

XSEDE Capability Delivery Plan

UCCAN-3 Remote File Access

Last revised 2016-06-01

Background

Use cases describe community needs, requirements, and recommendations for improvements to cyberinfrastructure “CI” resources and services. Engineers analyze use cases to identify which aspects are supported by production components and which constitute gaps in functionality. A Capability Delivery Plan (CDP) is an executive summary of use case support gaps and plans to fill those gaps with new or enhanced capabilities.

Use Case Summary

Use case CAN-3 (“Canonical 3”) describes how files on remote (non-local) systems can be accessed on a system as if they were in local filesystems. Significant requirements are for integration with XSEDE’s identity and authentication interfaces and the ability to access files from personal (home) systems, campus systems, or other XSEDE systems.

Use case document: <http://hdl.handle.net/2142/45687>

CDP Summary

The functionality described in this use case is fully supported by the operational components listed below.

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

- Accessibility
- Verification of quality attributes

Time and effort summary:

- None at this time

Functionality Gaps

1. Accessibility

One potential issue that is not mentioned in the use case description is the accessibility of these features. These features require installation of GFFS software (part of the Genesis II software suite) on any system from which files must be accessed and on the system where the files are to be accessed. Network connectivity between systems must be provided. (At a minimum, a GFFS

service must be accessible from all of the file hosts and from the accessing system.) In current practice, GFFS software is not pre-installed on all XSEDE resources, nor do all XSEDE resources have full Internet connectivity. GFFS services with full Internet access are available. Genesis II software is not widely pre-installed on campus or home systems, so scientists must download, install, and configure the software themselves. The issues regarding XSEDE resources and network connectivity can be resolved by providing network connectivity between XSEDE resources and XSEDE's GFFS services, though this is something that XSEDE service providers must arrange for themselves and it may be inconsistent with the design of some XSEDE resources. *There are no plans to address this gap.*

2. Verification of quality attributes

Verifying many quality attributes require significant one time and ongoing testing. XSEDE has decided that the costs of this testing would not bring sufficient benefit. Instead XSEDE will monitor user satisfaction, usage, and available performance metrics and address quality issues when raised by users. *There are no plans to address this verification gap.*

System Components That Support This Use Case

The following XSEDE system components currently support this use case.

(Hypelink the component <Name> to the XCSR Component Description Repository)

Component	Supported Functionality
Genesis II client (with GFFS)	Provides both the user interface for accessing files in GFFS and the client and server software for GFFS services. May be installed on end user systems, campus systems, science gateway systems, or XSEDE login servers. Files to be accessed must be present in ("exported to") one or more active (running) GFFS services. Files in GFFS can be accessed on any system with the Genesis II client installed and configured <u>and</u> network connectivity to the GFFS service.
XSEDE WS-Trust STS	Currently in development Translates XSEDE OAuth2 tokens (user identity, group membership) obtained from Globus Auth into the signed SAML chains required by the Genesis II client
Globus Auth	Provides the authentication and authorization services that issue XSEDE user credentials and group membership data, which is in turn used by WS-Trust STS to generate credentials used by Genesis II client