IdP Strategy - IdP-Installer Appliance Installation

Description

The IDP-Installer component is a lightweight tool to install both a Shibboleth 2.4 IdP and/or eduroam capable FreeRADIUS installation preconfigured for a given federation.
The design is modular and capable to be tailored for multiple federations of which Sweden's SWAMID and Canada's Canadian Access Federation have builds. It is multi-lingual and available to be tailored by anyone from github.

The process of installing the components is straightforward; an interview process via a bundled local webpage in the installer helps create and manage a configuration file used for input to the installer, the act of doing the installation with said configuration, and some post configuration steps.
The installer out of the box creates a ready dev or test environment in a few minutes and uses self signed certificates and a default installation.

The intent is to provide a rapid test environment and more importantly, a base configuration such that a production installation is a repeatable process with little effort using the configuration file approach.

Fact Finder

Chris Phillips, Technical Architect, Canadian Access Federation

Example Deployments

The IdP-installer has been used by more than 6 institutions in Canada to install their test environment as well as their production environment.
The IdP-Installer home

Support for the Recommended Technical Basics for IdPs, including the ability to consume metadata

Supported configurations are documented in the bundled documents (single hosts, active-standby production configurations etc) of the installer. It is pre-configured for Canadian Access Federation Metadata.

Support for Attribute Release

Shibboleth can be configured to release any attributes supported by the IdMS. The Shibboleth instance is expected to be pointed at Active Directory. Attribute filter policies are set on the IdP to release attribute values and done so in a privacy-preserving way.

Support for Entity Attributes/categories (e.g., R&S)

The IdP software supports the release of entity attribute bundles in fixed or dynamic subsets to all SPs or R&S SPs.The benefit of supporting attribute bundles is the decreased administrative overhead. An attribute is configured for the entity category.

Support for Multiple Authentication Contexts for Multi-Factor Authentication and Assurance

Identity assurance. The Multi-Context Broker, an extension to the Shibboleth IdP, supports multiple assurance profiles.

https://spaces.at.internet2.edu/display/InCAssurance/Multi-Context+Broker

Support for ECP (Enhanced Client or Proxy)

ECP is a SAML authentication profile for non-browser clients. There is a Java client which is a wrapper around the Apache HTTPClient that provides Shibboleth support.

https://github.com/reckart/shib-http-client

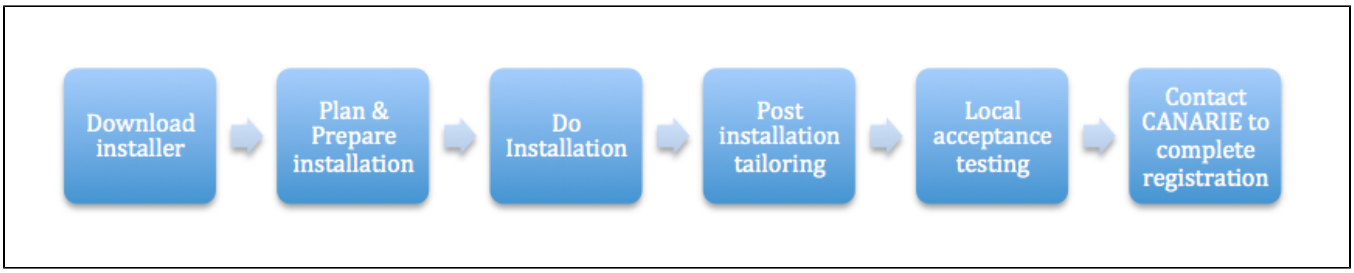
Support for User Consent

User attribute release consent. Technology exists via an extension for Shibboleth IdPs, uApprove, to implement attribute release consent. It also handles Terms of Use.
https://www.switch.ch/aai/support/tools/uApprove.html

User Consent in the IdP-Installer is not enabled by default.

Expertise Required

The IdP-installer is designed to reduce the required expertise to that of a general system administrator.
General knowledge of federation architecture is beneficial but is not required to commence the installation.
Many of the configuration decisions and barriers to implementation are reduced or eliminated via pre-configurations specific to the baseline federation operations and the Q&A interview style process at the beginning of the installation process.



The above is the usual process for using the IdP-Installer with the Canadian Access Federation operated by CANARIE.

Resources Required

The VM with 8gb of memory, 20gb disk, 2 CPUs is sufficient for a small to medium-sized production machine.See Latest IdP-Installer Documentation
The IdP-Installer can also be easily installed in a local virtual box image as described here https://collaboration.canarie.ca/elgg/file/view/1666/configuration-guide-to-setting-up-virtualbox-for-the-idp-installer

Upkeep and Feeding Required

Maintaining an IdP requires keeping up on security patches and advisories for the underlying resources as well as keeping current on the IdP software itself.
The IdP-Installer does not perform 'upgrades' as there is a significant amount of bespoke configuration post installation (specifically around the IdP WAR actually for login page customization etc). The upgrade path is to repeat the configuration in a VM from a base installation and re-configure from there.
It is up to the IdP operator to decide what is a major change that would require a fresh install (which only takes a few minutes) vs a minor change such as attribute release which edits can happen on the existing installation.

Applicable Environments

Shibboleth is highly adaptable to arbitrary environments.
The IdP-Installer also supports the inclusion of an eduroam ready FreeRADIUS server pre-configured for Canadian Access Federation use.

Pros / Benefits

This component has exactly the same benefits as the Shibboleth software selection, but is pre-configured for operation with default metadata settings, directory settings abstracted into a Q&A interview process the installation personnel go through to pre-flight check the installation.
This approach allows for more rapid IdP installation measured in days (for some, minutes) rather than weeks.
By designing for an out of box dev experience, the installer encourages a practice to have a test environment as well as a production environment for those who may not have these practices in place already.

Cons / Risks

The IdP-installer is available in a 'global' configuration and configurations for Canada (CAF) and Sweden (SWAMID), but none are available for inCommon.

While not difficult, no 'lead' or champion in the US space has voiced interest to craft the inCommon 'build' and CAF would be interested in identifying an interested person or group. Guidance on configuration can be provided if some wishes to self identify as interested.

There are two discrete areas for configuration -- Shibboleth and eduroam and tailoring the configuration is not difficult but inCommon specifics are needed for such an action.

If you are interested, please let us know.