Error handling in a distributed federated ecosystem

Guillaume Rousse <guillaume.rousse@renater.fr>

RENATER

June 7, 2023
Plan

1 Problem

2 Answer

Guillaume Rousse <guillaume.rousse@renater.fr>

Error handling in a distributed federated ecosystem
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 locally: identity provider negative SAML responses

handling is delegated to service provider

Guillaume Rousse <guillaume.rousse@renater.fr>
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 locally: identity provider negative SAML responses
  handling is delegated to service provider
Dispatching errors

Multiple causes

- low investment on error handling often result in default 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 responsible for anything going wrong

Results

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

Multiple causes

- Low investment on error handling often result in default 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 responsible for anything going wrong.

Results

- For us: useless work, and useless friction.
- For user: additional resolution delay.
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.
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 Environment, nor any Zoom service, we guess you’d better ask your own local support. BTW, why did you contact us ? Regards.
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

1. Problem

2. Answer

Guillaume Rousse <guillaume.rousse@renater.fr>

Error handling in a distributed federated ecosystem
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 through RENATER federation"
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

Guillaume Rousse <guillaume.rousse@renater.fr>

Error handling in a distributed federated ecosystem
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

```
h t t p s : / / e r r e u r . r e n a t e r . f r / s a m l / n o d e 1 ? n o w = F r i M a y 1 9 1 1 : 3 9 : 2 1 C E S T 2 0 2 3  
 & e r r o r T y p e = o p e n s a m l : : F a t a l P r o f i l e E x c e p t i o n  
 & s t a t u s C o d e = u r n : o a s i s : n a m e s : t c : S A M L : 2 . 0 : s t a t u s : R e s p o n d e r  
 & s t a t u s C o d e 2 = 
 & e r r o r T e x t = S A M L r e s p o n s e r e p o r t e d a n I d P e r r o r  
 & e n t i t y I D = h t t p s : / / i d p . i n s e r m . f r / i d p / s h i b b o l e t h  
 & r e q u e s t U R L = h t t p s : / / e v e n t o . r e n a t e r . f r / S h i b b o l e t h . s s o / S A M L 2 / P O S T
```

**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
Guillaume Rousse <guillaume.rousse@renater.fr>

Error handling in a distributed federated ecosystem
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...