMENTS	5
3.1.1. <i>Appliance OS</i>	5
3.1.2. <i>Physical or Virtual Infrastructure</i>	5
3.1.3. <i>IPv4 and IPv6 Support</i>	5
3.1.4. <i>Resource Requirements</i>	6
3.2. PREPARING YOUR NETWORK	7
Table 1: CAF Operational Server IP Addresses and Ports	7
3.3. PREPARING YOUR ENVIRONMENT	8
3.3.1. <i>About Which Directory to Connect to</i>	8
3.3.2.3. <i>Regarding Test Directories</i>	8
3.3.3. ABOUT TRANSPORT LAYER SECURITY (TLS) CERTIFICATES	9
3.3.3.1. <i>Certificates that end users will experience</i>	9
3.3.3.2. <i>Other Certificates</i>	9
3.4. DEPLOYMENT APPROACHES	10
4. INSTALLATION PROCEDURE	12
4.1. HOW THE INSTALLER WORKS	12
4.2. ASSUMPTIONS FOR THE INSTALLATION PROCESS TO BEGIN	12
4.3. BUILDING YOUR CONFIGURATION	12
4.3.1. <i>Loading a Pre-existing Configuration</i>	12
4.4. DOING YOUR DEPLOYMENT	13
5. AVAILABILITY CONSIDERATIONS	13
5.1. CHANGE MANAGEMENT PRACTICES	13
5.1.1. <i>Aspects of Reliability in the Services</i>	13
6. POST INSTALLATION STEPS	16
6.1. <i>Eduroam Specific Post Installation</i>	16
6.1.1. <i>Testing the default eduroam installation</i>	16
6.1.2. <i>Starting and Stopping the service</i>	16
6.1.3. <i>Replacing Auto-generated Self-signed Certificate</i>	16
6.2. <i>FedSSO Specific Post Installation</i>	17
6.2.1. <i>Testing the default FedSSO installation</i>	17
6.2.2. <i>Optional additional testing options</i>	17
6.2.2.1. <i>Testing using testshib.org</i>	17
6.2.2.2. <i>Testing using CAF test federation</i>	17
6.2.3. <i>Starting and Stopping the service</i>	18
6.2.4. <i>Replacing HTTPS webserver certificate with a commercial certificate</i>	18

6.2.5.	Customizing the login page for FedSSO / Shibboleth	18
6.3.	CONNECTING YOUR FEDSSO OR EDUROAM SERVER TO CAF PRODUCTION	19
7.	APPENDIX	20
7.1.	GLOSSARY	20
7.2.	REFERENCES	20
7.3.	INSTALLED SOFTWARE AND RELATED DIRECTORIES	21

1. Using This Guide

1.1. Preface

The Identity Provider (IdP) Installer is a tool to rapidly deploy services for federated RADIUS (eduroam) and SAML2 for Federated Single Sign On (FedSSO), both of which connect to your existing authentication and access management environment to enable your users to use their credentials safely and securely in these contexts.

The IdP Installer reduces the installation and configuration time to a matter of minutes for a test instance of the CAF services and then serve as the base for installing the production CAF services.

eduroam and FedSSO can be installed independently or together depending on a participant's needs.

This document is organized into sections; overview, planning, installation steps, and availability considerations. Section 4 contains the installation steps to perform the install.

1.2. Who Should Read This Guide

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

It may be the case that the person installing may not be the same person planning the deployment and that the updates to other pieces such as the firewall or accounts needed for directory connectivity are performed by others.

1.3. Skill and knowledge Expectation of Installation Personnel

The installation process is intended to minimize the required depth of knowledge across all the components to perform the installation. The following skills and knowledge base would be helpful for planners and or installers.

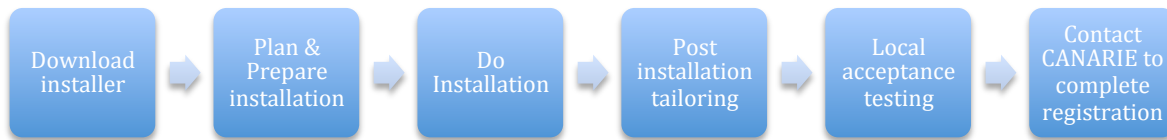
1.3.1. Required Operational Institutional Knowledge

- Sign on systems for wireless (for eduroam installs)
- Web based sign on (for fedSSO 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 a CentOS Linux operating systems
 - (start/stop services, reboot, review logs, edit files etc)
- Web Application structures and their design
- HTML and applications creating dynamic HTML.

2. Installation Overview



2.1. Download Installer

- a. From <http://bit.ly/caftools>

2.2. Plan & Prepare your installation

- b. Review System Requirements to prepare your environment.
- c. Prepare your network
- d. Prepare your environment (settings for Directory, Certificates, etc)
- e. Review and choose a preferred deployment approach
- f. Review your federation specific post install steps

2.3. Do the installation

- a. Create a configuration from your federations' configuration builder
- b. Save configuration as 'config' in this directory on your server
- c. Run the script `./deploy_idp.sh`
- d. Answer any inline questions (use self signed cert? password creation for keystores)

2.4. Perform Post installation Tailoring

- a. Based on items previously identified, finalize the installation
- b. Identity steps needed to be repeated in production

2.5. Locally Test Installation

2.6. Repeat installation steps for production installation as needed

3. Planning Your Installation

3.1. System Requirements

While both eduroam and federated SSO services can be installed on the same server using the same IdP-Installer tool, sites usually choose to use the IdP-Installer to install a single service on a single server. The requirements for the server be it eduroam or federated SSO are the same for simplicity.

eduroam uses the RADIUS protocol, which supports attribute exchange but is rarely used beyond the network UID, domain of origin, and related transactional information such as MAC address or Calling Station ID. The RADIUS server is almost exclusively connected to by other servers in your infrastructure.

Federated SSO uses the SAML2 protocol, where attribute exchange is the main benefit of the service and is used for the majority of time web authentication and has the capability of supporting non web authentication via the SAML2 ECP (Enhanced Client Proxy) profile.

3.1.1. Appliance OS

The appliance OS can be one of:

- CentOS 6.5 'minimal'
- CentOS 7.2 'minimal'
- Ubuntu 14.04 LTS
- RedHat 7.2
- Debian 8.3

3.1.2. Physical or Virtual Infrastructure

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 do system snapshots, cloning of instances, and full vm backups while the instance is operating.

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 development or production installation, the following are the recommendations for virtual resources. Some of the reasons behind the recommendations are:

- Consistency between test and production configuration is best to more accurately diagnose production from a test instance.
- The resourcing is designed for scaling the service to production levels for a campuses with good adoption of services.
- Instances exclusively for the purpose of functional testing can use a less resources but will not accurately reflect any load performance tests resourced as such.

Resource	Amount
System Memory	Minimum 6Gb physical
System total swap (/tmp)	12Gb
System disk with 1 partition (/)	20Gb

3.2. Preparing Your Network

See the table below for the IP addresses and ports associated with the Canadian Access Federation services for both eduroam and Federated SSO. CANARIE operates additional monitoring and operational tools for CAF services that participants are encouraged to participate with and permit their installation be reachable by CANARIE on the listed ports.

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, 80, 22	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, 80	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, 80	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, 80	UDP: 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
FedSSO	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. About Which Directory to Connect to

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 both Microsoft Active Directory and any directory presenting an LDAP v3 compliant interface. The IdP-Installer will perform runtime adjustments for specific fields to use 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 regular LDAP directories but is an advanced configuration. This advanced configuration would require adjustments after the IdP-Installer has completed it's run and is an advanced configuration.

3.3.2.2. For Federated SSO

Federated SSO has no limitations on which directory to connect to but does require a TLS connection over port 636 to ensure the communications channel is secure.

If your directory is not able to offer TLS over port 636 you may elect to install stunnel¹ to create a secure endpoint connection available to the IdP-Installer.

3.3.2.3. Regarding Test Directories

Test systems should connect to test directories wherever possible.

Test directories MUST not be connected to production IdPs. This would mean that the test identities are being used as if they were production and 'real' and is an inaccurate representation of an institutions data.

Test systems connecting to production directories may occur but realize that test systems are not necessarily bound by the same practices and rules as production systems. Take this into consideration in pre-production testing, which identities and functions you desire to test, and scope of testing.

¹ <https://www.stunnel.org/>

3.3.3. About Transport Layer Security (TLS) Certificates

TLS Certificates play a large role in protecting information in transit in both eduroam and FedSSO.

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 in the installer.

3.3.3.1. Certificates that end users will experience

- **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 seen on any mobile device, but only once, at the time of association to the eduroam SSID and rarely again.
- **FedSSO**
 - The certificate that is seen on a HTTPS website, usually a commercial issued certificate

3.3.3.2. Other Certificates

FedSSO 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

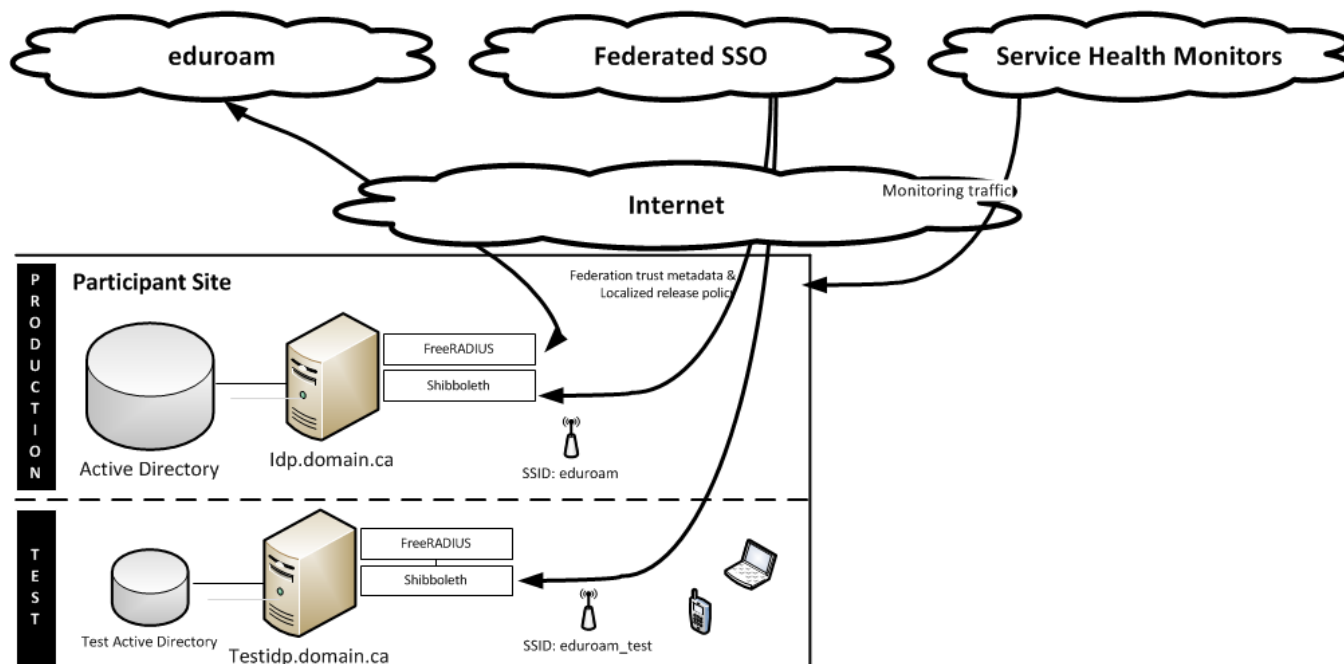


Figure 1. A typical site deployment with a test server and production server

The recommended deployment approach can serve organizations with a medium set of users and services and can be easily configured to have two production servers, one active, 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

More advanced deployments than the recommended type have these main drivers:

- Business continuity needs
- Availability needs
- Special feature needs

When working through an advanced deployment, it is recommended to capture the business continuity needs as inputs to adjustments to the recommended deployment.

As well, it is recommended to leverage the IdP-Installers existing deployment approach and then apply the additional settings/tailoring to the environment to achieve your outcome.

This approach minimizes the amount of hand manipulation of an IdP installation and can be automated to some degree.

3.4.2.1. About Federated SSO 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 clustering² is not necessary if it is sufficient to have a new IdP take over activity while one is being worked on. One trades simplicity for complexity if this is experience is not tolerable. The negative experience that may present itself during a change of servers is that users on their next sign on or activity requiring session verification will be challenged to log in again.

If this experience is not satisfactory, and cannot be mitigated with change control and service windows to manage updates then clustering is recommended to be configured post installation.

3.4.2.2. About Federated SSO Special Feature Configurations

The Fed SSO Shibboleth server is deployed along with a way to database and cache persistent identifiers for services. If there is a service that requires a special identifier that you must transmit to use the service (e.g. Office365 Uniqueld or a special SAML2 persistent NameID) it is recommended to review how that value is created and managed overall. The IdP's database can be a repository to such an attribute and then be retrieved locally by the IdP. In turn, a high availability configuration must take this into consideration and the data be 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>

² <https://wiki.shibboleth.net/confluence/display/IDP30/Clustering>

4. Installation Procedure

4.1. How the installer works

Using the IdP installer has three key parts:

- A configuration file builder that runs on the technicians desktop that is a dynamic HTML form that generates the configuration file
- An installer process that runs on the actual server ingesting the configuration and updating and doing the necessary customizations based on the configuration.
- Post installation steps to tailor the installation to your needs

All components are in the installer zip file and should be on both the technician's desktop and the server being installed. The installation can be retrieved from:

<http://bit.ly/caftools>

4.2. Assumptions for the installation process to begin

- The technician doing the installation will use either Firefox, Google chrome, or safari on their desktop to open the configuration building URL locally on their machine.
- Host(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 3.4.1)

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 interview questions, click 'Generate Configuration File' which will ensure the config file generation is up to date.

Additional help information about the key 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 the top right of the installation builder click 'import an existing configuration' and cut and paste it into the text area presented to you and then click 'Import My Existing Config From Below'.

4.4. Doing your deployment

On the server being worked on, sign on as a root and perform these steps:

- Ensure your host has accurate DNS and network configurations in `/etc/resolv.conf` and `/etc/hosts`
- Copy the `idp-installer-<version>` zip to the host
- update the host to install unzip with either `'yum -y install unzip'` or `'apt-get -y install unzip'` depending on your platform.
- `unzip idp-installer-<version> .zip`
- `cd` into the `idp-installer-<version>` directory
- copy or cut-and-paste your configuration from the HTML form into the file `'config'` and save and exit
- run the script `./deploy_idp.sh` as root
- answer any inline questions
- perform any post installation steps

5. Availability Considerations

A number of factors should be considered as you craft your deployment. The default behaviour of the IDP installer out of the box 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:

5.1. Change Management Practices

It is strongly recommended that some form of change management practices are applied to these services and mesh with the practices at the installation site. It is also recommended to capture and document any site-specific customizations as you perform the installation.

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, nightly backups of server instances and on demand snapshots are recommended.

5.1.1. Aspects of Reliability in the Services

eduroam and FedSSO services require different protocols each with their own operational aspects which may influence the deployment approach to be chosen and depend on whether or not a site has one or both services installed

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 is able to float between servers and have a heartbeat process check. If the IP address is up initially, and if it isn't

after a period of time, bring up a new IP address. It is possible to use this method with the services installed by 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..

5.1.1.1. 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 deal 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.

The RADIUS protocol does not require state retention between discrete connections to RADIUS. If the address presented to a client has one or more service instances behind it, the transaction will be processed regardless of which server it communicated with initially.

5.1.1.2. FedSSO Reliability Aspects

FedSSO uses the Shibboleth software to implement the SAML protocol, which travels over HTTPS TCP 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 FedSSO IdP 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 but is not supported by the IdP Installer at this time.

If the Shibboleth server is restarted, the impact is not an outage but triggers the end user to re-authenticate again once to re-create their session.

5.1.1.3. FedSSO and eduPersonTargetedID and persistentID

The Shibboleth server uses a local MySQL database as a local cache to store the calculated eduPersonTargetedID³ and persistentID values used in the SAML2 NameID identifier. eduPersonTargetedID is a pseudo-anonymous privacy preserving identifier that is calculated for each user per Service Provider. CANARIE's CAF requires it to be release as a default attribute given that it does not reveal any personally identifiable information.

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. More on this topic may be found in the advanced section of this document.

Table 3. Summary of service reliability aspects vis-a-vis load balancing

Service	Load balancer possible approaches	Service statelessness	DNS resolution practice for service
Eduroam RADIUS (FreeRADIUS)	Active-Active, Active-Standy	RADIUS is stateless	Only at startup. Do not rely on DNS entries to abstract or provide fault tolerance of other network elements.
FedSSO SAML (Shibboleth)	Active-Standy, Active-Active possible, but not by the IdP Installer	Authentication transactions and attribute resolution, can be stateless. Persistence of SSO session 'in memory' record on server, no.	Only at startup. Do not rely on DNS entries to abstract or provide fault tolerance of other network elements

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

6. Post Installation Steps

6.1. Eduroam Specific Post Installation

6.1.1. Testing the default eduroam installation

Connecting the RADIUS configuration to your access point or controller can test the default installation by 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 it would be WPA2, 802.1x authentication and points 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 either trust the certificate (self-signed) and likely the certificate authority as well.

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

6.1.2. Starting and Stopping the service

The freeRADIUS service use the standard start/stop methodology and should automatically start on server reboot.

Manually starting the service: *service radiusd start*

Manually stopping the service: *service radiusd stop*

6.1.3. Replacing Auto-generated Self-signed Certificate

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

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

6.2. FedSSO Specific Post Installation

6.2.1. Testing the default FedSSO installation

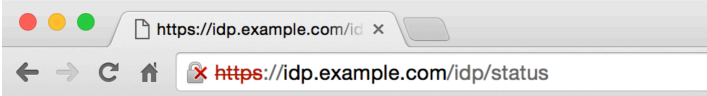
A very simple test is to invoke the URL of:

<https://<yourserversFQDN>/idp/status>

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

This simple test validates that:

- That the web server and certificate are operational and properly configured
- That IPTables is doing the proper thing.
- That 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)



```
### Operating Environment Information
operating_system: Linux
operating_system_version: 3.16.0-4-amd64
operating_system_architecture: amd64
jdk_version: 1.8.0_65
available_cores: 1
used_memory: 1979 MB
maximum_memory: 1979 MB

### Identity Provider Information
idp_version: 3.2.1
start_time: 2016-05-26T11:18:28-04:00
current_time: 2016-05-26T11:18:29-04:00
uptime: 1224 ms

service: shibboleth.LoggingService
last_successful_reload_attempt: 2016-05-17T01:44:44Z
last_reload_attempt: 2016-05-17T01:44:44Z

service: shibboleth.ReloadableAccessControlService
last_successful_reload_attempt: 2016-05-17T01:44:57Z
last_reload_attempt: 2016-05-17T01:44:57Z

service: shibboleth.MetadataResolverService
last_successful_reload_attempt: 2016-05-17T01:44:48Z
last_reload_attempt: 2016-05-17T01:44:48Z

    metadata_source: ShibbolethMetadata
    last_refresh_attempt: 2016-05-24T17:18:32Z
    last_update: 2016-05-24T17:15:32Z

service: shibboleth.RelyingPartyResolverService
last_successful_reload_attempt: 2016-05-17T01:44:48Z
last_reload_attempt: 2016-05-17T01:44:48Z

service: shibboleth.NameIdentifierGenerationService
last_successful_reload_attempt: 2016-05-17T01:44:48Z
last_reload_attempt: 2016-05-17T01:44:48Z

service: shibboleth.AttributeResolverService
last_successful_reload_attempt: 2016-05-17T01:44:46Z
last_reload_attempt: 2016-05-17T01:44:46Z

    DataConnector staticAttributes: has never failed
    DataConnector StoredId: has never failed
    DataConnector myLDAP: has never failed

service: shibboleth.AttributeFilterService
last_successful_reload_attempt: 2016-05-17T01:44:46Z
last_reload_attempt: 2016-05-17T01:44:46Z
```

6.2.2. Optional additional testing options

6.2.2.1. Testing using testshib.org

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

6.2.2.2. Testing using CAF test federation

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

6.2.3. Starting and Stopping the service

The Shibboleth service uses tomcat as it's 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`

6.2.4. Replacing HTTPS webserver certificate with a commercial certificate

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 replacing if it is to transition from self-signed to a commercial certificate.

A regular CSR may be generated and if both eduroam and FedSSO 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>

6.2.5. Customizing the login page for FedSSO / Shibboleth

The IdP Installer uses Shibboleth out of the box and does not tailoring of the login page to reflect the look and feel of the installing 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>

6.3. Connecting your FedSSO or eduroam server to CAF Production

Once you have done your testing of the installation to your satisfaction, please contact CANARIE at tickets@canarie.ca. This should be done by your authorized CAF technical contact. This contact is usually provided to CANARIE when your organization joins.

For eduroam we will need the IP address(es) of your server(s) and will provide the shared secret to you for connection.

To connect your Shibboleth IdP to CAF FedSSO we need the following information to accompany your email to tickets@canarie.ca:

- Your **entityid**
 - usually 'https://idp.yourschoolname.ca/idp'
- The **name** your organizations is a member of CAF as
- 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 your 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 a role based help desk account with
 - a phone number
 - an email
 - one or more personal technical contacts with
 - a phone number
 - an email.

7. Appendix

7.1. Glossary

Terms and acronyms to interpret this document properly:

SLA	Service Level Agreement
PII	Personally Identifiable Information
SAML	Security Authentication Markup Language
ADFS2	Active Directory Federation Services

7.2. References

Item.	Document Title	Date	Author
SAML	Security & Authentication Markup Language https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security		OASIS
OpenID	OpenID specification http://openid.net/specs/openid-authentication-2_0.html		IETF
OAuth2	OAuth2 specification (DRAFT) http://tools.ietf.org/html/draft-ietf-oauth-v2-31		IETF
WS-Federation	Web Services Federation Specification http://en.wikipedia.org/wiki/WS-Federation		OASIS
ADFS2	Active Directory Federation Services 2 http://technet.microsoft.com/en-us/library/adfs2(v=ws.10).aspx		Microsoft
SAML-EC	SAML Enhanced Client http://datatracker.ietf.org/doc/draft-ietf-kitten-sasl-saml-ec/		
RADSEC	Protocol for carrying RADIUS datagrams over TCP http://en.wikipedia.org/wiki/RadSec		IETF

7.3. 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 CentOS packages installed. Using RPM prior to installation it is possible to enumerate the packages and then compare the list after installation.

- SAML2 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 it's zip file
 - **Install dir:** /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