EGI Community Forum 2012

Contribution ID: **56** Type: **not specified**

Federated Access to Data Storage

Tuesday, 27 March 2012 15:00 (30 minutes)

Description of the Work

Moonshot is a set of technology for providing federated access to applications. It uses the Generic Security Services Application Programming Interface (GSS-API) to integrate RADIUS federation into most application protocols. SAML is also fully supported and provides rich attributes to describe federated subjects. Unlike other federation middlewares (e.g., Shibboleth), Moonshot is not tied with the web environment and can be utilized by non-web applications.

The Moonshot architecture is based on open standards and the Moonshot community actively contributes to the IETF. The components implementing the Moonshot architecture have been developed and are available under an open-source license. Moonshot requires changes on the client side and therefore it provides appropriate Linux packages and configurations to make the deployment easy. The Moonshot contributors have also developed a native Windows security support provider (SSP) that implements the Moonshot technology on MS Windows. This allows existing Windows applications to authenticate with Moonshot, which has been showed with e.g. MS Outlook or Internet Explorer.

The Moonshot software stack has proven to be mature enough and has been integrated with a wide range of applications. In this paper we focus on two basic storage services that are widely used—NFSv4 and CIFS. Both these services provide network file systems that can be used by clients to access disk volumes over a network. Nowadays, these systems are used rather in closed environments controlled by a single domain, which is not suitable for grids.

We will demonstrate a prototype extensions to the Samba 4 and NFSv4 file servers that permit the use of any GSS-API mechanism for CIFS/NFSv4 authentication, with Moonshot being such a mechanism. These changes are general enough and we will strive to push them to the upstream code bases. Using these changes it is possible to mount remote “shares” based on federated identities.

Conclusions

In this talk we discuss how to utilize the federated Moonshot authentication infrastructure to authenticate to network filesystems. Moonshot makes it possible to directly use federated identities to mount network shares, without any browser-based applications in between. We will show how the technology work with NFSv4 and CIFS, two major network filesystems used nowadays, along with IGTF certificates and other federated identities.

The architecture is also able to consume additional attributes about users' and we will summarize possibilities how these attributes can be used to control access to files distributed over these protocols.

Using the Moonshot infrastructure and the changes we have made, it is possible to establish a real global filesystem where people can easily yet securely share data based on their federated identities.

Impact

In order to demonstrate the viability of the federated access to data storage we are preparing a NFSv4 server that will be generally available to any user of the world-wide grid community. It will be also available to other users with proper federated identity (which will based on eduroam accounts), but the primary focus will be on grid users using IGTF certificates.

Having federated access to NFSv4 storage will allow users to mount shared directories to their desktop computers and thus easily work with data processed within their virtual organizations. Such a possibility does not exist nowadays and users have to manipulate with the data using some additional tools and services, which adds additional layer in the processing.

For authorization we use common mapping of authenticated users' identities to their unix identifiers. Besides that, we are also exploring the way how additional attributes can be consumed and used for assigning different group memberships. A possibility to add and utilize attributes managed by virtual organizations seems also to be attractive for the users. Therefore, we are working on a mechanism that will make this possible in our pilot environment.

The deployment and first users' experiences with the "gridified" NFSv4 storage will be presented in the talk.

Overview (For the conference guide)

Manipulation with data of different forms is something we do every day. Since data files often contain sensitive information users require they are secured properly. In grids PKI is traditionally used for authentication, however, it does not work with common filesystem like NFSv4 or CIFS. PKI has also a bad reputation in terms of users experience and people try to leverage other authentication mechanisms, like identity federations. Unfortunately, existing identity federations cannot be used smoothly for access to remote filesystems, either.

In this contribution we will demonstrate how the Moonshot federated authentication infrastructure can be utilized to provide easier access to storage systems, where users utilize their home identities to access file systems provided by other institutions. Unlike other solutions, we do not use a web portal or similar "translation" service but allow the users to directly mount remote volumes to their computers.

Primary authors: KOUŘIL, Daniel (CESNET); LUKE, Howard (PADL Software Pty Ltd); MICHAL, Procházka (CESNET)

Presenter: KOUŘIL, Daniel (CESNET)

Session Classification: Data Technologies

Track Classification: Middleware services