Geophysical Research Abstracts
Vol. 12, EGU2010-11737-1, 2010
EGU General Assembly 2010

Applying the Earth System Grid Security System in a Heterogeneous Environment of Data Access Services

Philip Kershaw (1), Bryan Lawrence (1), Dominic Lowe (1), Peter Norton (2), and Stephen Pascoe (1)

(1) NCAS/British Atmospheric Data Centre, Rutherford Appleton Laboratory, STFC (philip.kershaw@stfc.ac.uk), (2) Tessella Technology and Consulting PLC

CEDA (Centre for Environmental Data Archival) based at STFC Rutherford Appleton Laboratory is host to the BADC (British Atmospheric Data Centre) and NEODC (NERC Earth Observation Data Centre) with data holdings of over half a Petabyte. In the coming months this figure is set to increase by over one Petabyte through the BADC's role as one of three data centres to host the CMIP5 (Coupled Model Intercomparison Project Phase 5) core archive of climate model data. Quite apart from the problem of managing the storage of such large volumes there is the challenge of collating the data together from the modelling centres around the world and enabling access to these data for the user community.

An infrastructure to support this is being developed under the US Earth System Grid (ESG) and related projects bringing together participating organisations together in a federation. The ESG architecture defines Gateways, the web interfaces that enable users to access data and data serving applications organised into Data Nodes. The BADC has been working in collaboration with US Earth System Grid team and other partners to develop a security system to restrict access to data. This provides single sign-on via both OpenID and PKI based means and uses role based authorisation facilitated by SAML and OpenID based interfaces for attribute retrieval. This presentation will provide an overview of the access control architecture and look at how this has been implemented for CEDA.

CEDA has developed an expertise in data access and information services over several years through a number of projects to develop and enhance these capabilities. Participation in CMIP5 comes at a time when a number of other software development activities are coming to fruition. New services are in the process of being deployed alongside services making up the system for ESG. The security system must apply access control across this heterogeneous environment of different data services and technologies. One strand of the development efforts within CEDA has been the NDG (NERC Datagrid) Security system. This system has been extended to interoperate with ESG, greatly assisted by the standards based approach adopted for the ESG security architecture. Drawing from experience from previous projects the decision was taken to refactor the NDG Security software into a component based architecture to enable a separation of concerns between access control and the functionality of a given application being protected.

Such an approach is only possible through a generic interface. At CEDA, this has been realised in the Python programming language using the WSGI (Web Server Gateway Interface) specification. A parallel Java filter based implementation is also under development with our US partners for use with the THREDDS Data Server. Using such technologies applications and middleware can be assembled into custom configurations to meet different requirements. In the case of access control, NDG Security middleware can be layered over the top of existing applications without the need to modify them. A RESTful approach to the application of authorisation policy has been key in this approach. We explore the practical implementation of such a scheme alongside the application of the ESG security architecture to CEDA's OGC web services implementation COWS.