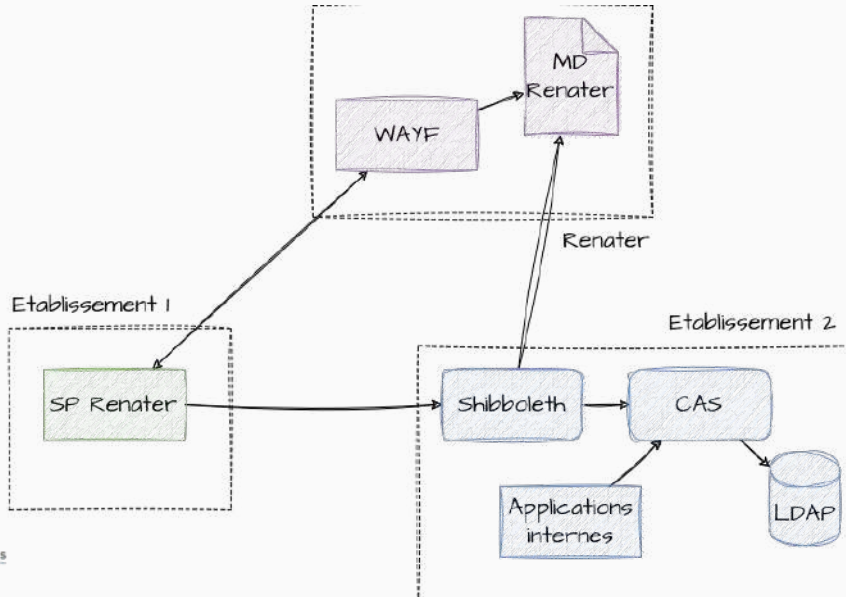


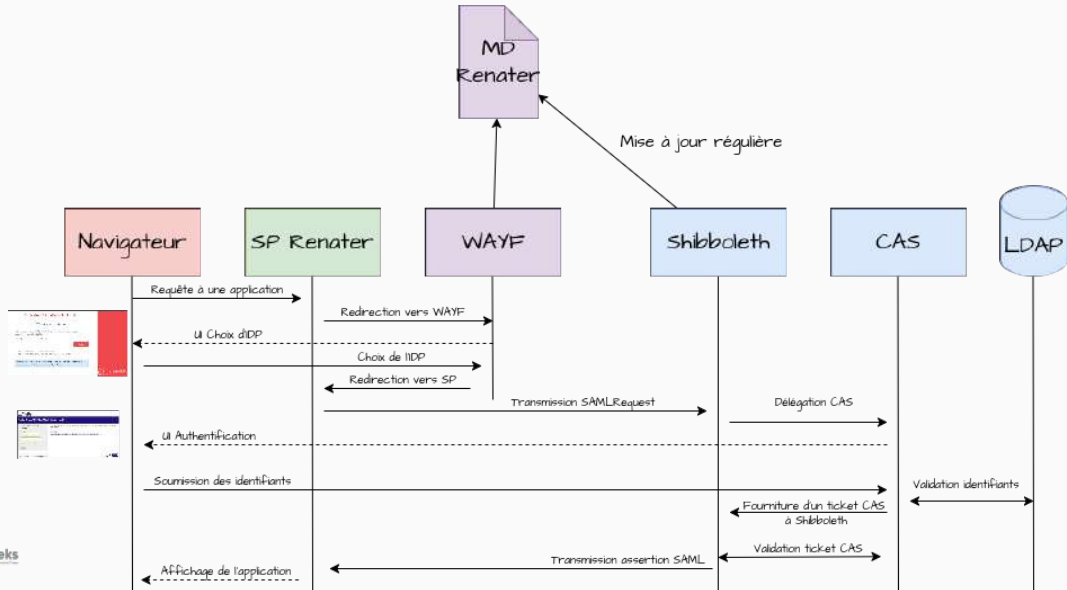
Shibboleth vers LemonLDAP::NG

Maxime Besson

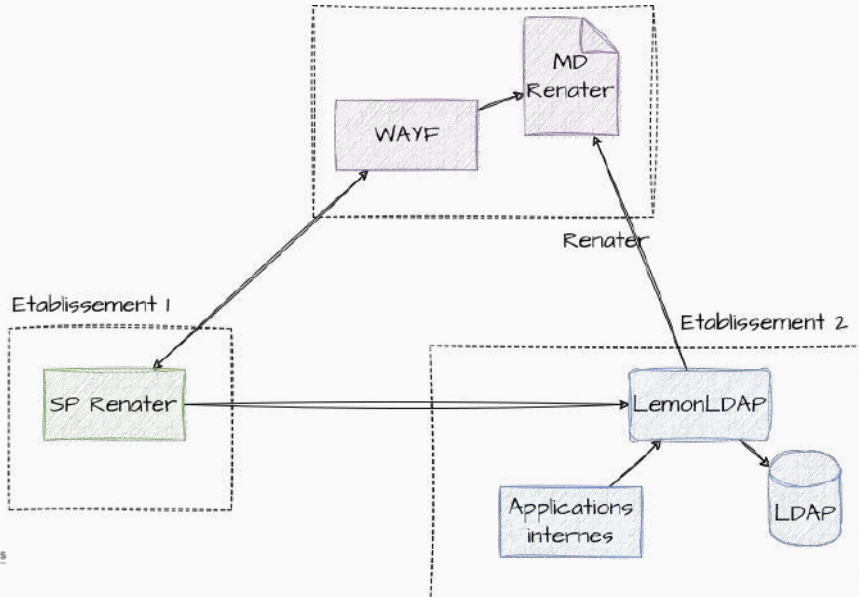
Authentication SSO historique



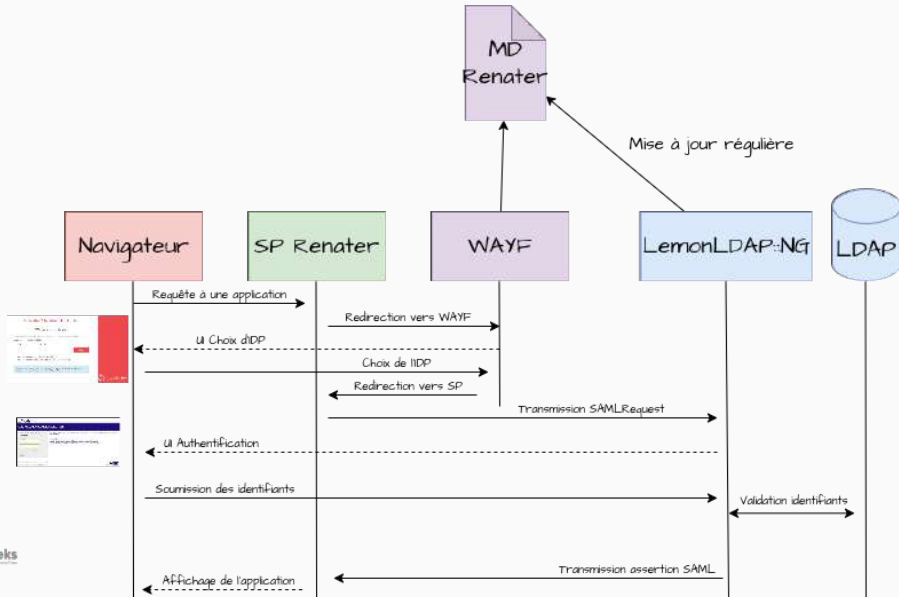
Authentication SSO historique



Migration vers LemonLDAP::NG



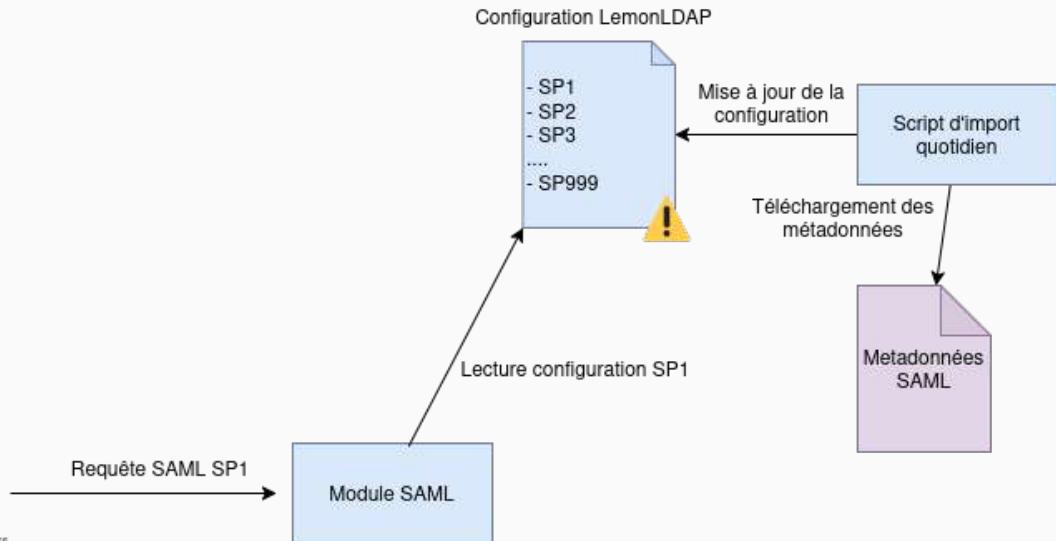
Migration vers LemonLDAP:NG



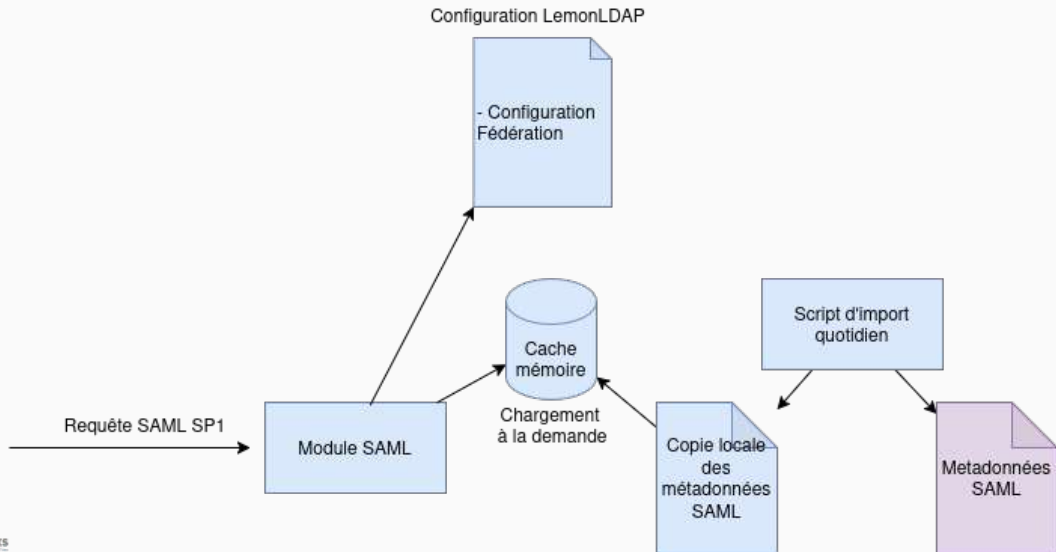
Avantages de LemonLDAP::NG

- Plus simple à installer et configurer que Shibboleth
- Un seul logiciel pour remplacer deux services
- Support du MFA, multiples types d'authentification

Ancien support des fédérations SAML



Système actuel support des fédérations SAML



- Les fédérations sont déclarées comme si elles étaient de simples applications SAML
- Multiple fédérations simultanément
- Possibilité de placer des options par défaut pour chaque fédération
- Possibilité de surcharger des options pour un SP particulier

SAML2 Service » Advanced

Federation

**SAML
Federation
Metadata
files**

/etc/lemonldap-ng/saml/main-sps-renater-metadata.xml|

Configuration

The screenshot displays the LemonLDAP:NG configuration interface. On the left is a sidebar menu with the following items: 'Policy', 'Is Passive', 'SAML Identity Providers' (expanded), 'fed-renater' (expanded), 'Metadata', 'Exported attributes', 'Session', 'Signature', 'Binding', 'Security', 'Options' (selected), 'Display', 'SAML Service Providers', and 'OpenID Connect Service'. The main content area at the top has navigation links: 'Home', 'Save', 'Browse', and 'Hide help'. Below these, the breadcrumb 'SAML Identity Providers - fed-renater - Options' is shown. The 'Federation' section contains the 'Entity Identifier' field with the value 'https://federation.renater.fr/'. The main heading is 'Configure template IDP/SPs'. The text explains that SAML metadata is generic and provides instructions on how to configure it. A list of steps is provided: adding a new SAML2 Service provider, leaving metadata empty, and setting the 'Entity Identifier' to the federation's Name attribute. It notes that all options set on this provider will be applied to SPs or IDPs in the Renater federation. It also mentions that Federation Metadata files contain a list of attributes that the SP wishes to receive, which can be flagged as optional or mandatory (using 'isRequired="true"'). Finally, it states that LemonLDAP:NG lets the user decide what to do with these attributes, with the option to 'Keep' the attribute definition from federation metadata.

Policy

Is Passive

▼ SAML Identity Providers

▼ fed-renater

Metadata

Exported attributes

Session

Signature

Binding

Security

Options

Display

SAML Service Providers

OpenID Connect Service

Home Save Browse Hide help

SAML Identity Providers - fed-renater - Options

Federation

Entity Identifier

Configure template IDP/SPs

SAML metadata does not contain all the information LemonLDAP:NG needs. It is recommended that you create a generic configuration for all the providers found in federation metadata.

In order to do this:

- Add a new SAML2 Service provider (or IDP)
- Leave the *Metadata* content empty
- Set *Options » Federation » Entity Identifier* to the *Name* attribute of the federation. (eg: `https://federation.renater.fr/`)

All options set on this special provider will be applied to SPs (or IDPs) defined in the Renater federation

In the case of Service Providers, Federation Metadata files contain a list of attributes that the SP wishes to receive. These attributes can be flagged as optional or mandatory (`isRequired="true"`).

LemonLDAP:NG lets you decide what to do with these attributes:

- **Keep**: The attribute definition from federation metadata will be handled by LemonLDAP:NG

Configuration

▼ SAML Service Providers

▼ fed-renater

Metadata

Exported attributes

▼ Options

Authentication response

Signature

Security

▼ Federation

Entity Identifier

Optional attributes

Required attributes

Home Save Browse Hide help

SAML Service Providers - fed-renater - Options

Federation

Entity Identifierhttps://federation.renater.fr/

Optional attributesKeep

Required attributesKeep

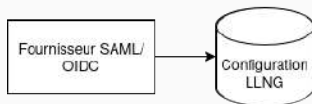
Options

Authentication response

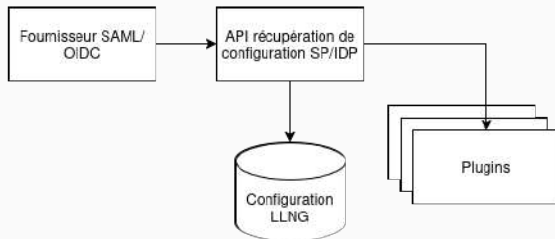
- **Default NameID format:** if no NameID format is requested, or the NameID format undefined, this NameID format will be used. If no value, the default NameID format is Email.
- **Force NameID session key:** if empty, the NameID mapping defined in [SAML service](#) configuration will be used. You can force here another session key that will be used as NameID content.
- **One Time Use:** set the OneTimeUse flag in authentication response (`<Conditions>`).

- Federation EduGain
 - Mauvaise gestion des multiples noms d'attribut (sn/suranne)
 - Pas de support natif de subjectid/pairwiseid
 - Problème avec certains SP nécessitant un eduPersonTargetedID
- Gestion des métadonnées
 - Pour l'instant: via une synchro périodique à mettre en place (downloadSamlMetadata)
 - Pas de support MDQ
- Un seul WAYF possible

Historique



Nouvelle API



- Le support de la fédération Renater est un simple plugin
- Possibilité d'implémenter ses propres plugins
 - Lazy loading
 - Source externe de configuration SP/IDP