eduGAIN Connectivity Check

Introduction

The purpose of the eduGAIN Connectivity Check is to identify eduGAIN Identity Providers (IdP) that are not properly configured. In particular, it checks if an IdP properly loads and consumes SAML2 metadata which contains the eduGAIN Service Providers (SP). The check results are published on the public eduGAIN Connectivity Check web page (https://technical.edugain.org/eccs/). The main purpose is to increase the service overall quality and user experience of the eduGAIN interfederation service by making federation and Identity Provider operators aware of configuration problems.

The check is performed by following two different wayfless URL and the various HTTP redirects until the IdP Login page. The expected result is a login form that allows users to authenticate (typically with username/password) or an error message. For those Identity Providers that output an error message, it can be assumed that they don’t consume eduGAIN metadata properly or that they suffer from another configuration problem. There are some cases where the check will generate false positives, therefore IdPs can be excluded from checks as is described below.

The Identity Providers are checked once per day. Therefore, the login requests should not have any significant effect on the log entries/statistics of an Identity Provider. Also, no actual login is performed because the check cannot authenticate users due to missing username and password for the IdPs. Only Identity Providers are checked but not the Service Providers.

The eduGAIN Connectivity Check 2 is configured to maintain a history of 7 days of the results collected.

If this page does not answer your questions or you need some more information about this service, please contact us at support@edugain.org.

Check performed on the IdPs

The check performed by the service follows these steps:

1. It retrieves the eduGAIN IdPs from eduGAIN Operator Team database via access API.
2. For each IdP the ECCS script:
   a. doesn’t check disabled IdP (added manually by an eduGAIN Operations Team via Python dictionary or dynamically by IdP administrator via “robots.txt”);
   b. verifies the SSL certificate;
   c. creates a Wayfless URL for two selected SP;
   d. tries to reach the IdP login page for both SPs without performing any authentication.

   It expects to find the HTML form with username and password fields. Therefore, no complete login will happen at the Identity Provider because the check stops at the login page.

   The SPs used for the check are “SP Demo” (https://sp-demo.idem.garr.it/shibboleth) from IDEM GARR AAI and the “AAI Viewer Interfederation Test” (https://attribute-viewer.aai.switch.ch/interfederation-test/shibboleth) from SWITCHaai. These SPs might change in the future if it will be needed.

   The SAML authentication request sent is not signed. Therefore, authentication request for any eduGAIN SP could be created because the SP’s private key is not needed.

3. At the end of the execution, the script is run again for those IdPs that have been failed the check due to a problem with the headless Webdriver (Google Chrome) used and writes each problem on the log file.

Statuses and results

The tool uses the following statuses for IdPs:

<table>
<thead>
<tr>
<th>Status</th>
<th>UI Color</th>
<th>Description and results</th>
</tr>
</thead>
</table>

[Index]
The IdP's response contains an HTTP Error or the web page returned does not look like a login page.
- **Invalid-Form**: considers those IdPs that do not load a standard username/password login page and do not return messages like "No return endpoint available for relying party" or "No metadata found for relying party".
- **Timeout**: considers those IdPs that do not load a standard username/password login page within 60 seconds.
- **Connection-Error**: considers those IdPs that are not reachable due to a connection problem.
- **IdP-Error**: the web page returned by the IdP does not contain a Login Form and reports an unspecified error such as "An error occurred". This has been seen on Microsoft ADFS based IdPs.
- The IdP most likely does not consume the eduGAIN metadata correctly. A typical case that falls into this category is when an IdP returns a message "No return endpoint available for relying party" or "No metadata found for relying party".
- **No-eduGAIN-Metadata**: The HTTP SSL certificate used by the IdP is either invalid or has chain issues (see below for further explanation): 
  - **SSL-Error**

The IdP most likely correctly consumes eduGAIN metadata and returns a valid login page. This is no guarantee that login on this IdP works for all eduGAIN services but if the check is passed for an IdP, this is probable.

The IdP is excluded because it cannot be checked reliably. The "Page Source" column, when an entity is disabled, shows the reason for the disabling.

**Common reasons for check failure**

1. Verify that you have a valid SSL certificate matching your IdP hostname and with a valid chain. You can test it yourself with the SSL Labs checker: [https://www.ssllabs.com/ssltest/](https://www.ssllabs.com/ssltest/)
   An "SSL-Error" may be related to a missing update of the CAs used by ECCS. If you suspect that this is the case, please contact the eduGAIN support at support@edugain.org.
2. Verify that the IP used by the client that is performing the checks, is permitted to reach your IdP: any firewall in-between must be configured to let pass TCP packets with:
   a. source IP X.X.X.X, source port 1024-65535
   b. destination YOUR-IDP-IP destination port 443
3. Verify that your IdP Login page contains a text that matches with the following regular expression:
   a. pattern_password = "<input[^<]*type="password[^"]*password([^>]*)[^"]*";"
4. Verify that your robots.txt is not unintentionally disabling ECCS.

**Limits**

There are some situations where the check cannot work reliably. In those cases, it is possible to disable the check for a particular IdP.

The so far known cases where the check might generate a false negative are:

- IdP does not support HTTP or HTTPS with at least SSLv3 or TLS1 or newer (these IdPs are insecure anyway)
- IdP is part of a Hub & Spoke federation (some of them manually have to first approve eduGAIN SPs)
- IdP does not use web-based login form (e.g. HTTP Basic Authentication or X.509 login)
- IdP that use more than one <iframe> inside their login page

**Disable Checks**

In cases where an IdP cannot be reliably checked, it is necessary to create or enrich the `robots.txt` file on the IdP's web root with:

```
User-agent: ECCS
Disallow: /
```

If it is not possible to create the `robots.txt` under the IdP web root directory, the check can be disabled by an operator of the federation, where the IdP is a member, with an email to support@edugain.org.
User interface

The eduGAIN Connectivity Check Service web page is available at https://technical.edugain.org/eccs

User interface parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>Show all the service results for a specific date</td>
<td>date=2020-02-20</td>
</tr>
<tr>
<td>reg_auth</td>
<td>Show all the service results for a specific Registration Authority</td>
<td>reg_auth=<a href="https://reg.auth.example.org">https://reg.auth.example.org</a></td>
</tr>
<tr>
<td>idp</td>
<td>Show all the service results for a specific Identity Provider</td>
<td>idp=<a href="https://idp.example.org/idp/shibboleth">https://idp.example.org/idp/shibboleth</a></td>
</tr>
</tbody>
</table>
| status         | Show all the service results for a specific Status:  
|                | - OK  
|                | - ERROR  
|                | - DISABLED | status=ERROR |
| check_result   | Show all the service results for a specific result of check:  
|                | - Invalid-Form  
|                | - Timeout  
|                | - Connection-Error  
|                | - No-eduGAIN-Metadata  
|                | - SSL-Error  
|                | - IdP-Error | check_result=SSL-Error |

Example:


API interface

The eduGAIN Connectivity Check has an API interface that provides access to the monitoring results in JSON format.

The table below describes the actions that can be performed by replacing "##ACTION##" in the URL:

https://technical.edugain.org/eccs/api/##ACTION##

<table>
<thead>
<tr>
<th>Action Name (JSON)</th>
<th>Action Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eccsresults</td>
<td>Returns all the eduGAIN Connectivity Check 2 service results</td>
</tr>
<tr>
<td>fedstats</td>
<td>Returns all the federation statistics collected by the eduGAIN Connectivity Check 2 service.</td>
</tr>
</tbody>
</table>

The table below, instead, describes the JSON parameters that actions can use:

https://technical.edugain.org/eccs/api/##ACTION##?##PARAMETER##=<value>

<table>
<thead>
<tr>
<th>Action Name (JSON)</th>
<th>Parameter Name (JSON)</th>
<th>Parameter Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>eccsresults</td>
<td>date</td>
<td>Returns all the service results for a specific date.</td>
<td>date=2020-02-20</td>
</tr>
<tr>
<td>fedstats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Parameter</td>
<td>Description</td>
<td>URL</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>eccsresults</td>
<td>reg_auth</td>
<td>Returns all the service results for a specific Registration Authority.</td>
<td>reg_auth=<a href="https://reg.auth.example.org">https://reg.auth.example.org</a></td>
</tr>
<tr>
<td>fedstats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eccsresults</td>
<td>idp</td>
<td>Returns the service results for a specific IdP by its entityID.</td>
<td>idp=<a href="https://idp.example.org/idp/shibboleth">https://idp.example.org/idp/shibboleth</a></td>
</tr>
<tr>
<td>status</td>
<td></td>
<td>Returns all the service results for a specific Status:</td>
<td>status=ERROR</td>
</tr>
<tr>
<td>check_result</td>
<td></td>
<td>Returns all the service results for a specific result of check:</td>
<td>check_result=SSL-Error</td>
</tr>
<tr>
<td>format</td>
<td></td>
<td>Formats the service results in a simple way</td>
<td>format=simple</td>
</tr>
</tbody>
</table>

Example URL:

- https://technical.edugain.org/eccs/api/eccsresults?
  - reg_auth=http://www.idem.garr.it/
  - status=ERROR
  - format=simple
- https://technical.edugain.org/eccs/api/eccsresults?
  - reg_auth=http://www.idem.garr.it/
  - status=ERROR
- https://technical.edugain.org/eccs/api/fedstats?
  - reg_auth=http://www.idem.garr.it/
- https://technical.edugain.org/eccs/api/fedstats?
  - reg_auth=http://www.idem.garr.it/
  - date=YYYY-MM-DD

[Index]

**GIT repository**

https://gitlab.geant.org/edugain/eccs

[Index]

**Presentations**

- ECCS2 4 GN4-3 WP5 Hands-All Meeting.pdf