

Grid Integrated RADIUS Authentication Fabric

Abstract

We propose a DOE-wide *authentication fabric* based on RADIUS. The RADIUS authentication fabric will enable interoperation of multiple authentication services, particularly hardware-based secure authentication technologies such as one-time password (OTP) tokens. It will provide a simple, standard interface for end users, applications, and administrators. The initial phase of the project is a feasibility study to evaluate the RADIUS protocol's ability to federate different OTP services, and the general fitness of the RADIUS server platforms. Positive outcome of the feasibility study will lead to a pilot deployment and integration with advanced Grid CA services, such as Gridlogon¹ and SIPS².

1 Collaborators

ESnet – PKI team: Tony Genovese, Michael Helm, Roberto Morelli, Dhivakaran Muruganantham, John Webster

NERSC – Steve Chan, Eli Dart

Possible: Fusion Grid (GA and PPPL) staff TBD; FNAL – Matt Crawford; others

Vendors: Infoblox (RADIUS); Possible: Cryptocard (OTP vendor); RSA (Securid); Globus; others

2 Deliverables

- 2.1 Demonstration Service
One RADIUS server, one OTP technology (Securid), and one application supported
- 2.2 Test Deployment
RADIUS servers with HA configuration deployed in two sites, supporting at least two token-based authentication services
- 2.3 Deployment project plan
Feasibility study report and draft deployment plan
- 2.4 Pilot deployment
At least one DOE site uses the test deployment
- 2.5 Grid Integration
On-RADIUS-authentication proxy certificate support

3 Motivation

Several DOE national laboratories have expressed the intention to require token based, one-time password (OTP) authentication for remote access to site resources by off-site employees and external collaborators. Some laboratories have already done this. Grid technology requires the use of public key technology for its security services. We need to bridge between the two authentication approaches securely. Grid security architecture

¹ Grid Credential service proposed by NCSA and Globus to support roaming; see [GridLogon].

² “Site Integrated Proxy Servers”, a Grid-specialized CA; to appear in [AuthProf].

has been moving towards an on-demand, site-integrated approach to creating and managing authentication information. RADIUS [RADIUS] is an important authentication, authorization, and accounting (AAA) protocol in wide use; many institutions are already using it for firewall and VPN access control, and for other remote access. RADIUS has wide support in industry, and is used by OTP technology vendors. RADIUS provides useful characteristics: ability to proxy RADIUS requests, manage and route requests to multiple domains, return appropriate information to the application verifying an authentication request. OTP solutions have some, but limited, interoperability capabilities, and it appears that RADIUS can do better.

4 Approach and Requirements

The RADIUS authentication fabric is one part of a larger project, which will integrate OTP technology, and perhaps other authentication token technologies, with advanced Grid certification services. We will focus on RADIUS, and specifically the [RADIUS One](#) “RADIUS appliance” provided by [Infoblox](#). RADIUS services are being developed in a Grid and OTP context, and specific requirements are drawn from [NOPS], [GridLogon], and OTP requirements, but the RADIUS authentication fabric will not rule out other uses. Specific issues related to OTP deployments, Grid authentication, and other services will be discussed in other project documents. The feasibility study and pilot will test:

- Ability of RADIUS to proxy OTP and PKI token authentications
- High-availability and geographic dispersion features of RADIUS appliance
- Reliability and scaling rules
- Security features and requirements

The feasibility report will describe how well the test bed dealt with the following requirements, goals, and tests:

- Support several OTP technologies, multiple instances, and multiple sites
- Manage on-board AAA data securely
- Provide a uniform interface to clients, and administrators
- Route (proxy) clients to the appropriate OTP site authentication service
- Fail gracefully:
- Replicate data rapidly and securely between RADIUS nodes.
- Support administrative partitioning between sites

Finally, the report will make recommendations for the pilot deployment and Grid integration, and outline the project plan for these steps.

5 Costs and Resources

Feasibility study only:

Approximately 1 FTE, drawn from ESnet SSG, NTSG, and NESG to solve various implementation problems. Support from collaborators.

3 RADIUS One appliances + support, \$30k

2 OTP back end server hosts (\$ TBD)

OTP tokens (demo licenses)

6 References

- [NOPS] Chan, S., Lau, S., Srinivasan, J., and A.Wong, "One Time Password Authentication for Open High Performance Computing Environments", *NOPS* group, Apr 2004 (unpublished)
- [GridLogon] Basney, J., Welch, V., and F. Siebenlist,, "A Roadmap for Integration of Grid Security with One-Time Passwords", NCSA and Globus (unpublished draft).
- [RADIUS] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", *IETF*, RFC 2865, June 2000;
<http://www.ietf.org/rfc/rfc2865.txt>
- [AuthProf] Genovese, T., "Grid Authentication profiles", *CAOPS WG, GGF*, May 15 2004 (draft).
- [ESRAD] "RADIUS and Securid", ESnet PKI Project, Access Grid presentation slides,
<http://www.doe grids.org/CA/Research/RADIUS%20and%20Securid.pdf>