XSEDE Capability Delivery Plan
IDM-13 - Authenticate to XSEDE OpenStack APIs
Last revised 2017-11-16

Background

Use cases describe community needs, requirements, and recommendations for improvements to cyberinfrastructure (CI) resources and services. A Capability Delivery Plan (CDP) is an executive summary of the current gaps in our support for a use case, current plans to fill those gaps with new or enhanced capabilities, and the operational components that currently support the use case.

Use case summary

Use case IDM-14 describes how application and science gateway developers would like to use their XSEDE identities to authenticate to the APIs offered by an XSEDE OpenStack resource. The full description of this use case is available in the CSR's use case registry.

Currently, developers who use OpenStack APIs on XSEDE systems authenticate using resource-specific credentials issued by the resource provider. They can't use their XSEDE identities or XSEDE's public authentication service to perform this authentication. Creating and issuing these credentials is a chore for resource providers and a nuisance for the developers.

CDP summary

The XSEDE system doesn't currently support this use case as described. Two critical components are in place: the XSEDE User Portal (XUP), where educators and their students can register with XSEDE and obtain XSEDE ID/passwords; and Globus Auth, an OIDC-based public authentication service intended to enable XSEDE authentication to external services, such as those described in this use case. What is currently missing is the ability to use Globus Auth to authenticate SSH connections.

Gap(s) that we currently plan to address:

- Using Globus Auth with OpenStack Keystone
- Mapping XSEDE to OpenStack identities

Gap(s) that will not be addressed at this time:

- None

Time and effort summary:

- **4 person-weeks** of effort, performed jointly with the IU/TACC Jetstream team with possible contribution from the PSC Bridges team
  - Test use of OpenID Connect with Keystone: 1 person week
  - Document Keystone configuration and Globus Auth API/SDK for developer use: 1 person week
  - Generalize Jetstream's XSEDE/OpenStack identity mapping: 1 person week
  - Document Keystone configuration for XSEDE identity mapping: 1 person week

Functionality gaps

1. Using Globus Auth with OpenStack Keystone (suggested priority: medium)

The OpenStack APIs use OpenStack's Keystone for authentication. We do not currently have documentation explaining how to use Globus Auth with Keystone.

Plans: OpenStack's Keystone supports OpenID Connect authentication. This should allow applications that use the OpenStack APIs to use Globus Auth to obtain access tokens for the Keystone server. The tokens will identify the XSEDE user who is authenticating. Applications will be able to request refresh tokens with their Keystone access token that will allow them to refresh the Keystone access token indefinitely. We will test the use of OpenID Connect with Keystone to make sure this works in practice. We will document how resource administrators should configure Keystone and how application developers can use Globus Auth to obtain tokens for use with Keystone.

2. Mapping XSEDE to OpenStack identities (suggested priority: high)

XSEDE authentication via Globus Auth will return an authenticated XSEDE user identity. Authorization in OpenStack is based on tenants, which are locally assigned and managed. The Keystone server for a given resource will need to verify that the authenticated XSEDE identity is associated with the OpenStack tenant specified in the API requests.

Plans: On the IU/TACC Jetstream system, the CyVerse Atmosphere software performs this mapping already. We will generalize the code used by Atmosphere to be usable by the Keystone server and document how to configure Keystone servers to use it.

System components that support this use case

The following XSEDE operational components currently support this use case.

Component	Supported Functionality
OpenStack APIs on SP resources	An API provided by SP cloud resources based on OpenStack that allows programmatic control of the resource subject to locally enforced authorization.
Globus Auth	XSEDE's public authentication interface, based on OpenID Connect (OIDC)
XSEDE User Portal (XUP)	The front-end (web browser-based) user interface to the XSEDE system where individuals register with XSEDE, manage their user profile information, request allocations to use XSEDE SP resources, and manage membership in projects that have active allocations.
XSEDE Central Database (XCDB)	The database that stores all project team membership data, individual user profile data, and active allocation data for XSEDE resources.
AMIE	A messaging system that passes allocation assignments, individual user and project group data, and allocation usage data between XCDB and individual XSEDE resources.