Testing S3 api for object storage, and Federated AAI for HNSciCloud

Daniil Pintjuk

September 1, 2017

Contents

1 Introduction

During my time at CERN join the HNSciCloud PCP project. A Pre-commercial Procurmet tender to develop a cloud platform to support high performance computing and big data capabilities for scientific research.

When I joined the project was moving into the stage of testing prototype platforms from the 3 contractors:

1. T-systems, Huawell, Cyfront, Divia
2. IBM
3. RHEA Group, T-systems, exoscale, SixSq

My contribution was going to be to perform 2 of CERN's tests sets of the prototypes.

The prototypes ware reacquired to provide Object Storage (OBS), and support a subset of S3 API for operations on the object storage. The purpose of the first set of tests was to validate that the S3 API for the object storage was implemented correctly.

It was also required that the prototypes supported Federated Authentication through EduGAIN. So that users of HNSciCloud could use there home University credentials to access the services of HNSciCloud. The second set, consisted of tests to ensure correct behavior of of this system.

During the first month of the project the prototype phase had not started yet. So I used the time to get up to speed on the project and learning the tools i was going to use for the tests. I ran S3 tests against CREN's openstack service.

In July the T-systems made there platform available for testing. Later in July T-systems and RHEA made there Federated Authentication portals available for testing.

In august IBM made there platform available for testing and I performed the S3 tests.

No results of the tests will be presented as they are confidential.

2 Background

2.1 Object storage

Object storage is a computer data storage architecture that manages data as objects, as opposed to other storage architectures like file systems which manage data as a file hierarchy and block storage which manages data as blocks within sectors and tracks.

S3 is an API for operations on the object storage, e.g.: creating a bucket (objects are organized into containers called buckets), uploading objects into the bucket, downloading objects from a bucket, deleting objects, etc.

2.2 Federated Authentication and Single Sign-on

Federated Authentication Is the means of linking a persons identity to accounts and data stored across multiple systems and organizations. Single Sign-on is a part of Federated Authentication that enables a service provider from one organization to delegate web based authentication to another organization. For example this allowed a CERN researcher to login to a HNSciCloud service managed by an external contractor using his CERN computing account.

EduGAIN is the Federated Authentication network that CERN and most Universities are part of.

3 Test description

3.1 S3 test

The S3 test consists on a script that attempts the following operations on specified S3 endpoint:

- S3 authentication (access key + secret key)
- PUT
- GET
- GET with prefix matching
- GET chunk
- GET multiple chunks

For more information, as well as the davix based test script: `https://gitlab.cern.ch/okeeble/s3test/tree/master`

AWS based s3test script: `http://cern.ch/stikked/view/a326d01a`

3.2 Eudigan AAI

These tests relate to evaluating compliance with edugain login requirements.

The following tests will be run manually:

	Tests	Expected Result
1	User attempts authentication from an eduGAIN IdP with R&S compliant attribute release	Authentication successful
2	User attempts authentication from an eduGAIN IdP with insufficient attribute release	Authentication unsuccessful and helpful error page produced
3	User attempts authentication from multiple eduGAIN IdPs with credentials sharing a common email address	Authentication resolves to multiple,distinct users
4	User accesses a permitted resource (e.g. tenant specific data)	Authenticated user is granted access
5	User accesses a forbidden resource (e.g. tenant specific data)	Authenticated user is denied access
6	User is blocked by Admin	Admin is able to block an individual user
7	Blocked user attempts authentication	Blocked user is denied access
8	>10 users authenticate simultaneously	Users authenticate in accordance with Reference Results (1) and (2)

The tests will be documented in a table with following columns:

test	idP	Result	Matches reference?	Comment
1				
2				
...				

4 Description of how the tests ware performed

4.1 S3 test

4.1.1 IBM

The davix client does not work with IBM, AWS s3api was used instead. A modified version of the davix based script was used where all the davix commands ware replaced by equivalent AWS s3api commands.

- Not yet possible for us to manage buckets, and access keys. So IBM created a test bucket emailed us the keys and endpoint URL.
- Created a VM with the HN.sh command line tool, with following parameters.
  - CPU: 1
  - Memory: 1024MB
  - Image: $\text{CENTOS}_{\text{LATEST64}}$
- Installed AWS s3api, configured AWS credentials with the keys and endpoint URL received from IBM.
- executed the AWS based s3test script.

4.1.2 T-Systems

- Created a bucket in OBS section of MyWorkspace dashboard with following parameters:
  - Class: Standard
- Created an ECS VM on MyWorkspace dashboard with following parameters:
  - ECS type: General-Purpose
  - vCPU: 1
  - Memory: 4GB
  - Image: $\text{Standard}_{\text{CentOS7latest}}$
- Installed davix client on the VM, cloned S3 endpoint test, and configured the s3 host to be the newly created bucket using the URL: s3://testbucket.obs.otc.t-systems.com
- Executed the script in S3 endpoint test repository

4.2 Auth AAI tests

4.2.1 RHEA

1. Test 1 Using my CERN eduGAIN account an account was created on nuv.la following the instructions on: `http://hn-prototype-docs.readthedocs.io/en/latest/administrator/index.html` After receiving administrative rights, I successfully logged in to fed-id.nuv.la/auth/. Selecting CERN Realm and CERN IDP. There I was able to check the attributes of my user account against the R&S specification.

2. Test 3

   - In CERN's user settings portal I changed my primary email address to the email address of my KTH account.
   - I attempted to login to fed-id.nuv.la using my CERN account. And checked the user id and email of the account i was logged into.
   - I attempted to login to fed-id.nuv.la using my KTH account, And checked the user id and email of the accounts i was logged into.

3. Test 6 & 7

   - A Colleague used there CERN EduGAIN account to login to nuv.la and fed-id.nuv.la, following the instructions on: `http://hn-prototype-docs.readthedocs.io/en/latest/administrator/index.html`.
   - Using my administrative account on fed-id.nuv.la I blocked my colleagues account by adding it to the black list as described in `http://hn-prototype-docs.readthedocs.io/en/latest/administrator/blacklisting.html`
   - My colleague used there blocked account to attempt a login to fed-id.nuv.la.
   - My colleague used there blocked account to attempt a login to. nuv.la.

4.2.2 T-systems

1. Test 1

   - Attempted To login to the portal at a URL provided by T-systems
   - Redirected To CERN authentication portal.
   - Outcome is confidential.
   - No further tests ware possible.