

Topic: (De)provisioning connector for services running on Windows OS

Mentor: Slavek Licehammer

Student: Adrian Rosinec

Identity provisioning and deprovisioning are a necessity for building modern authentication and authorization infrastructures. They are straightforward yet technically complicated part of identity and access management. The basic idea is to deliver identity and authorization information to the managed services, which is complicated by a lack of applicable standards in this area. Therefore, most of the Identity and access management solutions rely on a custom solution for provisioning.

Identity and access management components used in GÉANT eduTEAMS are not an exception. Thus they rely on custom connectors to deliver authorization data to managed services, usually utilizing standardized protocols like SSH or LDAP. Although this solution is not technically ideal, it works for most services operated on Unix-based operating systems. For services operated on Windows OS, there might be a problem to transfer the required data to the machines unless the service itself has an API for that, which is not always the case.

To overcome this obstacle, CESNET and Masaryk University piloted a simple connector for provisioning data to services hosted on Windows OS. The connector uses SSH as a data transfer protocol, which is currently supported by the latest Windows OS. SSH runs Powershell script on a destination which is customized for managed service, and its responsibility is to configure the service with provisioned identity and access control information.

Currently, there is a proof-of-concept solution of this which, as a part of T&I Mentorship Programme project, we would like to make it production ready, publish it as an opensource on a platform like Github and integrate with GÉANT eduTEAMS platform.