Error handling in a distributed federated ecosystem

Guillaume Rousse <guillaume.rousse@renater.fr>

RENATER

June 7, 2023

Plan

Full-mesh federation

Multiple stakeholders

- organization #1 manages the identity provider
- organization #2 manages the service provider
- organization #3 eventually manages the discovery service
  we let our community use our discovery service for their own services

Full-mesh federation

Multiple stakeholders

- organization #1 manages the identity provider
- organization #2 manages the service provider
- organization #3 eventually manages the discovery service
  we let our community use our discovery service for their own services

Complex ecosystem

- multiple points of failure
- multiple causes of failures: wrong configuration, metadata propagation delay, authentication problem, ...
- errors are not always handled localy: identity provider negative SAML responses handling is delegated to service provider

Dispatching errors

Multiple causes

- low investement on error handling often result in defaut error messages, incomprehensible for end users
- visibility bias: lost users often click on the first ’help’ button found, turning to the more visible stakeholder
- psychological bias: our federation is often mislabelled as the ’RENATER federation’, implying we’re responsable for anything going wrong

Dispatching errors

Multiple causes

- low investement on error handling often result in defaut error messages, incomprehensible for end users
- visibility bias: lost users often click on the first 'help' button found, turning to the more visible stakeholder
- psychological bias: our federation is often mislabelled as the 'RENATER federation', implying we're responsable for anything going wrong

Results

- for us: useless work, and useless friction
- for user: additional resolution delay

Typical example

User #1

Hello. Some of my colleagues don't have access to their Virtual Learning Environment. Some others do have access, but their Zoom connection time is limited to 40 minutes. Those persons really need access to intranet for their professional duty. Thanks for your help.

Typical example

User #1

Hello. Some of my colleagues don't have access to their Virtual Learning Environment. Some others do have access, but their Zoom connection time is limited to 40 minutes. Those persons really need access to intranet for their professional duty. Thanks for your help.

RENATER Support

Hello. We are RENATER, a service provider for the ESR community. As we don't manage any kind of Virtual Learning Environnement, nor any Zoom service, we guess you'd better ask your own local support. BTW, why did you contact us ? Regards.

Typical example

User #1

Hello. Some of my colleagues don't have access to their Virtual Learning Environment. Some others do have access, but their Zoom connection time is limited to 40 minutes. Those persons really need access to intranet for their professional duty. Thanks for your help.

RENATER Support

Hello. We are RENATER, a service provider for the ESR community. As we don't manage any kind of Virtual Learning Environnement, nor any Zoom service, we guess you'd better ask your own local support. BTW, why did you contact us ? Regards.

User #1

Hello. My helpdesk advised me to contact you...

Plan

Human automation: support procedure

Response for end-user

- response message template, with involved entities technical contacts
- user-targeted documentation: how to identify error source
- feedback loop: why did the user contacted us ?

Human automation: support procedure

Response for end-user

- response message template, with involved entities technical contacts
- user-targeted documentation: how to identify error source
- feedback loop: why did the user contacted us ?

Message for administrators

- please implement proper error interception mechanism, here is how to do...
- please set up proper error message, here is a suggestion...
- please don't use the wording "authentication trough RENATER federation"

Preventing problems: proactive support

Tooling

- plugin-based monitoring tool
- daily automated run
- human-based ticket opening

Preventing problems: proactive support

Tooling

- plugin-based monitoring tool
- daily automated run
- human-based ticket opening

Focus

- compliance: no simultaneous registration in test and production federation
- technical issues: registration in federation without corresponding metadata loading

Avoiding useless mediation: error service

Shibboleth SP error handler

- all RENATER services use centralized SP reverse-proxies
- Shibboleth SP allow to issue HTTP redirection in case of error

```
https://erreur.renater.fr/saml/node1?now=Fri May 19 11:39:21 CEST 2023
    &errorType=opensaml::FatalProfileException
    &statusCode=urn:oasis:names:tc:SAML:2.0:status:Responder
    &statusCode2=
    &errorText=SAML response reported an IdP error
    &entityID=https://idp.inserm.fr/idp/shibboleth
    &requestURL=https://evento.renater.fr/Shibboleth.sso/SAML2/POST
```

Avoiding useless mediation: error service

Shibboleth SP error handler

- all RENATER services use centralized SP reverse-proxies
- Shibboleth SP allow to issue HTTP redirection in case of error

```
https://erreur.renater.fr/saml/node1?now=Fri May 19 11:39:21 CEST 2023
    &errorType=opensaml::FatalProfileException
    &statusCode=urn:oasis:names:tc:SAML:2.0:status:Responder
    &statusCode2=
    &errorText=SAML response reported an IdP error
    &entityID=https://idp.inserm.fr/idp/shibboleth
    &requestURL=https://evento.renater.fr/Shibboleth.sso/SAML2/POST
```

Renater error service

- custom PHP application
- configuration-based error type determination, allowing customized error messages:
  - IdP side error: please contact your technical support, we can't do anything
  - SP side error: please open a support ticket using our support portal
- multilingual support

Error service screenshot

SERVICES RENATER

AUTHENTICATION PROBLEM FOR THE SERVICE EVENTO

OOOPS...

Your authentication service reports an error on its side.

If you are a user, you should contact your authentication service administrators (mailto:equipe-identitas@listes.renater.fr) or your local support, as only them can fix this problem. If you are an administrator of this authentication service, you should check its configuration.

As a last resort, you can open a request on our support portal with the following information:

- error time : Fri May 19 11:39:21 CEST 2023
- nature of the error : saml
- type de l'erreur : IdP-side error
- requested service : Evento
- SAML id of your identity provider : https://idp.inserm.fr/idp/shibboleth
- Requested URL : https://evento.renater.fr/Shibboleth.sso/SAML2/POST

The RENATER services team

TECHNICAL EXPLANATION

Those explanations are only intended for GIP users, and displayed only from internal network.

If the problem persists, please contact the requested service team.
Received parameters :

type	saml
node	node1
service	
now	Fri May 19 11:39:21 CEST 2023
errorType	opensaml::FatalProfileException
statusCode	urn:oasis:names:tc:SAML:2.0:status:Responder
statusCode2	
errorText	SAML response reported an IdP error
entityID	https://idp.inserm.fr/idp/shibboleth
requestURL	https://evento.renater.fr/Shibboleth.sso/SAML2/POST
X-Forwarded-For	195.98.239.132
Remote	10.45.16.5
adminContact	

All rights reserved © GIP RENATER - 2023 - Legal notice

Error service generalization

Multiple error sources support

- WAYF errors: switchWAYF support
- proxy errors: Apache error handler
- service unavailability: BigIP fallback mechanism
- other opportunities: missing attributes, invalid attribute values, ...

Conclusion

Does it work ?

- no actual statistics
- some users open support tickets, despite explicit message...