

**EGI-Engage**

Final CANFAR Integration Release

D4.10

|  |  |
| --- | --- |
| **Date** | 19 June 2017 |
| **Activity** | WP4 |
| **Lead Partner** | INAF |
| **Document Status** | FINAL |
| **Document Link** | <https://documents.egi.eu/document/3038> |

Abstract

CANFAR/EGI integration activity drives collaboration between EGI and the Canadian Advanced Network for Astronomical Research (CANFAR) cloud infrastructure. CANFAR is an integrated cloud to support collaborative astronomy (A&A) teams. This document summarizes the implementation results of CANFAR and EGI federated cloud in support of data-intensive collaborative astronomy research and it is organized as a demonstrator of the activity done in terms of: deployed infrastructure, software development, services and applications. During the EGI Engage project, a great deal of work has been done to improve the configurability and deployability out of the box of the CADC open-software API implementations which forms the basis on which CANFAR and EGI federated OATs-INFAF software infrastructures are built. The Access Control software used by CANFAR for authentication and authorization purpose has been modified and adapted to allow the interoperability between different software infrastructures geographically distributed. The same authentication mechanism based on X509 and VOMS proxies is now supported both by EGI FedCloud and the community services offered by CANFAR and OATs-INAF infrastructures. This provides users with an homogeneous authentication mechanism allowing transparent authentication to all available services. Because the CADC open-software APIs provides an IVOA VOSpace interface implementation, but not an underlying storage service, during the EGI Engage project a thin storage management service, compliant with the CADC VOSpace interface implementation and able to be interfaced with different storage solutions has been implemented. Specific tools for distributed data access and management have been made available to the EGI FedCloud users.

The federation model followed during the implementation is based on the assumption that the two clouds will remain independent and independently managed but users and projects will be able to use both e-infrastructures for data sharing and computing. The demonstrator highlights how the integration has been perused, showing step by step the pattern to achieve access, infrastructure interoperability and service exploitation. Despite, this demonstrator shows how the A&A communities and data centres can benefit from using EGI infrastructure and services federated during the project.

**COPYRIGHT NOTICE**



This work by Parties of the EGI-Engage Consortium is licensed under a Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). The EGI-Engage project is co-funded by the European Union Horizon 2020 programme under grant number 654142.

**DELIVERY SLIP**

|  |  |  |  |
| --- | --- | --- | --- |
|  | ***Name*** | ***Partner/Activity*** | ***Date*** |
| **From:** | Giuliano Taffoni | INAF/WP4 | 21/08/2017 |
| **Moderated by:** | Malgorzata Krakowian | EGI Foundation WP1 |  |
| **Reviewed by** | André Schaaff  Peter Solagna | Université de Strasbourg  EGI Foundation WP5 |  |
| **Approved by:** | AMB and PMB |  |  |

**DOCUMENT LOG**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Issue*** | ***Date*** | ***Comment*** | ***Author/Partner*** |
| **v.1** | 16/06/2017 | Document structure and TOC | Giuliano Taffoni /INAF |
| **v.2** | 20/06/2017 | Introduction and general description | Giuliano Taffoni /INAF |
| **v.3** | 24/06/2017 | Software description, new figures and appendix | Giuliano Taffoni /INAF |
| **v.4** | 30/06/2017 | New introduction, architectural description and figures | Giuliano Taffoni /INAF |
| **v.5** | 03/07/2017 | References | Giuliano Taffoni /INAF |
| **v.6** | 20/07/2017 | Final version ready for internal review | Giuliano Taffoni /INAF |
| **v.7** | 07/08/2017 | Reviewer comments |  |
| **v.8** | 21/08/2017 | Final release including reviewers comments | Giuliano Taffoni /INAF |

**TERMINOLOGY**

A complete project glossary and acronyms are provided at the following pages:

* <https://wiki.egi.eu/wiki/Glossary>
* <https://wiki.egi.eu/wiki/Acronyms>

CANFAR: Canadian Advanced Network for Astronomical Research

A&A: Astronomy and astrophysics

AAI: Authentication and Authorization Infrastructure

AC: Access Control

BE: Back-End

CA: Certification Authority

DAO: Data Access Objects

ESA: European Space Agency

FE: Front-End

IaaS: Infrastructure as a Service

IGTF: Interoperable Global Trust Federation

IVOA: International Virtual Observatory Alliance

LDAP: Lightweight Directory Access Protocol

RDBMS: Resource DataBase Management Service

SAML: Security Assertion Markup Language

Single Sign-on (SSO)

VM: Virtual Machine

VOMS: Virtual Organization Membership Service

**Contents**

1 Introduction 6

1.1 Background and motivations 6

1.2 CANFAR Cloud for Astronomy 7

1.3 Infrastructure 9

1.3.1 CANFAR Infrastructure 9

1.3.2 EGI FedCloud Infrastructure 10

2 Demonstrator 10

2.1 Overview 10

2.2 Architecture 12

2.2.1 Detailed Implementation 17

2.3 Demonstration 20

2.3.1 Scenario 20

2.3.2 Service Demonstrator 22

2.3.3 Feedback 27

2.4 Future plans 28

3 Conclusions, lessons learnt, future work 29

4 Plan for Exploitation and Dissemination 30

5 References 32

Appendix: Command line interface, Web Gui 33

Users registration and management 34

User’s credentials verification and access management. 35

Groups management 36

Delegations management 38

VOSpace service client 38

Appendix: Manuals and Documentation 40

**Executive summary**

This document summarizes the implementation results of CANFAR and EGI federated cloud in support of data-intensive collaborative astronomy research and it is organized as a demonstrator of the activity done in terms of deployed infrastructure, software development, user tools and services. The Canadian Advanced Network for Astronomical Research is a digital infrastructure for Astronomy and Astrophysics (A&A) based on cloud storage and cloud processing middleware and on tools and services developed by the International Virtual Observatory Alliance (IVOA).

The demonstrator of the implemented platform and its capabilities can be organized in 3 different areas:

1. **Authentication and Authorization demonstrator**. The authentication is based on two possible mechanisms: X509 certificates and VOMS proxies usage and login-password authentication. All the involved infrastructures support both methods. The authorization is based on the community service called GMS (Group Management Service) which stores information on user’s group memberships.
2. **Data Sharing demonstrator**. The ability to share data between users of different infrastructures is based, after the common authentication strategy, on two services: VOSpace and GMS. VOSpace implements an IVOA standard interface providing a common communication protocol between services and stores data access rights information in terms of groups allowed to access data. GMS stores information on user’s groups membership and delegates to the project principal investigator the right to grant access to data to different groups of users.
3. **Virtual Machines (VM) exploitation**. Specific applications to access infrastructures and data and to reduce/analyse astronomical data are under testing and as soon as validated by pilot users they will be made available in a Virtual Machine. This VM will be registered in the EGI Application Database and in the CANFAR cloud marketplace, to be available to a truly wide A&A community.

# Introduction

## Background and motivations

The A&A community has gathered rich experiences in cloud computing within the CANFAR federated cloud deployed on Compute Canada resources and operated by National Research Council Canada. However, Europe is missing a Research Infrastructure for A&A. The Canadian cloud infrastructure represents a unique example of an A&A oriented infrastructure that joins together the IaaS and the standards and services developed by the IVOA e.g. for user authentication and authorization, data sharing, access to data and archives, and finally data processing.

Starting from the existing CANFAR infrastructure and the EGI FedCloud, an OpenStack cloud has been deployed at INAF, it is OpenStack based, so compliant with the EGI Federated Cloud Architecture, and the process to join the EGI federated cloud as resource provider has been started.

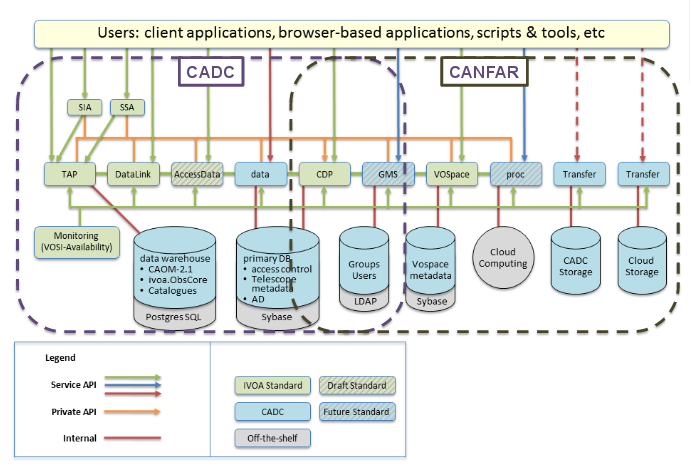
At the same time, the INAF cloud site provides a set of community services implementing the IVOA standards, able to interoperate with the CANFAR infrastructure. This way, a Virtual Observatory infrastructure is available in the EGI FedCloud. To achieve this result, a heavy development work has been done

* to improve the configurability and deployability out of the box of the CADC open-source software, on which are based CANFAR infrastructure and INAF cloud site provided services,
* to introduce an authentication and authorization mechanism able to manage data and compute access of users coming both from CANFAR infrastructure and EGI FedCloud,
* to develop a storage manager service compliant with the IVOA VOSpace interface and able to manage different storage solutions,
* to make available to the EGI users specific tools to access a huge amount of astronomical data and to manage and share them.

## CANFAR Cloud for Astronomy

The Canadian Advanced Network for Astronomical Research (CANFAR)[[1]](#footnote-1) is a digital infrastructure combining the Canadian national research network (CANARIE)[[2]](#footnote-2), cloud processing and storage resources (Compute Canada)[[3]](#footnote-3) and an astronomy data centre (Canadian Astronomy Data Centre – CADC)[[4]](#footnote-4) into a unified ecosystem for storage and processing. It is an operational system for the delivery, processing, storage, analysis, and sharing of very large astronomical datasets: CANFAR stores about 2PBs of data and 900 Million of files. The project has combined the best features of the grid and cloud processing models by providing a self-configuring virtual cluster deployed on multiple cloud clusters. CANFAR processed about 2.7 Million of jobs for about 500 cores per year. The project has provided users a robust and secure virtual storage environment layered on distributed storage resources. The CANFAR services make use of many technologies from the grid, cloud and International Virtual Observatory (IVOA) communities. Initially deployed in 2011, CANFAR has continuously evolved in response to operational needs and user input.

CANFAR has four principal user-facing services: user storage (VOSpace), virtual machines on demand (Horizon/NOVA), batch processing (proc/Condor/CloudScheduler/NOVA) and group management (GMS), all RESTful web services[R6] accessible via http or browser user interfaces. CANFAR is developed, maintained and operated by the CADC with contributions from several Canadian universities. In Fig. 1 we provide a description of CANFAR infrastructure and the connection between the IVOA services offered by CADC and the CANFAR computing services.



**Fig.1** CANFAR infrastructure schema. This picture shows the main components of the infrastructure and the connection between the IVOS services offered by CADC and the CANFAR computing service

CADC is offering data access to astronomical archive data using IVOA standards. Both proprietary and public data can be accessed. An authentication and authorization infrastructure is used to provide access to proprietary data. The same infrastructure is used by CANFAR to allow access to computing and storage resources providing the computing and storage services for proprietary data analysis.

## Infrastructure

The CANFAR/EGI interoperability demonstrator is based on two infrastructures able to interoperate: the CANFAR infrastructure and the INAF-OATs cloud infrastructure EGI federated.

### CANFAR Infrastructure

In this section we will briefly describe CANFAR services that has been used in the demonstrator and that constitutes the CANFAR infrastructure.

**Authentication and Authorization** - Each user is identified by username/password and a X.509 certificate and must be the member of the Virtual Organization that identify the collaboration (in our case astronomy. If the user has a certificate it can be uploaded to the access control service otherwise a CANFAR certificate is automatically issued. Any certificate that has been issued by a Certification Authority (CA) from a member of the Interoperable Global Trust Federation (IGTF) can be accepted by CANFAR. To manage authorization, CANFAR implements a RESTful web service to manage groups and memberships. It supports three classes of operations: (i) Creating, getting, updating and deleting a group; (ii) Adding and deleting a user to a group; (iii) Adding and deleting a group to a group. Credential delegation is an IVOA RESTful web service that enables users to create temporary credentials at a site enabling that site to perform web service actions on their behalf [R4]. This feature is the key to allow services from different sites to interact (e.g. CANFAR VOSpace using an EU Group Management Service for authorization and delegated credentials for authentication).

**Storage service** - The distributed storage layer allows users to access, process and share their data. It is based on VOSpace IVOA service [R1] and on a data transfer service. CANFAR provides also a FUSE[R6] VOSpace implementation to allow users to mount their VOspace on virtual machines. The data transfer service is responsible for handling the upload and download of data to and from physical storage locations for VOSpace. The VOSpace service points users to the preferred data transfer service based on the requirements of the user's file transfer.

**Monitoring** - Each web service supports a RESTful monitoring interface that complies with the VOSI-availability (IVOA) standard. These interfaces can be monitored via periodic requests from many standard monitoring packages (e.g. Nagios) to provide a central view of a system. The IVOA Support Interfaces (VOSI) are discussed in [R2].

**Computing** - CANFAR is offering a cloud computing facility based on OpenStack that allows the creation of on demand virtual machines and data-location-aware virtual clusters to process and analyse data. Web interfaces allow users to create both single machines and virtual clusters to execute batch jobs.

### EGI FedCloud Infrastructure

The FedCloud infrastructure used in the demonstrator is based on an EGI FedCloud Site based on OpenStack Mitaka integrated with the monitoring and accounting services. The Authentication and Authorization Infrastructure (AAI) is based on the VOMS OpenStack plugin with two different Virtual Organizations: planck (a Virtual Organization that was open to support the ESA planck satellite collaboration), and astro.vo.eu-egee.org (a generic A&A virtual organization). The EGI Applications Database (EGI AppDB)[[5]](#footnote-5) is used to deploy the virtual machines equipped with infrastructure software clients as described in the next sections. The EGI FedCloud has been extended with a set of community services that allows the integration with CANFAR:

* An Access Control Service to manage internal users and groups, capable to verify group memberships both internal and external
* A Credential Delegation Service to manage X509 credentials of every user, internal and external
* A Storage Service supporting IVOA VOSpace standard interface to storage resources in the EGI FedCloud.

# Demonstrator

## Overview

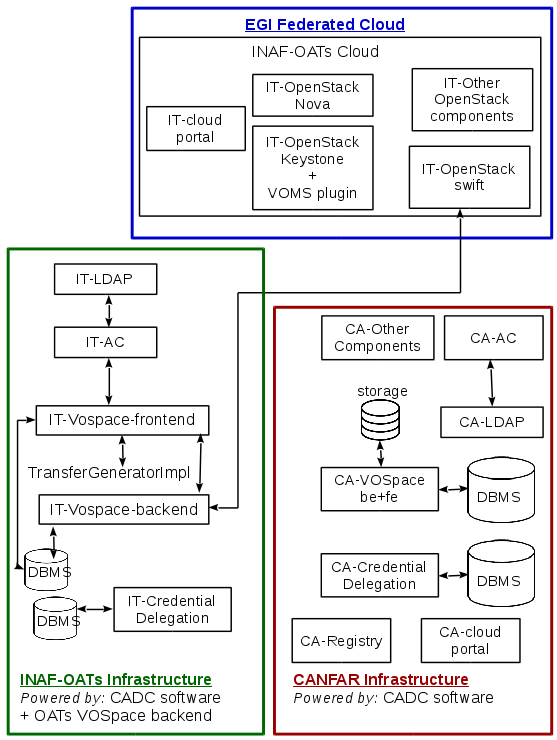
|  |  |
| --- | --- |
| **Name** | Astronomical Cloud infrastructure for EGI |
| **URL** | * Data Interoperability Video Demo: <https://youtu.be/T1U0qGLWTzA> * Computation Interoperability Video Demo: <https://www.youtube.com/watch?v=NjeH7_gOxdk> |
| **Description** | CANFAR-EGI federated e-infrastructure. The platform we set up demonstrates the actual interoperability level between CANFAR and EGI FedCloud and how the Astronomers can use the e-infrastructure to share data and to perform computation (data reduction or analysis) on it. |
| **Value proposition** | The adoption by European Astronomical Data Centers of standards of reference for the Astronomical Community proposed by the IVOA for data access and standards developed by EGI for cloud access, monitoring and VMs share, will allow A&A users to access astronomical data sets, tools and resources available worldwide in a transparent way.  The platform aims at facilitating the access to data and computing resources adopting standards interfaces towards EGI cloud. This work has been proposed also as a solution for SKA in particular for what regards the AAI and the Group Managing. |
| **Customer/user of the demonstrator** | Astronomers, Astronomical Data Centres, Astronomical projects (e.g. EUCLID, SKA) |
| **Scenario** | We presented the demonstrator at "ASTERICS DADI Technology Forum 3"[[6]](#footnote-6), at the EGI conference 2017[[7]](#footnote-7), at "IVOA Interoperability Meeting 2017 [[8]](#footnote-8) during the Grid and Web service working group session[[9]](#footnote-9) . At all of these venues, this demonstrator was received with interest because it covers a common use case (to access from Europe the data hosted by CANFAR) providing useful and easy to use tools. Besides the demonstrator presentation opened a profitable discussion on proposed solutions. |
| **Success criteria** | The short term success criteria for the demonstrator is the ability to be a driver for new technical discussion, new standards adoption and new users and developers engagement in EGI and IVOA.  The long term success criteria is a wide adoption of proposed tools and the increasing of the EGI community users. |
| **User Documentation** | <https://github.com/oats-cadc>, http://gms01.oats.inaf.it/doc/index.html |
| **Technical Documentation** | <https://github.com/oats-cadc>, http://gms01.oats.inaf.it/doc/index.html |
| **Developer team** | Taffoni Giuliano, Claudio Vuerli, Sara Bertocco, Fabio Pasian, Severin Gaudet, Patrick Dowler, Brian Major. |
| **License** | GPL version 2 or any later version |
| **Source code** | <https://github.com/opencadc>  https://www.ict.inaf.it/gitlab/OATS-CADC |

## Architecture

There are three main big architectural components:

* INAF-OATs cloud site, which EGI federation process is ongoing
* INAF-OATs infrastructure based on IVOA standards and recommendations, powered by CADC open-source software and by a general purpose storage management interface, VOSpace compatible, called VOSpace-backend.
* CANFAR infrastructure based on IVOA standards and recommendations, powered by CADC open-source software plus some proprietary software.

A general and complete picture of the architecture is depicted in figure where the single components, services and tools involved in the demonstrator are pointed out.



**Fig. 2** General architecture of the demonstrator scenario and main involved components

User management and data access community services deployed at INAF-Trieste on EGI FedCloud consists of:

**Access Control Service**: is a client and server authentication and authorization implementation for user and group management, customized during the EGI-Engage project to achieve interoperability between community services geographically distributed. It has LDAP as default persistence layer built-in and it provides a RESTful interface to authentication, authorization and users and groups management.

**Credential Delegation Service**: is a client and server implementation of the IVOA Credential Delegation Protocol. The Credential Delegation Protocol allows a client program to delegate a user's credentials to a service such that that service may make requests of other services in the name of that user. The service provides a RESTful interface.

**Data Storage Service**: is a client and server implementation of a data storage service. It involves two components (both providing a RESTful interface):

**VOSpace**: an implementation of the IVOA VOSpace interface.

**VOSpace** is a lightweight interface to distributed storage specifying how VO agents and applications can use network attached data stores to persist and exchange data in a standard way. It is supposed to sit on top of existing storage solutions and the underlying storage system is not specified.

The CADC implementation of the VOSpace interface is based on a SQL RDBMS where metadata and data access authorization information are stored.

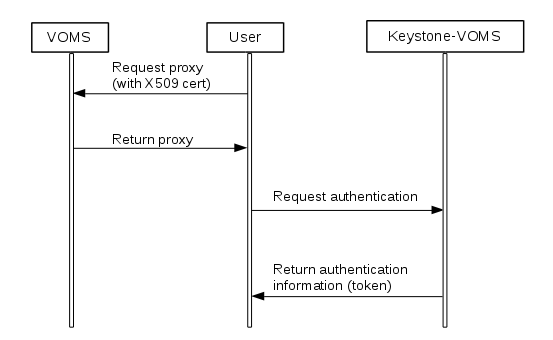
**VOSpace Storage Service**: a plug-in based storage access service, developed during the EGI-Engage project, managing the physical data storage operations satisfying the VOSpace requirements. Currently a posix file system based plug-in has been developed, tested, and made open source available. An OpenStack Swift plugin has been also developed.

User management and data access infrastructure hosted by CANFAR provides the same services and in addition an:

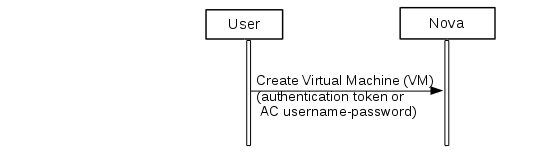
**IVOA Registry** which provides a mechanism with which VO applications can discover and select resources (e.g. data and services).

Both infrastructures provide a cloud portal to exploit all the provided resources. The INAF-OATs cloud site is EGI federated allowing access to all provided services to the EGI community. All the tools and software in Europe are provided as EGI FedCloud A&A Community components.

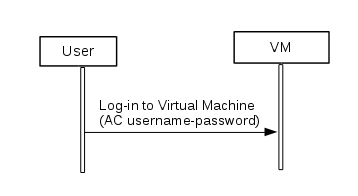
The next figures summarize the main interactions occurring in the demonstrator.



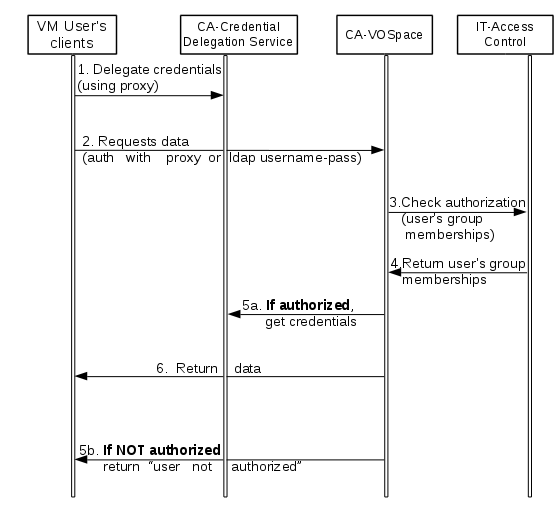
**Fig. 3** User authentication in EGI FedCloud using X509 certificates and VOMS proxies.



**Fig. 4** User creates a virtual machine in the OpenStack cloud querying Nova. The image to be used is provided by the project with specific tools installed and it is registered in the EGI Application Database. The user can authenticate himself using the authentication token or username-password (the same used to access community services -managed by Access Control).



**Fig**. 5 User can log-in to the created virtual machine using username-password used to access community services -managed by Access Control.



**Fig.6** Data sharing interoperability use case main interactions.

### Detailed Implementation

During the EGI-Engage project, an infrastructure, twin of the CANFAR one, has been deployed at OATs-INAF. This infrastructure is a link between the CANFAR infrastructure and the EGI FedCloud as it provides a set of services for A&A community completely interoperable with the CANFAR services, thanks to the IVOA standards implementation, and, on the same time, it is accessible by the EGI users because exploitable through EGI infrastructure and sites.

To achieve this result, all the services described below, based on the CADC open source software distribution, have been modified and extended to deploy the interoperable infrastructure, in particular: the access control has been modified to allow interoperability between different access control service installations geographically distributed. The VOSpace interface implementation authorization mechanism has been modified to take into account the fact that users registered in more than one access control services can ask access and that they have a X509 certificate with VOMS extensions (that are transparent to the CANFAR Service). All the services have been adapted to be more configurable and deployable out of the box.

#### Access Control software description

The Access Control is a client and server authentication and authorization implementation for users and groups management.

It contains four modules:

1. **cadc-access-control**: Access control clients and common model objects and exceptions. This module contains the shared model classes and exceptions used by the access control clients and server. It also contains the user and group management service clients.
2. **cadc-access-control-admin**: Administrative tool for managing users. This module provides a command line tool for managing users. It uses the persistence layer code (rather than the web service) for the various functions.
3. **cadc-access-control-server**: Access control web service implementation. It provides a RESTful interface to authentication, authorization and users and groups management. There are three software layers:
   * The action classes - these coordinate the functions of the REST API
   * The persistence layer - Authorization and connection management
   * The DAO layer - interface to persistent storage

cadc-access-control-server has a default LDAP persistence layer built-in. However, by implementing the Persistence and DAO interfaces, one can easily configure this service to communicate with a different storage mechanism (such as a relational database).

1. **cadc-access-control-identity**: Access control web service client implementation to discover all the identities of a user.

When the cadc-access-control-identity jar file is in the classpath of any of the web services offered in opencadc, it will, upon entry into the web service, make a call to the cadc-access-control-server service to discover all the identities of the user making the initial web service call. We call this subject augmentation. These identities are available for use by downstream code for purposes such as authentication decisions and logging. Without the cadc-access-control-identity jar file, web services only know about the identity which the user used to connect to the web service (a cookie value for example). With the jar file, web service will know about the other identities for the user, such as username, X.509 distinguished name, and potentially various external identity provider information. Additionally, this information allows services to call other community services as the user by making use of the credential delegation service.

1. **cadc-tomcat**: Tomcat 7 authentication realm implementation plugin to manage username-password authentication based on the Access Control web service.
2. A SSL plugin, provided by EGI, to enable x509 Client Certificates to work directly with tomcat

#### Credential Delegation Protocol software description

The Credential Delegation Protocol (cdp) module is a client and server implementation of the IVOA Credential Delegation Protocol.

It contains two main modules:

1. **cadc-cdp**: Credential Delegation Protocol clients and common model objects and exceptions.
2. **cadc-cdp-server**: Credential Delegation Protocol server and common model objects.

#### VOSpace software description

The VOSpace (vos) module is a client and server implementation of the IVOA VOSpace Interface standard.

It contains two main modules:

1. **cadc-vos**: VOSpace clients and common model objects and exceptions.
2. **cadc-vos-server**: VOSpace server and transfer service.

#### VOSpace-backend software description

The vospace-backend software is a RESTful web service implementation providing a storage service management to interface a VOSpace interface implementation with a storage solution. Main features of this service:

* provides an implementation of VOSpace Node persistence:

|  |
| --- |
| cadc-vos-server/src/main/java/ca/nrc/cadc/vos/server/DatabaseNodePersistence.java |

* provides an implementation of UWS Job persistence:

|  |
| --- |
| uws/cadc-uws-server/src/main/java/ca/nrc/cadc/uws/server/DatabaseJobPersistence.java |

* provides an implementation of a transfer generator service:

|  |
| --- |
| cadc-vos-server/src/main/java/ca/nrc/cadc/vos/server/transfers/TransferGenerator.java |

An interface to the VOSpace storage back-end for provided transfer details during the transfer negotiation process. Given the transfer details, this implementation returns a list of URLs to support the most general use case in which the storage system has multiple copies of a file or multiple locations in which a file can be saved. Returning only one URL in the list is a perfectly normal response though.

* has a plug-in architecture allowing to load at run-time a configurable physical storage support, simply implementing the abstract class

|  |
| --- |
| vospace-backend/blob/master/src/main/java/it/inaf/oats/  vospacebackend/implementation/VOSpaceBackend.java |

* the current vospace-backend implementation provides a posix filesystem based storage plug-in, as an example, and an OpenStack Swift plug-in is also available.

#### Services URLs

Services involved in the demonstrator:

* At INAF-OATs:
  + <https://gms01.oats.inaf.it/ac/capabilities>
  + <https://gms01.oats.inaf.it/cred/capabilities>
  + <https://space01.oats.inaf.it/vospace/capabilities>
* At CANFAR:
  + <http://apps.canfar.net/ac/capabilities>
  + <http://www.canfar.phys.uvic.ca/cred/capabilities>
  + <https://www.canfar.phys.uvic.ca/vospace/capabilities>

## Demonstration

### Scenario

The main goal of the demo is to proof that the implementation allows to achieve complete interoperability of distributed data access services in a transparent way from the user's point of view. This goal achievement is proved using a   geographically distributed environment based on two data access infrastructures: the first one located at INAF-OATs, in Italy (Europe) and the second one located at CANFAR in Canada. Use case description:

Landscape:

* Two Astronomers working on the same project, one located at CANFAR and the other one located at INAF-OATs want to share data.
* Astronomer A, PI of the project, has an account both at CADC and OATs and a space allocation (a folder) at CADC
* Astronomer B has an account at INAF-OATs only, i.e. astronomer B has an account at INAF-OATs being registered in the INAF-OATs Access Control service
* Astronomer A shares data with Astronomer B in his CANFAR located space allocation

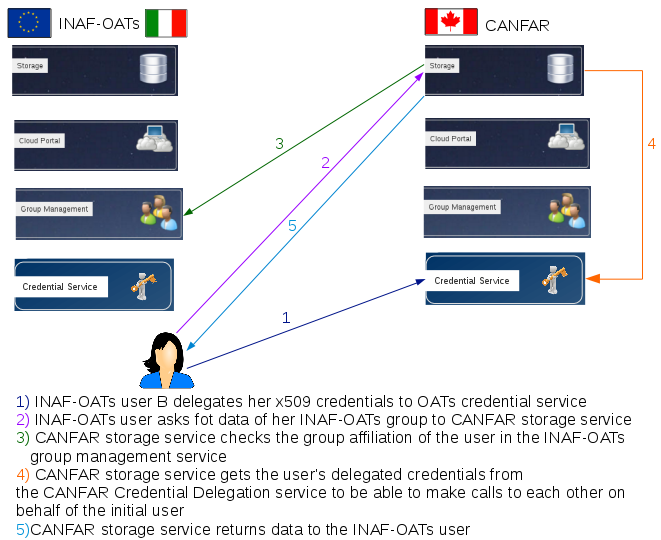
Interoperability requirements:

* Astronomer A must create a project group in the INAF-OATS users and groups management (access control service)
* Astronomer A must assign Astronomer B membership to the project group in the INAF-OATS users and groups management (Access Control service)
* Astronomer A must add group-write permission to his CADC folder at the project group existing in the INAF-OATs Access Control service

At this point, the Astronomer B (an INAF-OATs infrastructure user) is authorized to access data.

To download a file from the Astronomer A folder located at CANFAR and shared with the project group,

* Astronomer B is authorized to download a file from the user A folder CANFAR located.



**Fig.7** Data sharing interoperability steps to perform

Authorization steps (see figure):

* Astronomer B asks CANFAR storage service to download the file, CANFAR storage service checks file access permissions, receiving a list of groups having access rights. **The group names are indicated using a “special” identifier containing the information to know which Access Control service manages this group.** CANFAR storage service asks to the group origin access control service if the querying Astronomer B is known and his groups memberships. If the user is known and member of a group having access rights,
* CANFAR storage service gets from the CANFAR Credential Delegation service the Astronomer B credentials
* Using these credentials, the CANFAR storage service returns the required file to Astronomer B
* Using the same credential (X509 certificate), the Astronomer B is able to instance a VM configured with data reduction and analysis software. To interact with EGI services and sites the Astronomer B must be a valid member of a VO (e.g. planck, astro.vo.eu-egee.org). The VM is configured so that all the general purpose software available for astronomers (Scisoft, IRAF, MIDAS, Astropy, DS9, cfitsio and more) is installed and properly configured.
* The VMs has been configured so that the username/password used by the Access Control can also be used to login (no ssh public key is required). The Access Control and the VM are sharing the same external users database (the VM does not contain any form of credential, such as passwords or private keys). The VM also host the EGI FedCloud Astronomy Community service clients, in particular the user can mount the VOSpace (both the CANFAR one or the EGI one) to further use the A&A software on a Posix filesystem.

### Service Demonstrator

* Practical use case demonstration:
* User A needs his access credentials. He has to create an rfc VOMS proxy starting from his X509 certificate. X509 certificates are the authentication method common to CANFAR and EGI allowing a uniform authentication in the two infrastructures. The only difference is that CANFAR did not adopt VOMS, but supports general proxy (including voms proxy) authentication, EGI supports VOMS for authorization. For this reason, it is irrelevant for CANFAR that an Astronomer is using a VOMS virtual organization, however it is absolutely necessary for EGI otherwise the user will not be able to access any EGI service. A CANFAR astronomer that wants to use an EGI service must register to an EGI VO, in this example to planck one.

The voms proxy can be obtained with the command:

|  |
| --- |
| voms-proxy-init -voms planck --hours 2100 -rfc |

The x509certificate (cert and key) must be located in /home/userA/.globus directory

* User A creates a collaboration folder where to load the data to share:

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main --cert=$X509\_USER\_PROXY  --create=ContainerNode  --target=vos://cadc.nrc.ca\!vospace/userA/data\_share |

* User A loads the data to be shared:

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main \  --cert=$X509\_USER\_PROXY \  --copy \  --src=/home/bob/shared\_file.tar \  --dest=vos://cadc.nrc.ca\!vospace/userA/data\_share/shared\_file.tar |

* User A creates a collaboration group in the INAF-OATs Access Control Service:

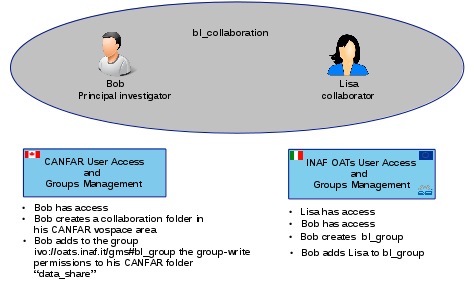
|  |
| --- |
| java ca.nrc.cadc.ac.client.Main \  --cert=$X509\_USER\_PROXY \  --create \  --group=ivo://oats.inaf.it/gms?AB\_group |

* User A adds Lisa as member of the collaboration group:

|  |
| --- |
| java ca.nrc.cadc.ac.client.Main \  --cert=$X509\_USER\_PROXY \  --add-member \  --group=ivo://oats.inaf.it/gms?AB\_group  --userid=userB |

* User A grants write access to the share\_data folder to the collaboration group:

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main \  --cert=$X509\_USER\_PROXY \  --set  --target=vos://cadc.nrc.ca~vospace/bob\_space/data\_share  --group-write=ivo://oats.inaf.it/gms#AB\_group |



**Fig.8** Data management interoperability use case description

At this point data can be shared: user B can access user A’s data at CANFAR, download them, analyze them and, if required, upload the result in the CANFAR share area to share results with User A.

All these tasks can be performed exploiting the INAF-OATs cloud infrastructure, both using command line and OpenStack Horizon user interface (available at <https://cloud.oats.inaf.it>). In this demonstrator the command line is used:

* User B needs his access credentials. He has to create an rfc VOMS proxy starting from her X509 certificate with the command:

|  |
| --- |
| voms-proxy-init -voms planck --hours 2100 -rfc |

The x509certificate (cert and key) must be located in /home/userB/.globus directory

* User B can use his VOMS credentials to access the INAF-OATs cloud. He creates an identity token:

|  |
| --- |
| curl --cert $X509\_USER\_PROXY -d '{"auth":{"voms": true, "tenantName": "planck"}}' -H "Content-type: application/json" https://cloud.oats.inaf.it:5000/v2.0/tokens | python -m json.tool |

* User B uses the identity token to connect to the OpenStack console

|  |
| --- |
| openstack --os-auth-type token --os-auth-url https://cloud.oats.inaf.it:5000/v2.0 --os-project-name planck --os-token $TOKEN\_ID |

* User B can now list available images, flavours, networks and to create a Virtual Machine, using an image (canfarprod) created by the collaboration and providing clients to access and manage CANFAR and INAF-OATs services:

|  |
| --- |
| (openstack) image list  +---------------------------------------------------+---------------------------------+----------+  | ID | Name | Status |  +---------------------------------------------------+---------------------------------+----------+  |  | 1feb7485-99ea-4769-b743-f769b38352d3 | CentOS 7.4 x86\_64 | active |  | 3bc3c9e2-ea32-4c32-baa4-b5526e0fa268 | EGI FedCloud Appliance | active |  | dc1672fc-d948-4c99-b098-d6a2bea1d735 | canfarprod | active |  | e84156bf-3c86-4fb1-a86d-a2ec1a2e9088 | fedora20 | active |  +--------------------------------------------------+---------------------------------+----------+  (openstack) flavor list  +--------+------------------+--------+------+---------------+---------+------------+  | ID | Name | RAM | Disk | Ephemeral | VCPUs | Is Public |  +--------+------------------+--------+------+---------------+---------+------------+  | 0 | oats.large | 40960 | 40 | 0 | 8 | True |  | 1 | m1.tiny | 512 | 1 | 0 | 1 | True |  | 2 | m1.small | 2048 | 20 | 0 | 1 | True |  +--------+------------------+--------+------+---------------+---------+------------+  (openstack) network list  +----------------------------+------------+---------------------------------+  | ID | Name | Subnets |  +----------------------------+------------+---------------------------------+  | xxxxxxxxxxxxxxxxxx | ext-net | \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |  | yyyyyyyyyyyyyyyyyy | oats\_net | \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |  | zzzzzzzzzzzzzzzzzzzzz | egi01 | \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |  +----------------------------------------+----------+------------------------+  (openstack) server create --flavor m1.medium --image "canfarprod" --nic net-id=zzzzzzzzzzzzzzzzzzzzz --security-group default --key-name egi-sshkey --user-data mydata.cfg canfar-prod  > cat mydata.cfg  #cloud-config  ssh\_authorized\_keys:  - ssh-rsa AAAB3NzaC1yc2EAAAAB…H5qV7NZ mykey@host |

The file mydata.cfg is a cloud-init file used to configure the Virtual Machine to allow the user B to use the same username-password credentials used to log-in in the INAF-OATs Access Control service.

Now user B can use the created virtual machine in two ways:

* accessing the console using the URL displayed with:

|  |
| --- |
| (openstack) console url show canfar-prod  +-------+--------------------------------------------------------------------------------------+  | Field | Value | |-------+--------------------------------------------------------------------------------------+  | type | novnc |  | url |https://140.xxx.xx.xxx:6080/vnc\_auto.html?token=TOKEN\_ID |  +-------+--------------------------------------------------------------------------------------+ |

* Assigning a floating IP to the machine and logging with ssh connection using the same username-password credentials used to log-in in the INAF-OATs Access Control service.

|  |
| --- |
| (openstack) ip floating list ext-net  (openstack) floating ip create ext-net  (openstack) server add floating ip canfar-prod 140.xxx.xx.xxx |

When logged-in, the user B can use the provided clients to get shared data.

* User B has to delegate her credentials to the CANFAR credential service:

|  |
| --- |
| java ca.nrc.cadc.cred.client.Main \  --cert=$X509\_USER\_PROXY \  --resourceID=ivo://cadc.nrc.ca/cred \  --delegate \  --daysValid=31 |

* User B downloads data shared by User A:

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main \  --cert=$X509\_USER\_PROXY \  --copy \  --src=vos://cadc.nrc.ca\!vospace/userA/data\_share/shared\_file.tar \  --dest=/home/userB/shared\_file.tar |

User B is ready to exploit shared data, he can analyse them using INAF-OATs VM provided tools. After elaboration, results can be uploaded into the shared area at CANFAR:

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main \  --cert=$X509\_USER\_PROXY \  --copy \  --dest=/home/userB/results\_to\_share.tar \  --src=vos://cadc.nrc.ca\!vospace/userA/data\_share/results\_to\_share.tar |

### Feedback

The demonstration has been done in two different occasion to a wide A&A audience, and some important feedback has been collected.

In the Framework of ASTERICS project we involved CTA and SKA users. The SKA authentication and authorization community has been involved in testing Access Control functionalities and VOSpace authorization mechanisms. SKA is now evaluating the tools and software presented and the Cloud Infrastructures. In the environment of Euclid[[10]](#footnote-10) project, interest has been expressed in using these technologies exploiting VOSpace interfaces for data movement and to have/bring data close to computation resources. In particular, our demonstrator triggered a discussion on the technical solutions to access data when the proprietary period is expired (how to allow Astronomer not directly involved in Euclid to profit of data).

In the IVOA environment discussions have been stimulated to

* deep the Single Sign-on (SSO)[R5] discussion, with special interest in identifying technologies to implement SSO authentication not only for web based applications (like e.g. SAML) but also for command line applications, which are the most common for data reduction;
* clarify the opportunity to use the group membership as base of the authorization policies and the usability of nested groups to increase the authorization mechanism granularity.

On the other hand some comments has been done on the use of X509 certificates, the authentication through X509 certificates is not well accepted by Astronomers.

This method has been used in the demonstrator for two reasons:

1. it is already supported both by CANFAR infrastructure and EGI FedCloud, and so speeding up the authentication integration task and being the best fitting solution with the project schedule and resources.
2. It can be used not only for web-based authentication (like for example SAML), but also for off-line applications. This is an important A&A community use case, e.g. in the astronomical data pipelines management.

In a short term vision, this issue will be addressed because all the services support different types of identities (e.g. x509 cert identity and login-password identity, SAML), so the user can use the login-password identity until the software manages the x509 identity automatically behind the scenes. This is already implemented in the CANFAR infrastructure. On the long term, we are planning to implement the EGI CheckIn service to allow users to use their preferred authentication method.

The Access Control service and the proposed group based authorization policy management has been welcomed as a good solution to fit the A&A data centers access policies. At the same time, this solution has opened a discussion on the opportunity to support the “group of groups” use case and on the need to provide an authorization information exchange to make possible the use of different group management services (requirement of grouper users).

The idea to provide and share a Virtual Machine specific for the A&A community specific needs has been welcomed. The use of containers for the same scope has been suggested, in conjunction with tools for scientific computing like Jupiter to make easier the computation tasks.

The community has suggested the use of pre-configured containers to facilitate the deployment of community services. This is envisaged as a good mechanism to enhance the adoption of the software in the astronomical data centers.

## Future plans

The demonstrator presents a pre-production environment that has been setup during the EGI-Engage project. The federated infrastructure is under continuous development on both sides (EGI and CANFAR), in particular from the EGI side we are working on the full implementation of EGI CheckIn with the Access Control components. CANFAR is now evaluating OneData as a distributed filesystem to substitute their current implementation. This will allow a new setup involving a larger number of EGI Services.

To simplify the demonstrator setup we will port the services deployment procedure in a container environment based on docker. Some pilot study/test has been done to use docker or singularity as technical solution to provide services deployed in containers, but the finalization of this task requires more development and test work.

A work on VOSpace to VOSpace high performance data movement could speed up the data exchange between infrastructures.

The development and testing activities will continue in the framework of the ASTERICS project for the aspects related to SSO and authorization mechanisms. The standardisation activity, particularly regarding the grouping and authorization aspects, will be carried on in the framework of the IVOA projects.

# Conclusions, lessons learnt, future work

A great deal of work has been done to achieve interoperability of two geographically distributed infrastructures based on the open-source software provided by CADC and on the EGI services. The configurability and deployability out of the box of the CADC open-software API implementations have been greatly improved. The work done has been documented to allow its reproducibility, with the scope to ease the adoption of these technologies. Our target is to allow data centres and A&A experiments to benefit of the EGI FedCloud services and technologies thanks to a set community specific services based on A&A reference standards. On the other hand, large scale experiments that involved different infrastructure all over the world may adopt our setup as a starting point to support A&A community on a large scale.

This work has been also extremely useful for the A&A technology providers and community, triggering discussion and standard development at different levels.

In the IVOA framework, this work opens the discussion on the use of AAI for accessing data and computing and on the necessity to move computation close to data. In this pilot, the interoperability of different infrastructures has been obtained introducing specific features, like, for example, the use of an IVOA-like annotation for the group name

|  |
| --- |
| ivo://<authority>/gms?groupY |

The presence of the <authority> in the group name allows the services to know which Access Control to query to have information on the group. At present this is not an IVOA standard or recommendation, but its use is under discussion with the group management and the use of group memberships to manage data access authorization.

The use of the ‘--resourceID’ parameter in the Credential Delegation Client has been introduced. In the original CADC open-source software this parameter was not present and the credential delegation client was able to query only one credential delegation service previously configured. With the introduction of this parameter, the user can delegate his credential to the credential delegation service “associated to” the VOSpace where he intends to upload/download data (which means the credential delegation service that will be queried by the VOSpace service to get the user credentials).

This opened a discussion, between developers, but at IVOA level also, on how to make available the information on the associated credential delegation service to be able to later query the specific VOSpace. The first proposed solution is to publish in the service capabilities the reference credential delegation service.

As a future plan, we will work to finalize the discussion inside the IVOA community to provide an Authorization profile based on group management standard, involving EGI and EGI AAI work as an example.

We will also provide developers with simple guidelines and possibly a very simple tutorial implementation, on how to develop and deploy a completely interoperable VOSpace on top of EGI FedCloud.

As there was an expression of interest on this activity from the ViaLactea EU project, in the next months we will focus on the integration of ViaLactea data and applications and in particular on the integration of a “cut out” service that works on VOSpace stored data both in EGI and in CANFAR.

SKA is now evaluating the Access Control and GMS as a possible solution for the authorization in SKA Observatory. We will support SKA in this evaluation procedure, and eventually extend this work also in the framework of AENEAS project aiming at identifying requirements for the European SKA regional centers.

# Plan for Exploitation and Dissemination

|  |  |
| --- | --- |
| ***Name of the result*** | CANFAR/EGI integration |
| ***DEFINITION*** | |
| ***Category of result*** | Software & service innovation |
| ***Description of the result*** | Integration of CANFAR and EGI through INAF, the Italian National Institute for Astrophysics, towards a seamless and uniform platform for international astronomy research collaboration. |
| ***EXPLOITATION*** | |
| ***Target group(s)*** | RIs, international research collaborations and the long-tail of science, service providers (e.g. the astronomical data centres in Europe, SKA, CTA, etc.) |
| ***Needs*** | The need is to offer to the A&A community an easy and transparent access to the CANFAR data archives from Europe, specifically using the EGI infrastructure. This infrastructure must provide easy access and tailored tools. |
| ***How the target groups will use the result?*** | In further research activities other than those covered by the project concerned. The target groups can install and configure a collaboration infrastructure for astronomy using the software and documentation produced inside the EGI-Engage project, offering a community specific collaboration environment based on astronomical standards. |
| ***Benefits*** | The adoption by European Astronomical Data Centers of standards of reference for the Astronomical Community proposed by the IVOA for data access and standards developed by EGI for cloud access, monitoring and VMs share, will allow A&A users to access astronomical data sets, tools and resources available worldwide in a transparent way.  The platform aims at facilitating the access to data and computing resources adopting standards interfaces towards EGI cloud. |
| ***How will you protect the results?*** | Open Source License (GPL v3) |
| ***Actions for exploitation*** | Actions for exploitation are the provisioning of packaged containers to ease the installation of the community services and to provide the tailored tools for astronomical data reduction/analysis. When containers will be ready, the administrators and users documentation must be accordingly updated. |
| ***URL to project result*** | <https://github.com/opencadc>  <https://github.com/oats-cadc>  <https://www.ict.inaf.it/gitlab/OATS-CADC> |
| ***Success criteria*** | The short term success criteria for the demonstrator is the ability to be a driver for new technical discussion, new standards adoption and new users and developers’ engagement in EGI and IVOA.  The long term success criteria is a wide adoption of proposed tools and the increasing of the EGI community users. |
| ***DISSEMINATION*** | |
| ***Key messages*** | *What messages will you tell to the target groups when informing about the results?*   * A new set of services for the A&A community is available in the EGI infrastructure * Through these services astronomical data and computations resources (VMs) can be shared using IVOA standards and EGI Federated Cloud services * Software, documentation and support are available to deploy new cloud sites including A&A specific community services. * The new set of EGI provided services are interoperable with the CANFAR infrastructure |
| ***Channels*** | Participation in conferences, workshops and technical meetings |
| ***Actions for dissemination*** | Presentation at European and international workshops that involves projects and data center:   * IVOA Interop, * ASTERICS tech forum (March 2017), * SKA TM meetings, * AENEAS project Meetings, * VO Road shows * EGI Conference 2017 |
| ***Cost*** | *The estimated costs for the conferences, workshops and technical meeting mentioned as dissemination channels is around 10.000 euros* |
| ***Evaluation*** | The impact of the dissemination actions will be evaluated in terms of involved users and projects, new standards outcomes and proposed solutions adoption. |

# References

|  |  |
| --- | --- |
| ***No*** | ***Description/Link*** |
| R1 | VOSpace specification Version 2.0  <http://www.ivoa.net/documents/VOSpace/20130329/index.html> |
| R2 | IVOA Support Interfaces  <http://www.ivoa.net/documents/VOSI/index.html> |
| R3 | The universal worker service  <http://www.ivoa.net/documents/UWS/index.html> |
| R4 | Credential delegation protocol  <http://www.ivoa.net/documents/CredentialDelegation/> |
| R5 | SSO profile  <http://www.ivoa.net/documents/latest/SSOAuthMech.html> |
| R6 | Filesystem in Userspace (FUSE)  <http://fuse.sourceforge.net> |
| R7 | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile  <https://tools.ietf.org/html/rfc5280> |

# Appendix: Command line interface, Web Gui

**User Registration and management**

CANFAR Access Control Service provides the ability to manage

* user management
* user’s credentials verification and access management.

Different kinds of identities are supported:

* + X509 credentials
  + user-password credentials
  + Cookies identification
* Groups management including
  + group creation
  + group members’ assignment
  + group administrator assignment
  + group membership verification
  + group details display
  + group listing

The CADC Access Control open-source software is provided with a java client interface, or it can be queried exploiting its restful interface. The most common commands used to manage users are described below.

### Users registration and management

A new use registration requires an XML user description. Example:

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?>  <userRequest>  <password>\*\*\*\*\*\*\*\*\*</password>  <user>  <identities>  <identity type="HTTP">new\_user\_nickname</identity>  </identities>  <personalDetails>  <userName>UserName</userName>  <firstName>UserFirstName</firstName>  <lastName>UserLastName</lastName>  <email>UserFirstName.UserLastName@my.domain.org</email>  <address>User’s Institution address</address>  <institute>User’s Institution</institute>  <city>User’s Institution City</city>  <country>User’s country</country>  </personalDetails>  </user>  </userRequest> |

User registration request (RESTFul call):

|  |
| --- |
| curl -v -T newUserDescription.xml "AccessControlService.url/UserServlet" |

User management operations can be done by authenticated users. In this example the user authenticate himself through X509 credentials, the same credentials used to access the INAF-EGI FedCloud site.

Pending registration requests can be listed:

|  |
| --- |
| java ca.nrc.cadc.ac.admin.Main --list-pending --cert=$X509\_USER\_PROXY |

A new user registration request must be accepted or rejected by an authorized user (recognized by his x509 certificate):

* New user accept

|  |
| --- |
| java ca.nrc.cadc.ac.admin.Main --approve=new\_user\_nickname  --dn=uid=new\_user\_nickname,ou=Users,ou=dc,dc=oats,dc=inaf,dc=it  --cert=$X509\_USER\_PROXY |

where dn=distinguished name of the user

* New user reject

|  |
| --- |
| java ca.nrc.cadc.ac.admin.Main --reject=new\_user\_nickname --cert=$X509\_USER\_PROXY |

Registered users can be listed:

|  |
| --- |
| java ca.nrc.cadc.ac.admin.Main --list --cert=$X509\_USER\_PROXY |

### User’s credentials verification and access management.

The data access is granted based on:

* user credential verification
* user group membership

The user credential verification is performed by the Access Control Service which is able to recognize

* X509 certificates and proxies
* user-password identity
* cookies

When a user is recognized, the group membership is verified querying the right Access Control service with this mechanism:

The meta-data associated to data contain information if the data is public or not. If not, the information about groups having read and write permissions is present. The software checks groups having permissions, the group name contains the authority hosting each group, the software can find each group members with an https query:

|  |
| --- |
| https://access-control-host.authority-domain/ac/search?&ROLE=member&GROUPID=groupX |

At this point all data to assign access rights are available.

### Groups management

* Create a group

|  |
| --- |
| java ca.nrc.cadc.ac.client.Main  --create  --group=ivo://<authority>/gms?groupX  --cert=$X509\_USER\_PROXY |

* Add a group member

|  |
| --- |
| java ca.nrc.cadc.ac.client.GMSClientMain  --add-member  --group=ivo://<authority>/gms?groupX  --userid=userA  --cert=$X509\_USER\_PROXY |

* Remove a group member

|  |
| --- |
| java ca.nrc.cadc.ac.client.GMSClientMain  --remove-member  --group=ivo://<authority>/gms?groupX  --userid=userA  --cert=$X509\_USER\_PROXY |

* Delete group

|  |
| --- |
| java ca.nrc.cadc.ac.client.GMSClientMain  --delete  --group=ivo://<authority>/gms?groupX  --cert=$X509\_USER\_PROXY |

* Add group admin

|  |
| --- |
| java ca.nrc.cadc.ac.client.GMSClientMain  --add-admin  --group=ivo://<authority>/gms?groupY  --userid=userB  --cert=$X509\_USER\_PROXY |

* Remove group admin

|  |
| --- |
| java ca.nrc.cadc.ac.client.GMSClientMain  --remove-admin  --group=ivo://<authority>/gms?groupY  --userid=userB  --cert=$X509\_USER\_PROXY |

### Delegations management

The IVOA credential delegation protocol allows a client program to delegate a user's credentials to a service such that that service may make requests of other services in the name of that user.

Available delegation functions:

* create new proxy certificate on the server:

|  |
| --- |
| java ca.nrc.cadc.cred.client.Main  --delegate  --daysValid=1  --resourceID=ivo://<authority>/cred  --cert=$X509\_USER\_PROXY |

* get a new proxy certificate from the server, using both userid and userdn:

|  |
| --- |
| java ca.nrc.cadc.cred.client.Main  --get  --userid=sabe  --resourceID=ivo://<authority>/cred  --cert=$X509\_USER\_PROXY |

* view the currently deleagted proxy certificate:

|  |
| --- |
| java ca.nrc.cadc.cred.client.Main  --view  --resourceID=ivo://<authority>/cred  --cert=$X509\_USER\_PROXY |

### VOSpace service client

Main VOSpace client features:

* Upload a file to VOSpace:

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main  --copy  --src=<local\_path\_of\_file>  --dest=vos://<authority>!vospace/<path\_of\_node>  --cert=$X509\_USER\_PROXY |

* Download a file from VOSpace:

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main  --copy  --src=vos://<authority>!vospace/<path\_of\_node>  --dest=<local\_path\_of\_file>  --cert=$X509\_USER\_PROXY |

* View a node (file or folder):

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main  --view  --target=vos://<authority>!vospace/<path\_of\_node>  --cert=$X509\_USER\_PROXY |

* Create a folder

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main  --create  --target=vos://<authority>!vospace/<path\_of\_node>  --cert=$X509\_USER\_PROXY |

* Move a file

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main  --move  --src=vos://<authority>!vospace/<path\_of\_src\_node>  --dest=vos://<authority>!vospace/<path\_of\_dest\_node>  --cert=$X509\_USER\_PROXY |

* Delete a file

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main  --delete  --target=vos://<authority>!vospace/<path\_of\_node>  --cert=$X509\_USER\_PROXY |

* Change file permissions

|  |
| --- |
| java ca.nrc.cadc.vos.client.Main  --set  --target=vos://<authority>!vospace/<path\_of\_node>  --group-write=ivo://<authority>/gms?groupY  --cert=$X509\_USER\_PROXY  java ca.nrc.cadc.vos.client.Main --set  --target=vos://<authority>!vospace/<path\_of\_node>  --group-read=ivo://<authority>/gms?groupX,ivo://<authority>/gms?groupY  --cert=$X509\_USER\_PROXY |

# Appendix: Manuals and Documentation

OATS-CADC collaboration documentation source repository:

<https://github.com/oats-cadc>

Modules (containing guides source files):

* + - Access Control service administrators’ guide source   
      <https://github.com/oats-cadc/oats-ac-admin-guide>
    - Credential Service administrators guide source

<https://github.com/oats-cadc/oats-cred-admin-guide>

* + - VOSpace service administrators guide source

<https://github.com/oats-cadc/oats-vospace-admin-guide>

* + - VOSpace backend service administrators guide source   
      <https://github.com/oats-cadc/oats-vospace-backend-admin-guide>
    - Access Control service users guide source

<https://github.com/oats-cadc/oats-ac-users-guide>

* + - Credential Service users guide source

[https://github.com/oats-cadc/oats-cred-users-guide](https://github.com/oats-cadc/oats-vospace-admin-guide)

* + - VOSpace service users guide source

<https://github.com/oats-cadc/oats-vospace-users-guide>

* + - VOSpace back-end developers guide source

[https://github.com/oats-cadc/oats-vospace-developers-guide](https://github.com/oats-cadc/oats-vospace-users-guide)

* OATS-CADC collaboration on-line documentation summary:

<http://gms01.oats.inaf.it/doc/index.html>

* Guides:
  + Access Control service administrators’ guide

<http://gms01.oats.inaf.it/doc/ac-admin/index.html>

* + Credential Service administrators guide

<http://gms01.oats.inaf.it/doc/cred-admin/index.html>

* + VOSpace service administrators guide

<http://gms01.oats.inaf.it/doc/vospace-admin/index.html>

* + VOSpace backend service administrators guide

<http://gms01.oats.inaf.it/doc/vospace-backend-admin/index.html>

* + Credential Service users guide

<http://gms01.oats.inaf.it/doc/cred-users-guide/index.html>

* + VOSpace Service users guide

<http://gms01.oats.inaf.it/doc/vospace-users-guide/index.html>

* + Access Control Service users guide

<http://gms01.oats.inaf.it/doc/ac-users-guide/index.html>

* + VOSpace backend developers guide   
    <http://gms01.oats.inaf.it/doc/vospace-backend-devel-guide/index.html>

1. <http://www.canfar.net> [↑](#footnote-ref-1)
2. <https://www.canarie.ca/about-us/> [↑](#footnote-ref-2)
3. <https://www.computecanada.ca/about/> [↑](#footnote-ref-3)
4. <http://www.cadc-ccda.hia-iha.nrc-cnrc.gc.ca/en/> [↑](#footnote-ref-4)
5. <https://appdb.egi.eu/> [↑](#footnote-ref-5)
6. <https://www.asterics2020.eu/dokuwiki/doku.php?id=open:wp4:wp4techforum3> [↑](#footnote-ref-6)
7. <https://indico.egi.eu/indico/event/3249/session/61/?slotId=0#20170510>

   <https://indico.egi.eu/indico/event/3249/timetable/#20170510> [↑](#footnote-ref-7)
8. <http://ivoa2017shanghai.csp.escience.cn/dct/page/1> [↑](#footnote-ref-8)
9. <http://wiki.ivoa.net/twiki/bin/view/IVOA/InterOpMay2017-GWS> [↑](#footnote-ref-9)
10. <https://www.euclid-ec.org> [↑](#footnote-ref-10)