Installation Guide

CANARIE Inc.

Canadian Access Federation

Identity Appliance Installer

SOFTWARE VERSION:	REVISION DATE:
1.0.x	Jan 8,2014

Table of Contents

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 is a tool to reduce 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 participants needs.

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.

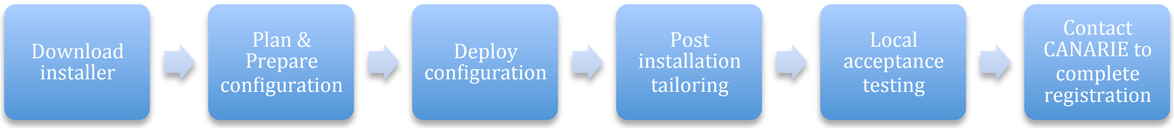
1.3.1. Required Operational Institutional Knowledge

- 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 and 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


Download installer
Plan & Prepare configuration
Deploy configuration
Post installation tailoring
Local acceptance testing
Contact CANARIE to complete registration

2.1. Plan your installation

a. Review System Requirements to prepare your environment.
b. Review and choose a preferred deployment approach
c. Determine your deployment type
d. Prepare your deployment hardware
e. Prepare your network
f. Review your federation specific post install steps

2.2. 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 (self signed cert? password creation for keystores?)

2.3. Perform post installation steps

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

2.4. Repeat installation steps for production installation as needed

3. Planning Your Installation

3.1. System Requirements

These are the minimum requires needed for each server.

3.1.1. Appliance OS

The appliance OS should be CentOS ‘minimal’ 6.4, x86_64 (64bit)

URL to fetch the ISO from:

http://isoredirect.centos.org/centos/6/isos/x86_64/

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.

These items are presumed to be addressed by the technician doing the installation.

3.1.3. Resource Requirements

Whether the installation is a development or production installation, the following are the recommendations for virtual resources.

Resource	Amount
System Memory	Minimum 6gb physical
System total swap (/tmp)	12gb
System disk with 1 partition (/)	20gb
CPU	Min 2x2ghz CPU

3.1.4. 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.

3.1.4.1. Backup and Recovery Point Snapshots

The role of the server and change management practices usually guide the necessity of backups and Snapshots. A dev server may not necessarily need the same treatment as a production server due to different availability requirements.

- Nightly backups of server instances are recommended .
- On demand snapshots depending on the magnitude of change.

3.1.5. 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.

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

4. Deployment Approach

The recommended deployment approach is to have a minimum of two servers at your site, one production and one test server that mirrors the production configuration as best possible.

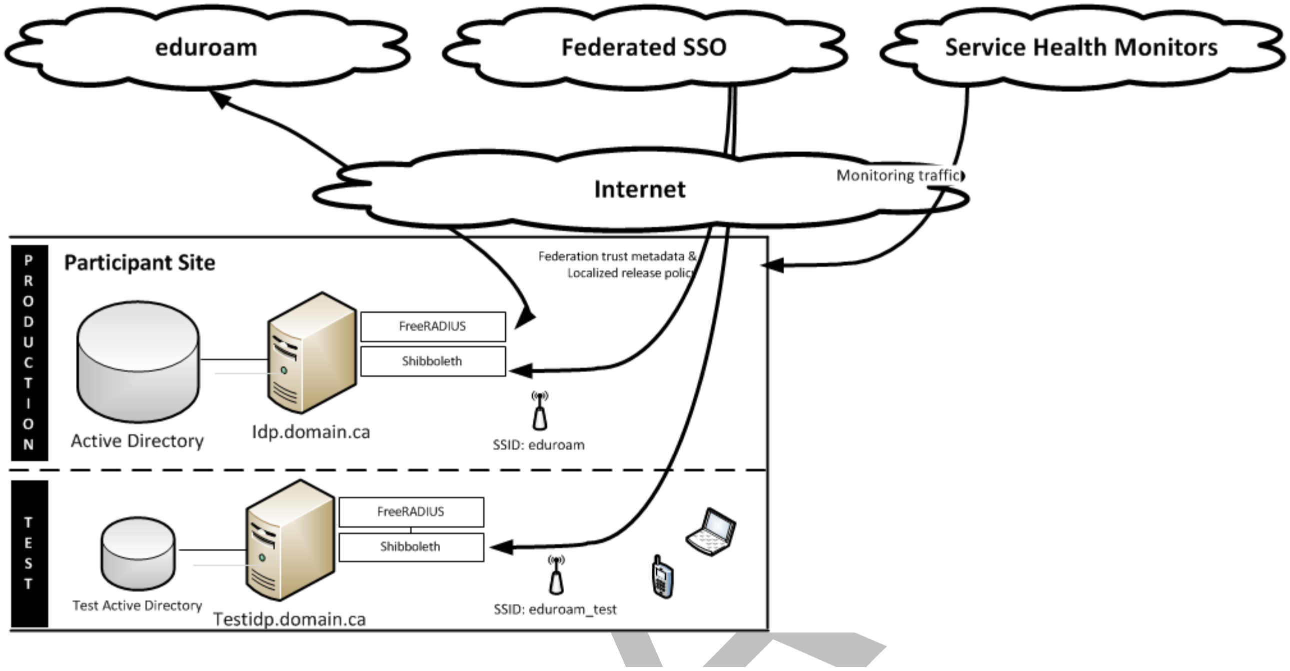


Figure 1. A typical site deployment with a test server and production server

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.

Going forward, maintaining the test server is useful to use to diagnose issues as well as to exercise any tests you would like to perform for the initial deployment and future changes to production.

3.1. Deployment Factors to Consider

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

3.1.1. The infrastructure in which the services are hosted

Section 2's requirements allow the installer to defer a number of things that used to be managed on a system by system basis. With a simple practice of taking a snapshot of the entire server prior to changes can serve as a safety net and tool to manage how to roll back services.

3.1.2. Your availability profile requirement

Availability of services has a number of influencing factors that have been taken into consideration:

3.1.2.1. Infrastructure Reliability

Reliability of the infrastructure is improved and options to respond to an issue are broader when the installer is used in a virtualized environment. This is discussed in requirements section 2.1.2 and assumed to be in place and available as a way to manage backups, snapshots, and time to recovery.Needs

3.1.2.2. 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.

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

An alternative ad-hoc method is to identify a IP address that is able to float between servers and have a heart-beat process check if the IP address is up, and if it isn't after a period of time, bring up a new IP address. This method is possible to be used with the services installed by the IdP Installer but is up to the technician to install and reliably configure.

Having multiple entries in DNS and expect it to round robin has been empirically found to be unsatisfactory to improve reliability and is not recommended to be used.

3.1.2.2.1. Specific eduroam aspects of Reliability

eduroam uses the RADIUS protocol which is a stateless protocol. It uses UDP over ports 1812 and 1813 as network transport and has a designed in ability to deal with failover servers, usually used upstream or to reflect a pool of servers for a particular function. The IdP Installer only installs a single instance of FreeRADIUS with 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.

. This means that a whether the address presented to a client has one or more service instances behind it, the transaction will be processed regardless of which server was communicated with before.

3.1.2.2.1.1. Summary for eduroam RADIUS service

Loadbalancer friendly: Yes. Active-Active, and Active-Standby

Stateless: Yes

DNS resolution practice: Only at startup. Do not rely on DNS entries to abstract or provide fault tolerance of other network elements.

3.1.2.2.2. FedSSO Aspects of Reliability

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. It is a single request and the end users browser handles the delivery of the authentication assertion to the service provider in the SAML2 assertion over HTTPS. However, subsequent visits to FedSSO IdP link you to the in memory record of your session, otherwise you are 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.

Databased eduPersonTargetedID

The Shibboleth server uses a local MySQL database to store the calculated eduPersonTargetedID[1] value. eduPersonTargetedID is a pseudoAnonymous 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 loadbalanced model of 2 production servers are used in an active-standby strategy, the MySQL database MUST be replicated to the standby server otherwise eduPersonTargetedIDs will be created when they should and the database will become divergent. More on this topic may be found in the advanced section of this document.

[1] https://www.internet2.edu/media/medialibrary/2013/09/04/internet2-mace-dir-eduperson-201203.html#eduPersonTargetedID

3.1.2.2.2.1. Summary for FedSSO RADIUS service

Loadbalancer friendly: Yes. Active-Standby, Active-Active is possible but not configured by the IdP Installer.

Stateless: Authentication transactions and attribute resolution, yes. Persistence of SSO session 'in memory' record on server, no.

DNS resolution practice: Only at startup. Do not rely on DNS entries to abstract or provide fault tolerance of other network elements.

3.1.3. Recommended Deployment Approaches

Size of organization, magnitude of use of the service, and services deployed drive the style of deployment approach along with the items described in section 3.1.2. All deployment approaches rely on virtualization for backup, snapshots, and recovery.

- **Default deployment for an IdP operating one or both eduroam and FedSSO**
    - A test server is deployed and used as a testbed.
- **Usual deployment approach for IdP operating one or both eduroam and FedSSO**
    - A test server deployed and used to validate configuration for production
    - a single production instance operating eduroam and FedSSO
- **Redundant eduroam deployment for multiple eduroam instances.**
    - A test server deployed and used to validate configuration for production
    - Multiple identically configured production instances with only hostnames and IP addresess changing
    - Optionally a loadbalancer abstracting away IP addreses if more than 2 servers
- **Advanced Active-Standby deployment approach for IdP operating only FedSSO**
    - A test server deployed and used to validate configuration for production
    - Multiple identically configured production IdP instances with
        - hostnames and IP addresess changing
    - site specific creation of a MySQL replication agreement between active and standby instances of the IdP.
    - Change management practices to migrate changes to both prod servers.

5. Preparing Your Network

The table on the following page summarizes the IP addresses and ports associated with the Canadian Federation Level RADIUS servers (FLRs) for eduroam, FedSSO, as well as monitoring and operational tools for CAF services. CAF services are operationally available over IPv4 end to end. IPv6 support is available in certain portions of the CAF infrastructure, but not operationally available end to end. IPv6 is not yet a required element.

Table 1: CAF Operational Server IP Addresses and Ports

Status	Location	DNS CNAME	IPv4 Address	IPv6 Address	Eduroam Site Ports	Ports accepted by this host
Legacy - being decommissioned Jan 30, 2014	Vancouver BC	moose.bc.net	128.189.4.1		icmp ping, UDP & TCP 1812, 1813, 2083	UDP: 1812, 1813
New	Kelowna BC	prod1-west.eduroam.ca	128.189.5.5		icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
Legacy remaining active	Vancouver BC	prod2-west.eduroam.ca (new name) grizzly.bc.net (old name)	142.231.112.1		icmp ping, UDP & TCP 1812, 1813, 2083, 3799	UDP: 1812, 1813
New	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
New	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
CAF Monitoring host 1	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
CAF Monitoring bastion host 1	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
CAF Monitoring fallback bastion host	Ottawa, ON	tools.canarie.ca	205.189.33.67	2001:410:102:1::67	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443, 80	TCP: 443, 80
CAF FedOps	Ottawa, ON	cafmgr-dev.canarie.ca	205.189.33.69	2001:410:102:1::69	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443, 80	TCP: 443, 80
CAF FedOps	Ottawa, ON	cafmgr.canarie.ca	205.189.33.68	2001:410:102:1::68	icmp, ping, UDP & TCP: 1812, 1813, 2083, 3799, TCP: 443, 80	TCP: 443, 80
CAF Logging	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

80

5.1. Host specific network configuration

The actual hosts comes with IPTables Note that IPtables firewall is enabled and customized on the CentOS installation of the IdP.

Nuances to port 443 for non root webserver

In order to have a non root installation of the tomcat webserver, IPTables performs portforwarding of port 443 to a tomcat localhost port (7443). This allows for a non root tomcat installation according to recommended install practices[2]

5.2. Important Host Specific Ports and Their Network Visibility

Service	Transport/Port	Visiblity
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

6. About Which Directory to Connect to

The IdP Installer requires directory to connect to for validation of userid and passwords and also to retrieve and populate attributes where needed.

Eduroam uses the RADIUS protocol which does support 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.

[2] https://wiki.shibboleth.net/confluence/display/SHIB2/IdPLinuxNonRoot

FedSSO uses the SAML2 protocol which is where the attribute exchange is the main benefit of the service.

1.1. What Directory is Needed for Which Service?

The IdP Installer is intended be to connect to Microsoft Active Directory as the directory of choice when both eduroam and FedSSO servers are deployed.

If FedSSO is being installed by itself, it is possible to use an alternative LDAP directory and is considered an advanced configuration.

AD as a requirement is to support MS-CHAPv2 protocol for eduroam RADIUS. For MS-CHAPv2 to work, the IdP host MUST be joined to the domain via the command line in order for MS-CHAPv2 password validation to function. The IdP Installer prompts you when this occurs

1.2. Test Directories

Test systems should test 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, who you desire to test, and to what scope.

7. 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.

7.1. Certificates that end users will experience

- **Eduroam**
  - The certificate that FreeRADIUS uses 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

7.2. Other Certificates

FedSSO uses the Shibboleth software which 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.

8. Installation Process

8.1. Assumptions for the installation process to begin

- The technician doing the installation has a desktop and is using either firefox or google chrome to build the installation configuration file
- Host(s) have been provisioned with appropriate resource levels
- Necessary network configurations have been done
- A deployment approach and target configuration has been chosen

8.2. How the installer works

The IdP installer has two 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.

All components are in the installer zip file and should be on both the technician's desktop and the server being installed.

8.3. Building your configuration

Open the configuration builder in your browser by opening the URL:

file:///<location_of_unzipped_installer>/ida-deployer/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.

8.3.1. 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’

8.4. Doing your deployment

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

- Copy the idp-installer zip to the host
- update the host to install unzip with ‘yum -y install unzip’
- unzip idp-installater.zip
- cd ida-deployer
- 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
- answer any inline questions
- perform any post installation steps

9. Post Installation Steps

Common Post installation Steps

Eduroam Specific Post Installation

FedSSO Specific Post Installation

10. Advanced Configurations

Eduroam

SAML

12. Appendix

9. 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

10. Installed Software

Software installed specifically by the IdP Installer is listed below. Many packages have dependencies automatically installed so this list is not exchaustive of all the discrete CentOS packages installed. Using RPM prior to installation it is possible to enumerate the packges and then compare the list after installation.

- SAML2 Related:
  - tomcat6
  - shibboleth-identityprovider-2.4.0
  - cas-client-3.2.1-release
  - mysql-connector-java-5.1.27 (for EPTID)
  - apache-maven-3.1.1 (for building FTICKS plugin)

- eduroam Related:
  - freeRADIUS-2.1.12
  - samba-3.6.9 (to connect to AD for MS-CHAPv2)