IAM Frameworks for Collaboration

CANS 2017 DUKE KUNSHAN UNIVERSITY 昆山杜克大学

Speakers

- CHEN Ping: 陈萍 Advances in CARSI and EduROAM
- Dean Lane: TIER at Rice University
- LIN Jingqiang: 林璟锵 Consolidated Privilege Management and Authorization for Loosely-Hierarchical Organizations: Practices in CAS
- Keith Hazelton: TIER ABAC/RBAC support with Grouper

Eduroam & Identity Federation Development in CERNET

PROF. PING CHEN

PEKING UNIVERSITY

OCT. 25TH, 2017

Operation & Management

From eduroam@CERNET operator's point of view:

- To promote the efficiency and save human resources
- To support prov./univ. requirements with best efforts, but on a base line.
  - Chinese Network Security Law effected in Jun. 1st, 2017
- A hierachical operation mechanism and community contribution are fundamental.

From univ. eduroam operator's point of view:

- Joining & debugging: online guide, whole process self-served
- Operating
  - Operating Analysis System: each view for each univ.
- Campus wide management for visitor roaming in and local people roaming out.

Technical assist: http://www.eduroam.edu.cn

Community communication:

- WeChat eduroam@CERNET community, WeChat public number, email, hotline

Why TIER?

Dean Lane

Manager of Identity and Access Management

Rice University, Houston, Texas, USA

Rice and TIER

Through the TIER Campus Success Program, Rice hopes to not only replace our aging infrastructure but to also move to a more standard scalable solution that will enable us to answer the needs of the future.

We are very excited that through this process, we will be able to give back to the community and help other institutions that will come along later. And as we move forward, any integrations or components that we add to the architecture will be more easily shared back to the community thereby helping everyone.

Consolidated Privilege Management and Authorization for Loosely-Hierarchical Organizations: the Practices in Chinese Academy of Sciences

JINGQIANG LIN

INSTITUTE OF INFORMATION ENGINEERING,

CHINESE ACADEMY OF SCIENCES

CANS 2017, KUNSHAN, CHINA

Work-in-Progress

Consolidated Identity & Access Management System in Chinese Academy of Sciences

- The development started in about 2011
- It is being used and being improved
  - SSO works well now

Privilege Management and Authorization

- Not so good/friendly for IT managers
- We are working on it, since 2016 …

Feature

Security, least privilege
- Private privilege
- Private application

Flexibility, for diverse requirements
- Privilege: Mandatory > Restricted > Private
- Application: Public > Protected > Private

Autonomy, final control by the owner institute
- Each institute has its own managers
- With private privileges and private application

Convenience, easy to configure
- Only a little number of configuration rules are enough

TIER ABAC and RBAC Support with Grouper

Keith Hazelton (hazelton@wisc.edu)
Sr. IT Architect, University of Wisconsin-Madison
Architect, TIER, Internet2

TIER: Access Management as a Gap

- A user's rights to access online materials depend on many factors
  - Their affiliation with the organization
  - Their roles and responsibilities (RBAC)
  - Other attributes about them such as
    - Have they had the required training?
    - Are they on a specific project team?
    - Are they taking a specific course?
    - NIST calls this Attribute Based Access Control (ABAC). See NIST sp 800-162
- How to manage these rights and privileges?

6.3 Access Control Model 3 - RBAC User to Role Mapping

Policy Administration Point: PAP	Policy Information Point: PIP
Policy Decision Point: PDP	Policy Enforcement Point: PEP

Subject -> Role assignment in Grouper Permission -> Role at service

1. Fine-grained permission sets are managed at the target service (Role -> Permissions) and assigned a Role Name

2. Grouper access control group statically mapped to target service Role Name and provides User -> Role mapping

3. PAP split between Grouper and target service, PDP and PEP at service

For copies of today's presentations email keith.hazelton@wisc.edu