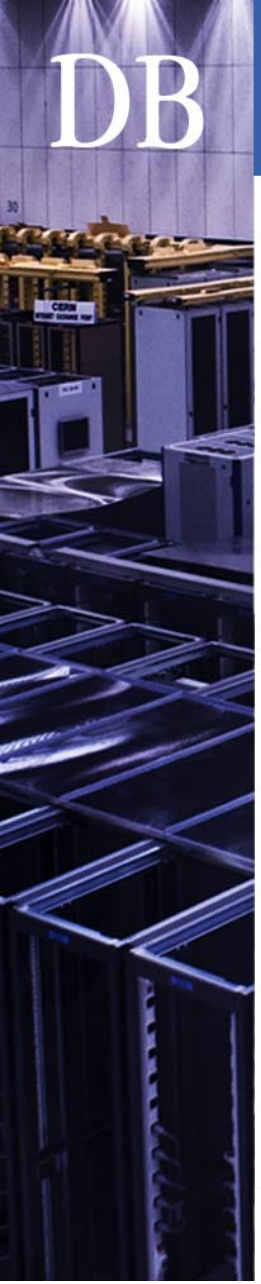
Database Access Management

Giacomo Tenaglia
CERN IT/DB

HEPiX Spring 2012

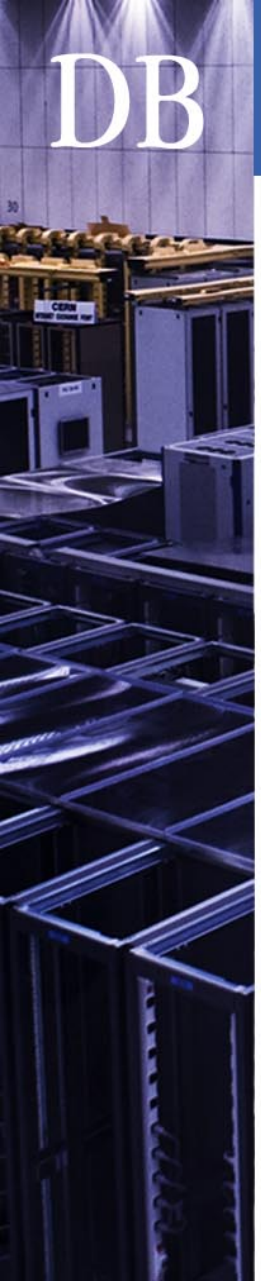
CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it



Agenda

- Scenario and requirements
- DAM: overview
- Implementation details

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it



Scenario

- O(100) servers
- “Clusters” of 1 to 6 nodes
- Access via SSH

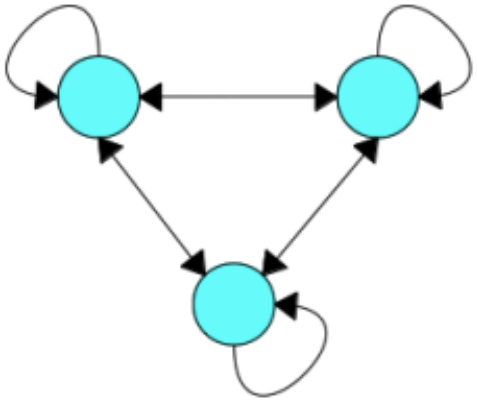
- High turnover of people
  - Admins
  - Users

- “Flat” network

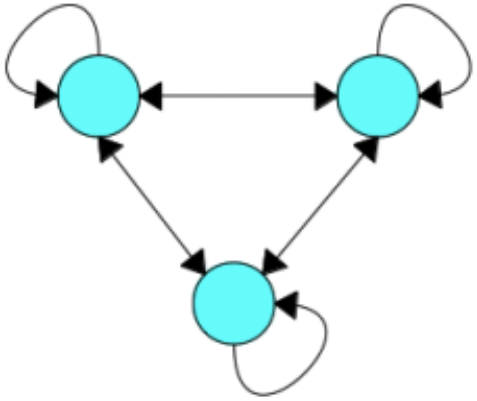
CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

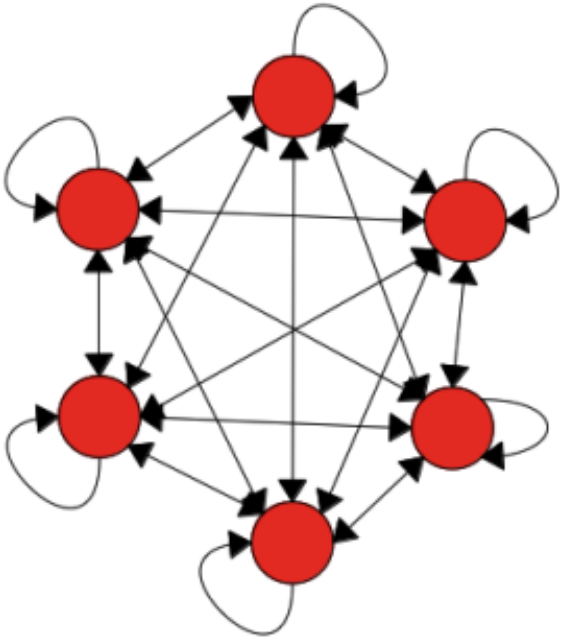
Requirements: DB clusters

Requirements: DB clusters

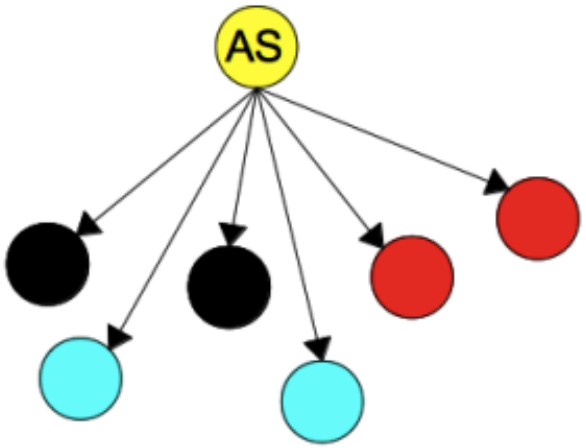


Requirements: DB clusters

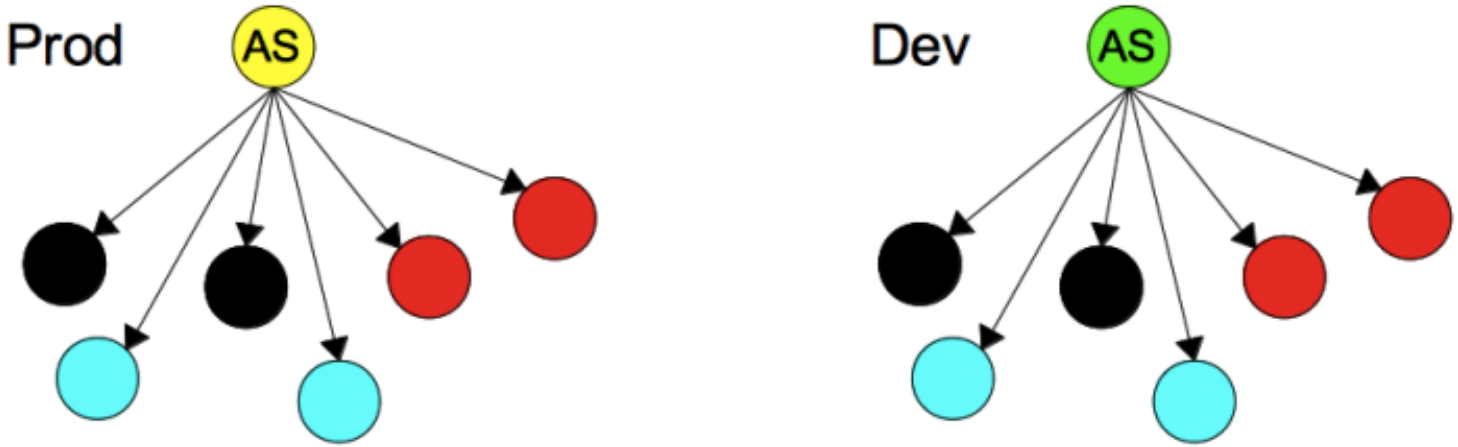




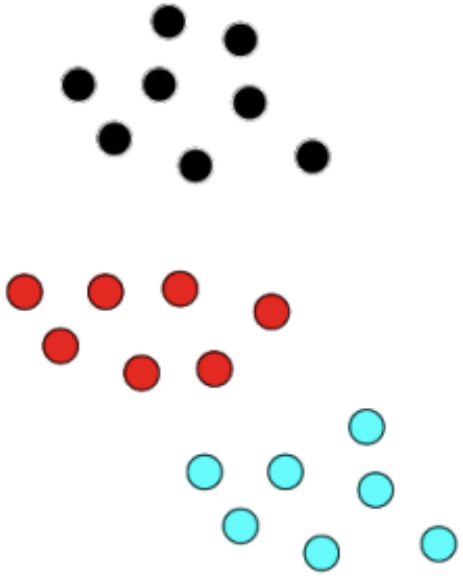
Requirements: Middleware

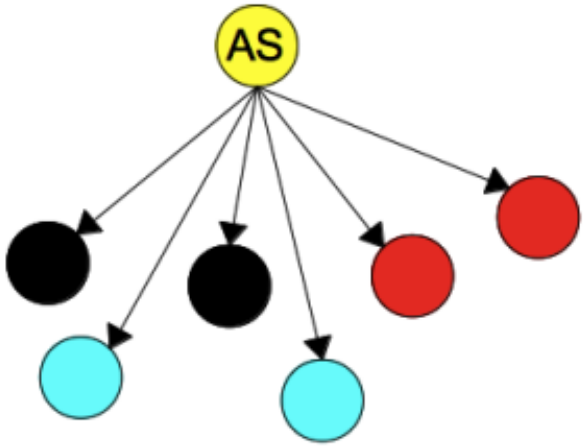


Requirements: Middleware

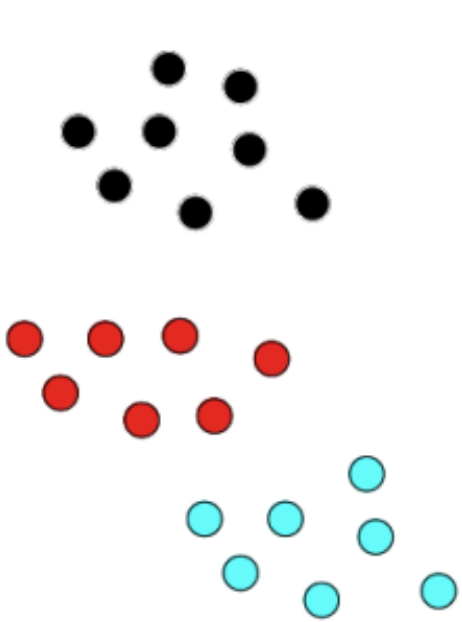


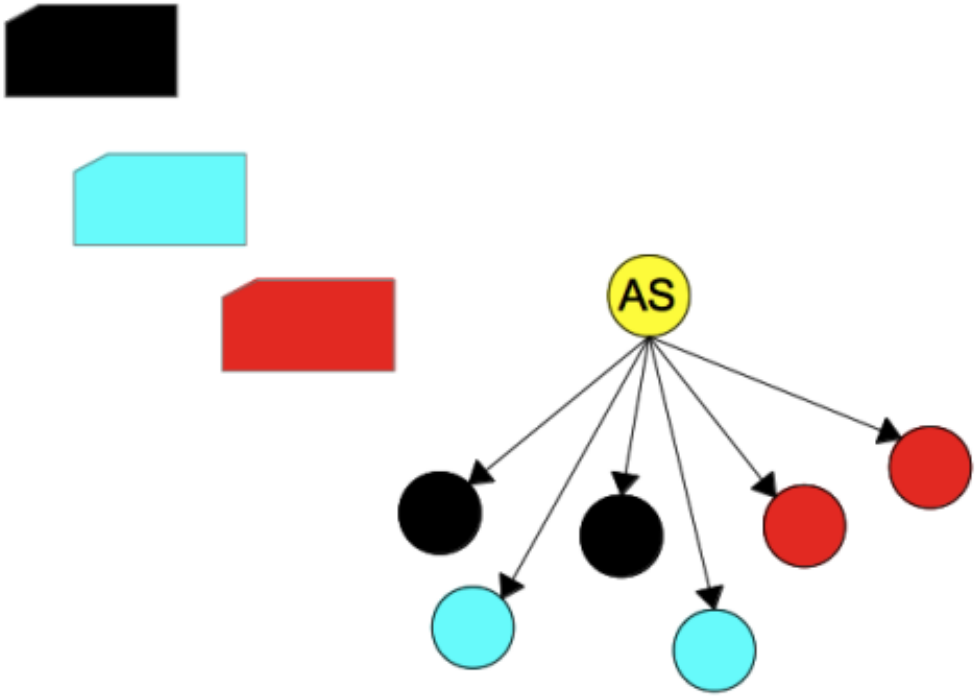
Requirements: Middleware



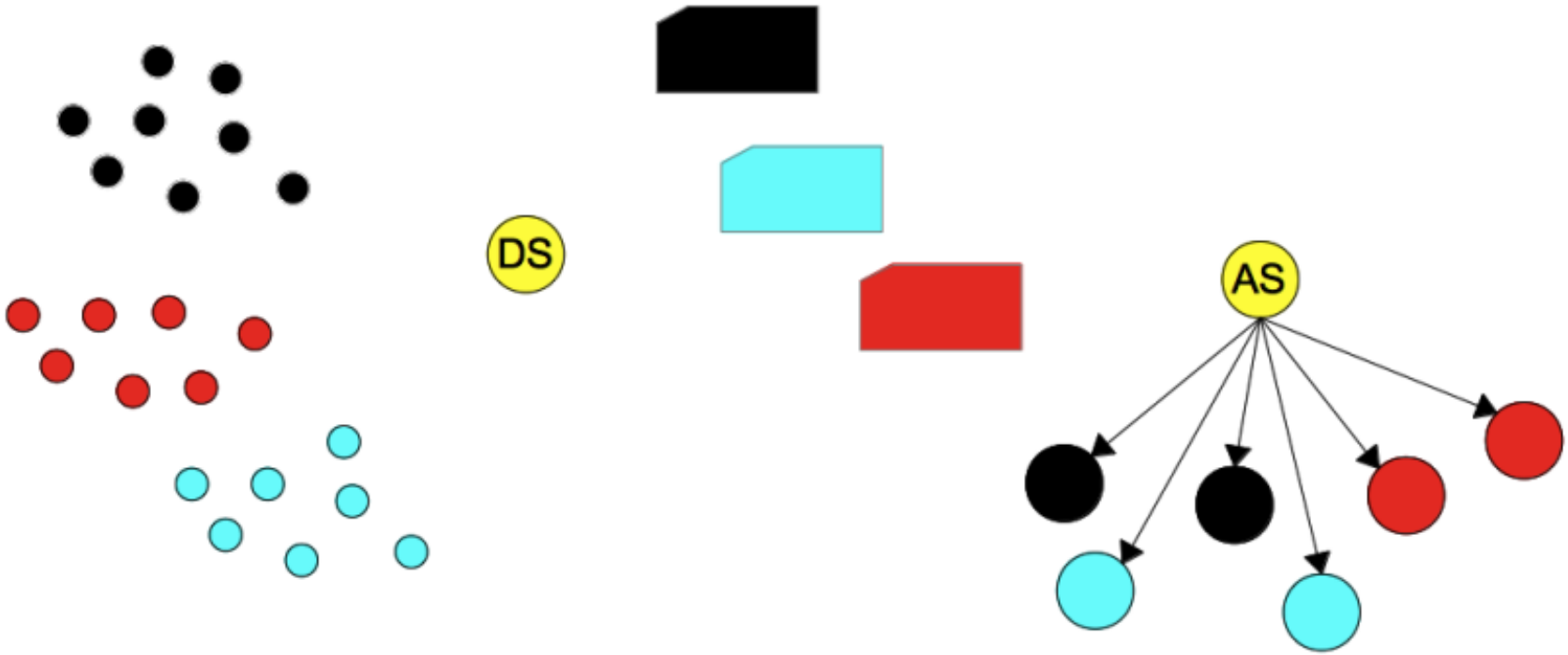


Requirements: Middleware

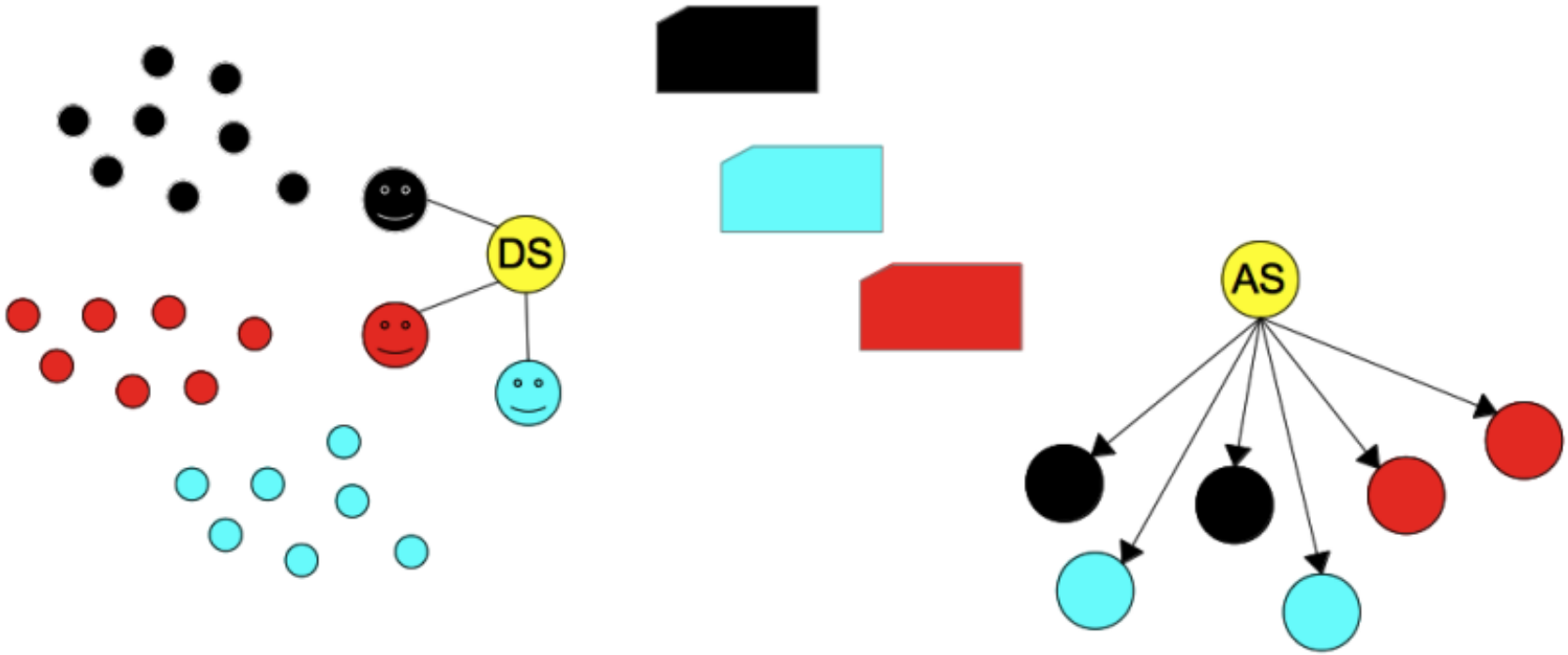




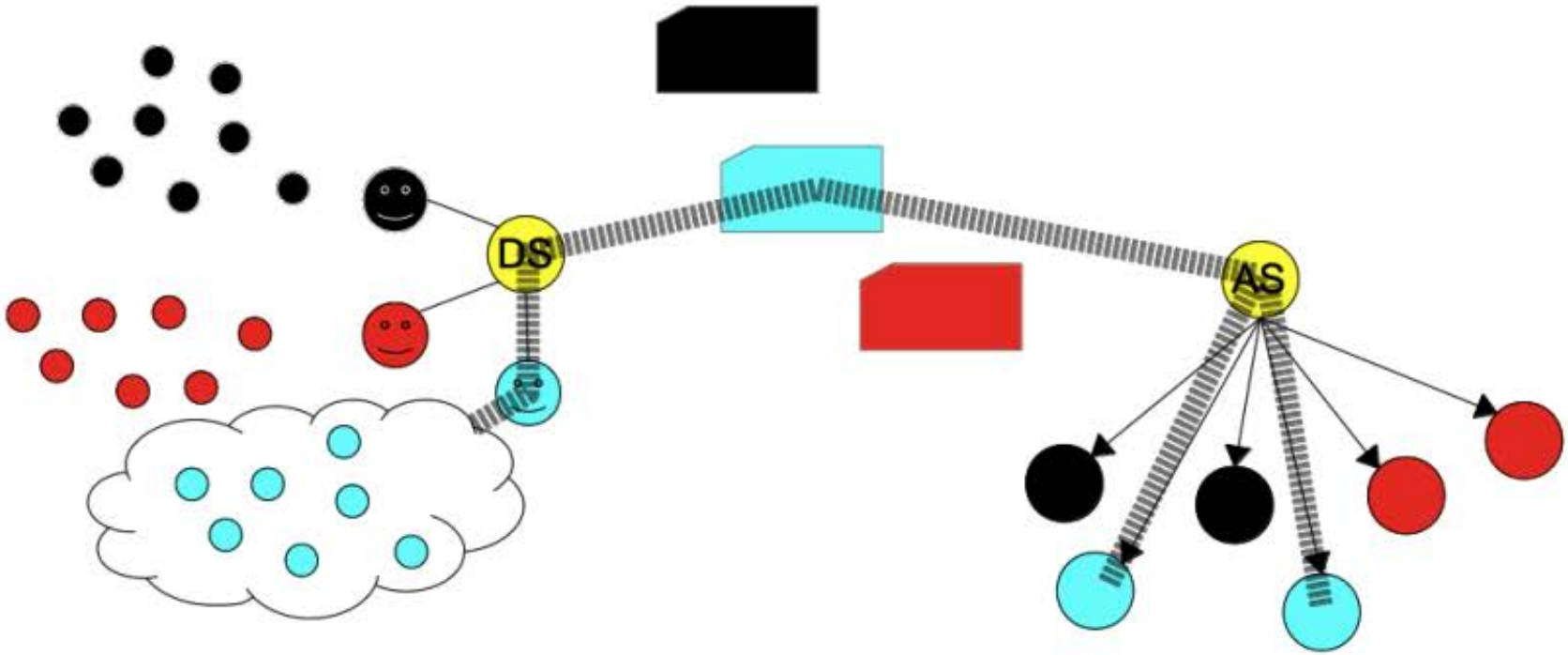
Requirements: Middleware

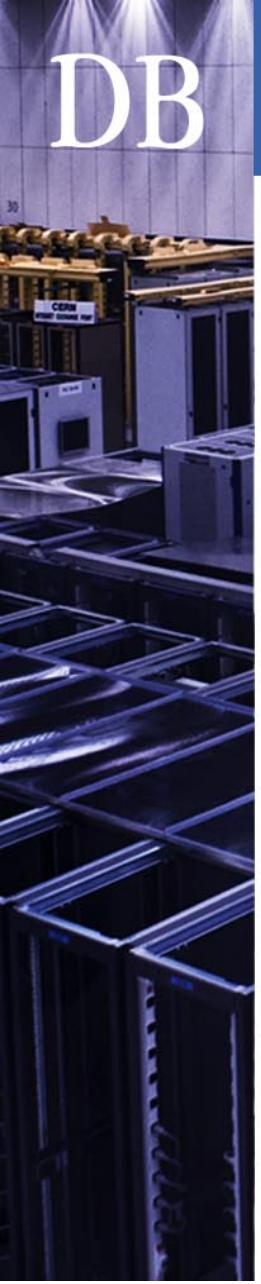


Requirements: Middleware



Requirements: Middleware



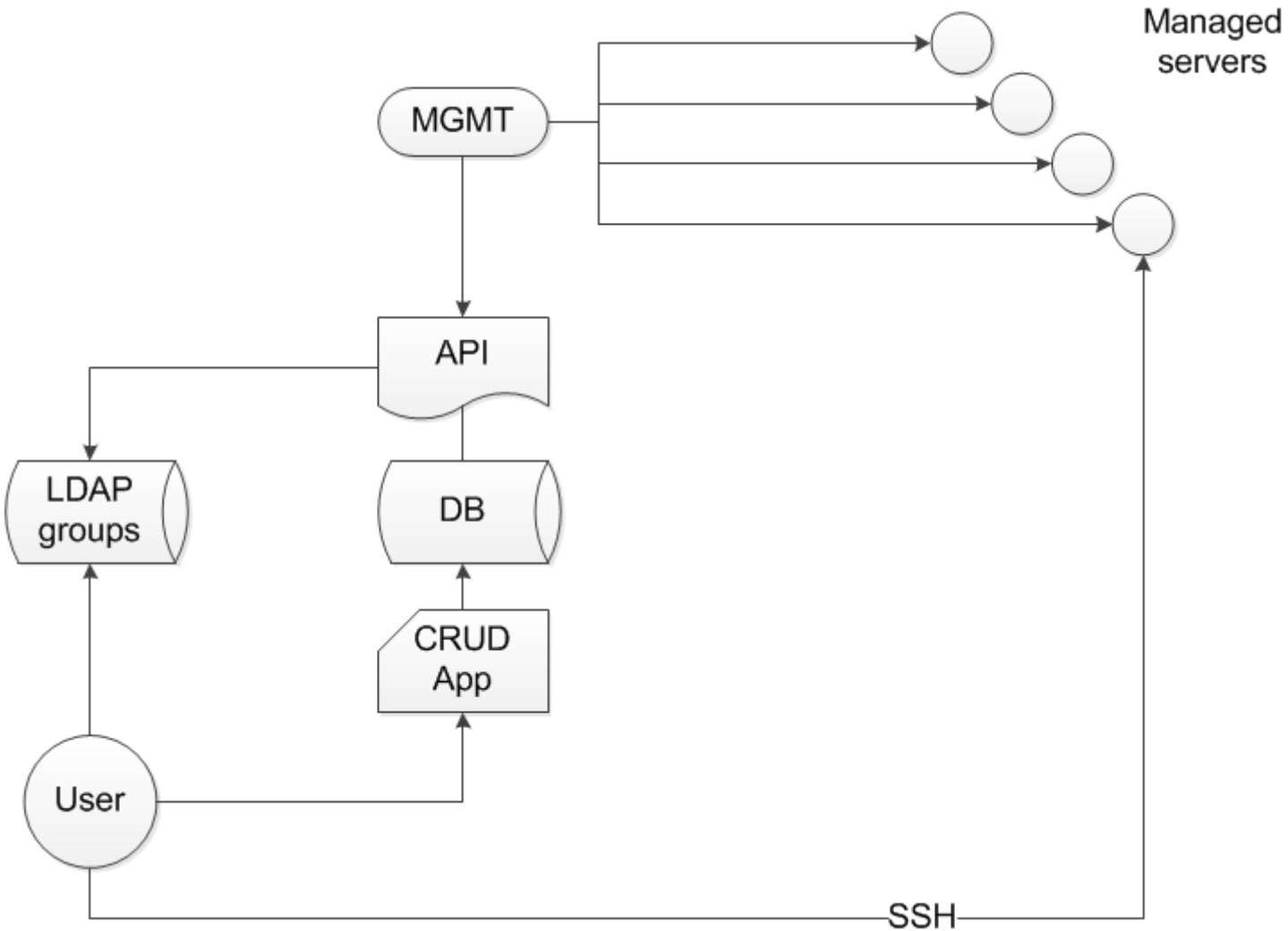


Requirements

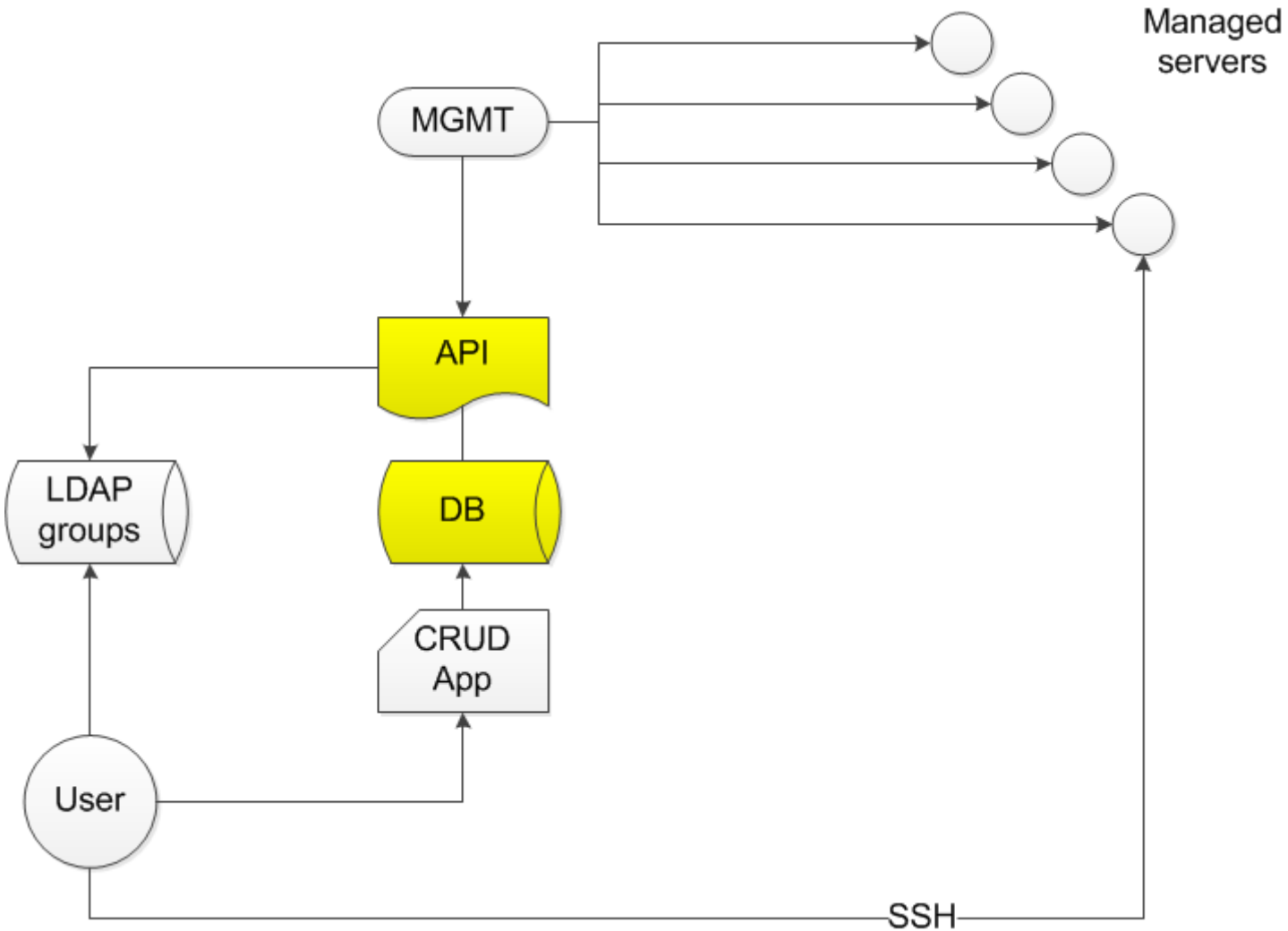
- Functional requirements
  - Group management
    - Track relationships (“who can access what”)
    - Membership delegation to group admins
    - Cluster equivalence
  - Ease key management
  - CLI and Web
  - Use standard CERN IT tools
- Security requirements
  - Revoke access
  - PKI not shared passwords

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

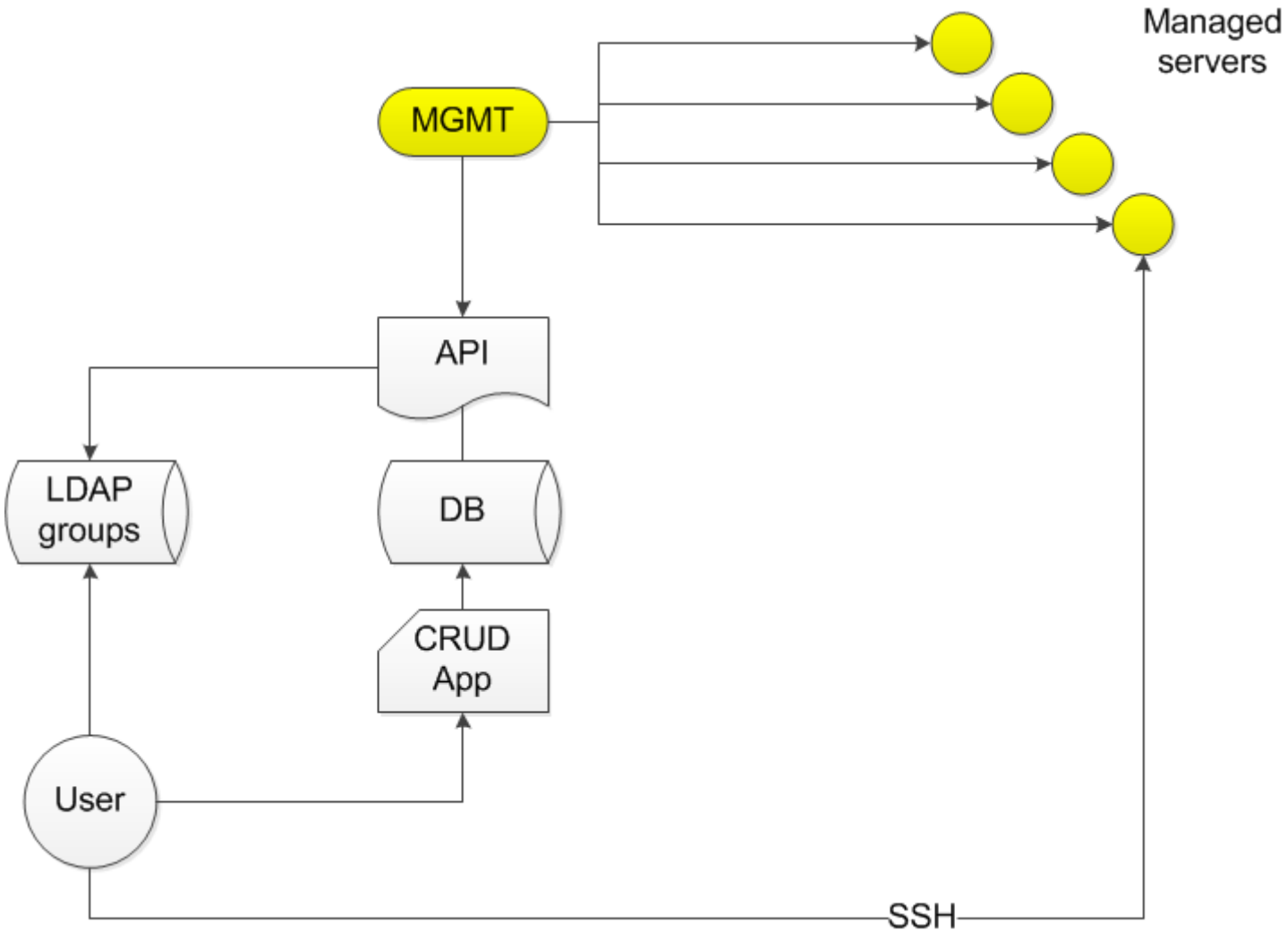
DAM Overview



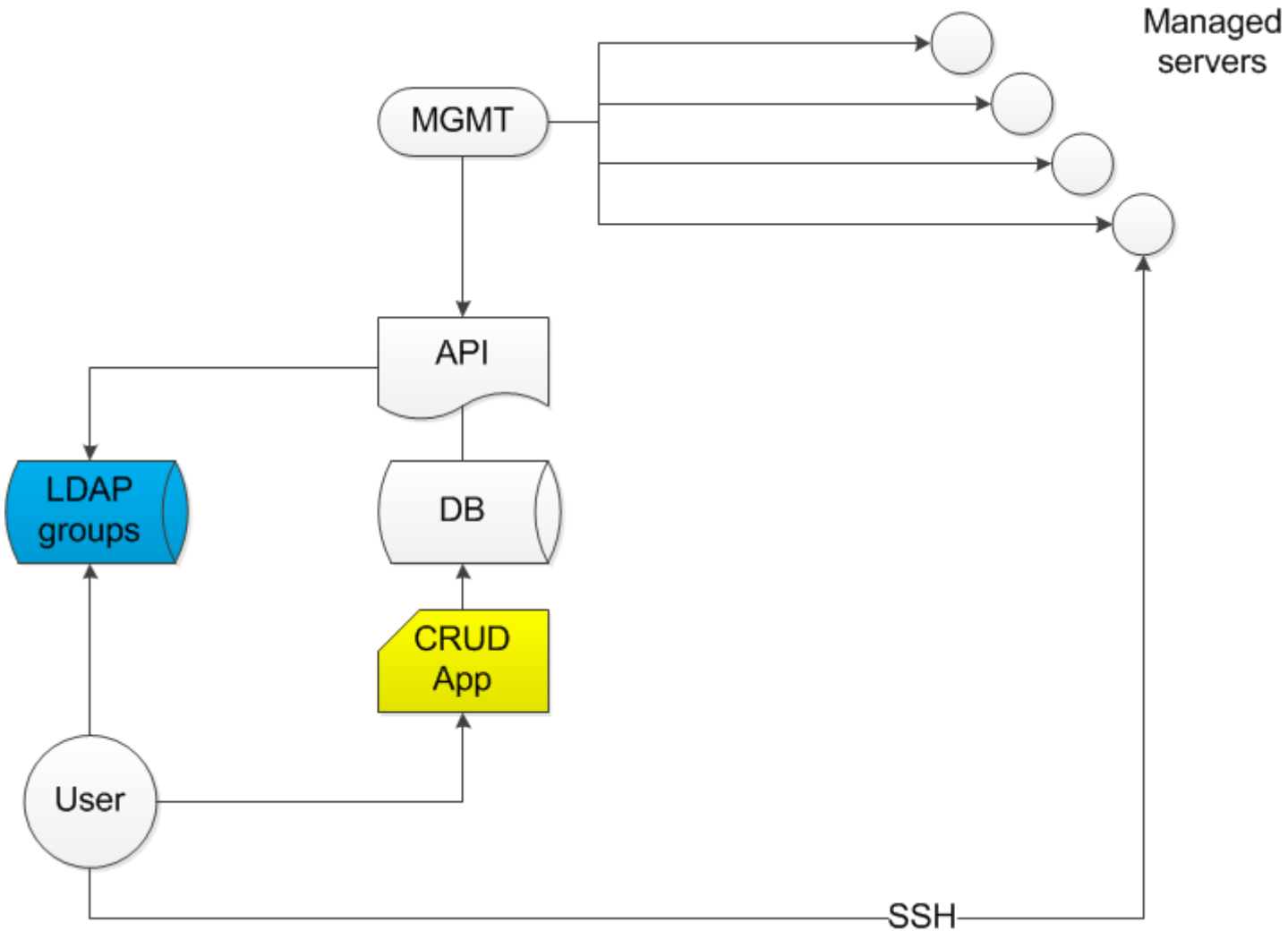
DAM Overview



DAM Overview



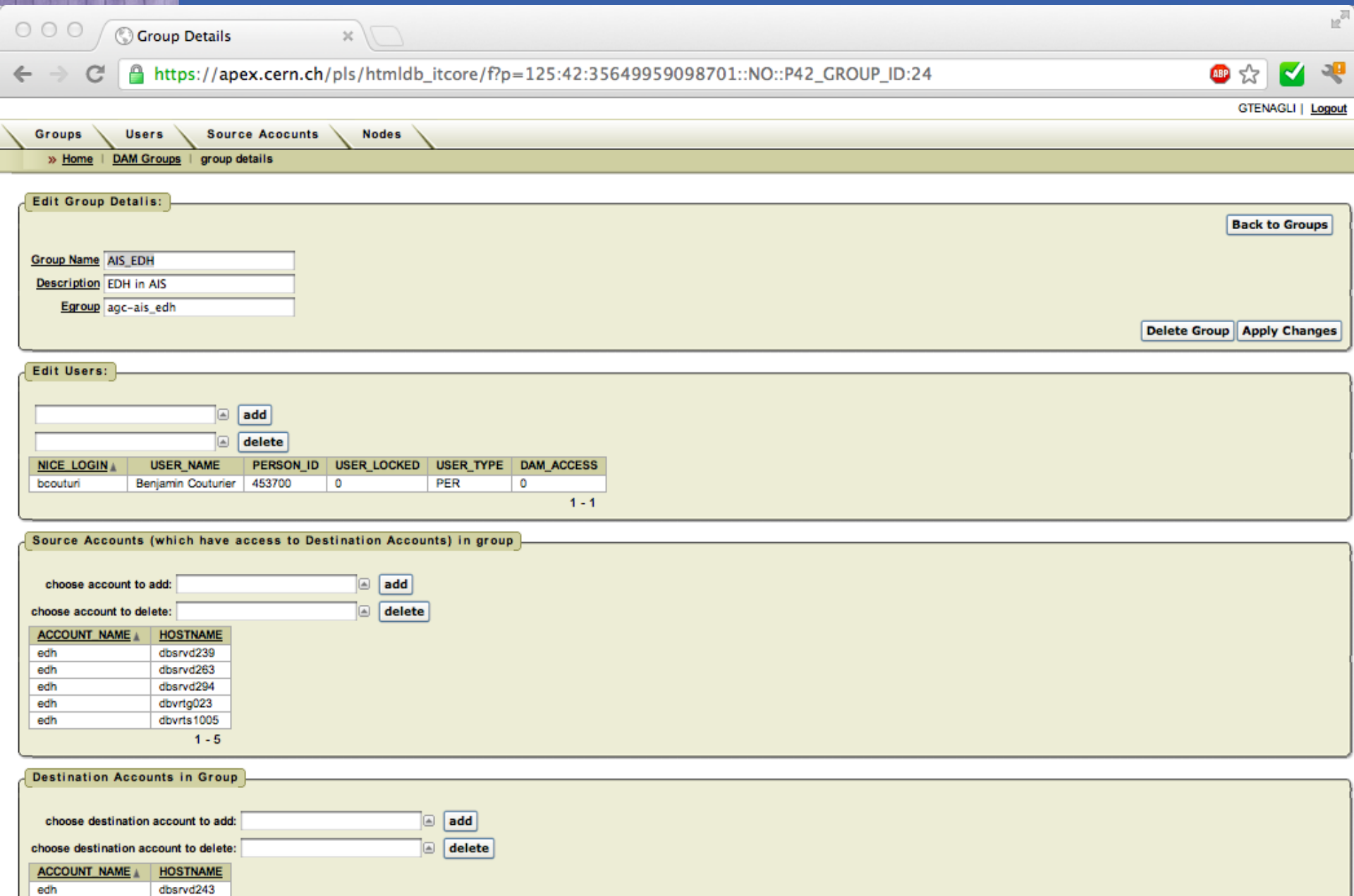
DAM Overview



System Requirements

- Database
  - Currently Oracle, API can be ported
- Management Server
  - Password-less access to managed nodes
- LDAP directory with groups (if needed)
  - Currently e-groups published via LDAP

Interface for Administrators



Edit Group Details:

Group Name: AIS_EDH

Description: EDH in AIS

Egroup: agc-ais_edh

Edit Users:

add

delete

NICE_LOGIN	USER_NAME	PERSON_ID	USER_LOCKED	USE
bcouturi	Benjamin Couturier	453700	0	PER

Source Accounts (which have access to Destination Accounts) in gr

choose account to add: add

choose account to delete: delete

ACCOUNT_NAME	HOSTNAME
edh	dbsrvd239
edh	dbsrvd263
edh	dbsrvd294
edh	dbvrtg023
edh	dbvrts1005

1 - 5

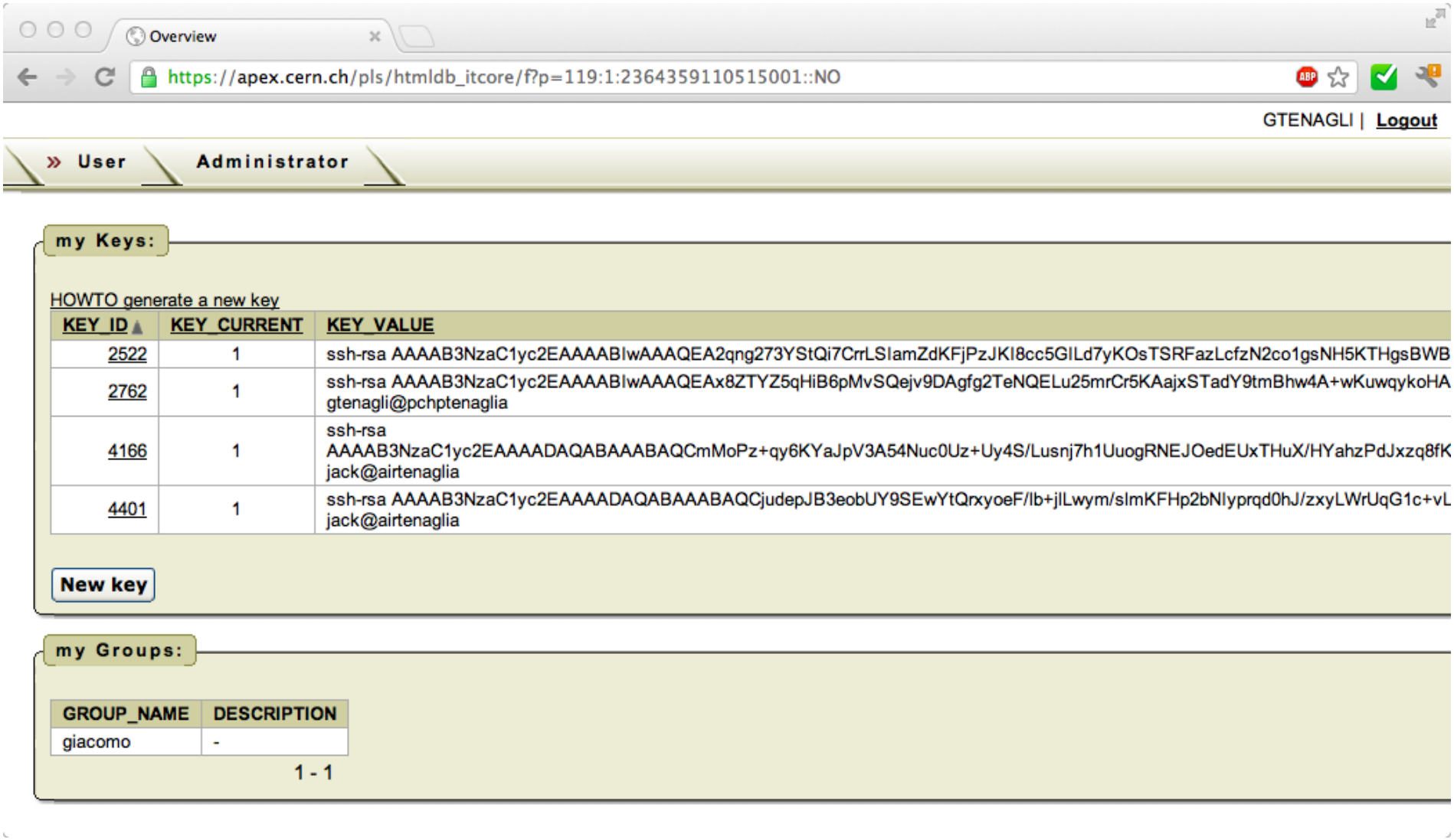
Destination Accounts In Group

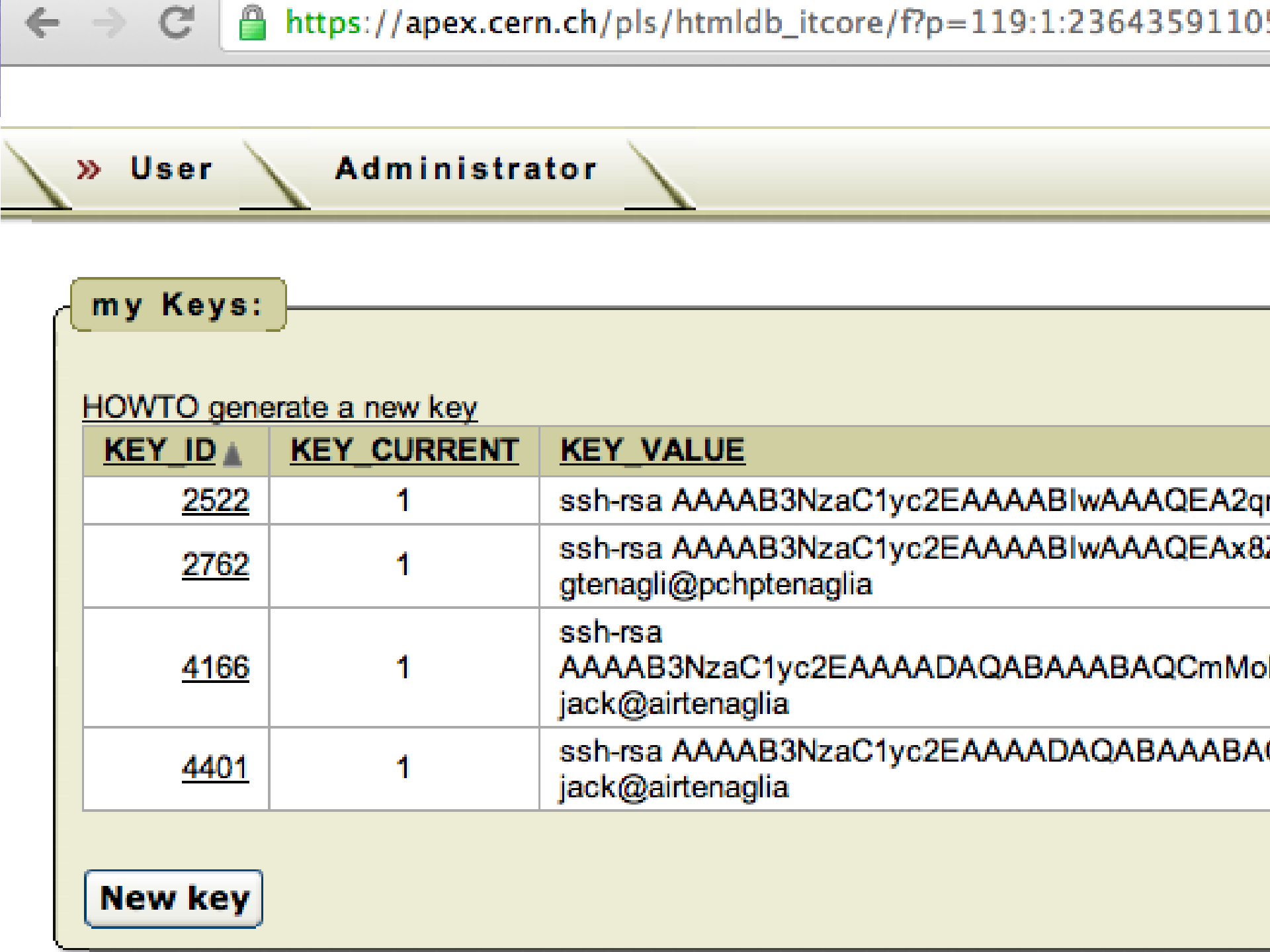
choose destination account to add: add

choose destination account to delete: delete

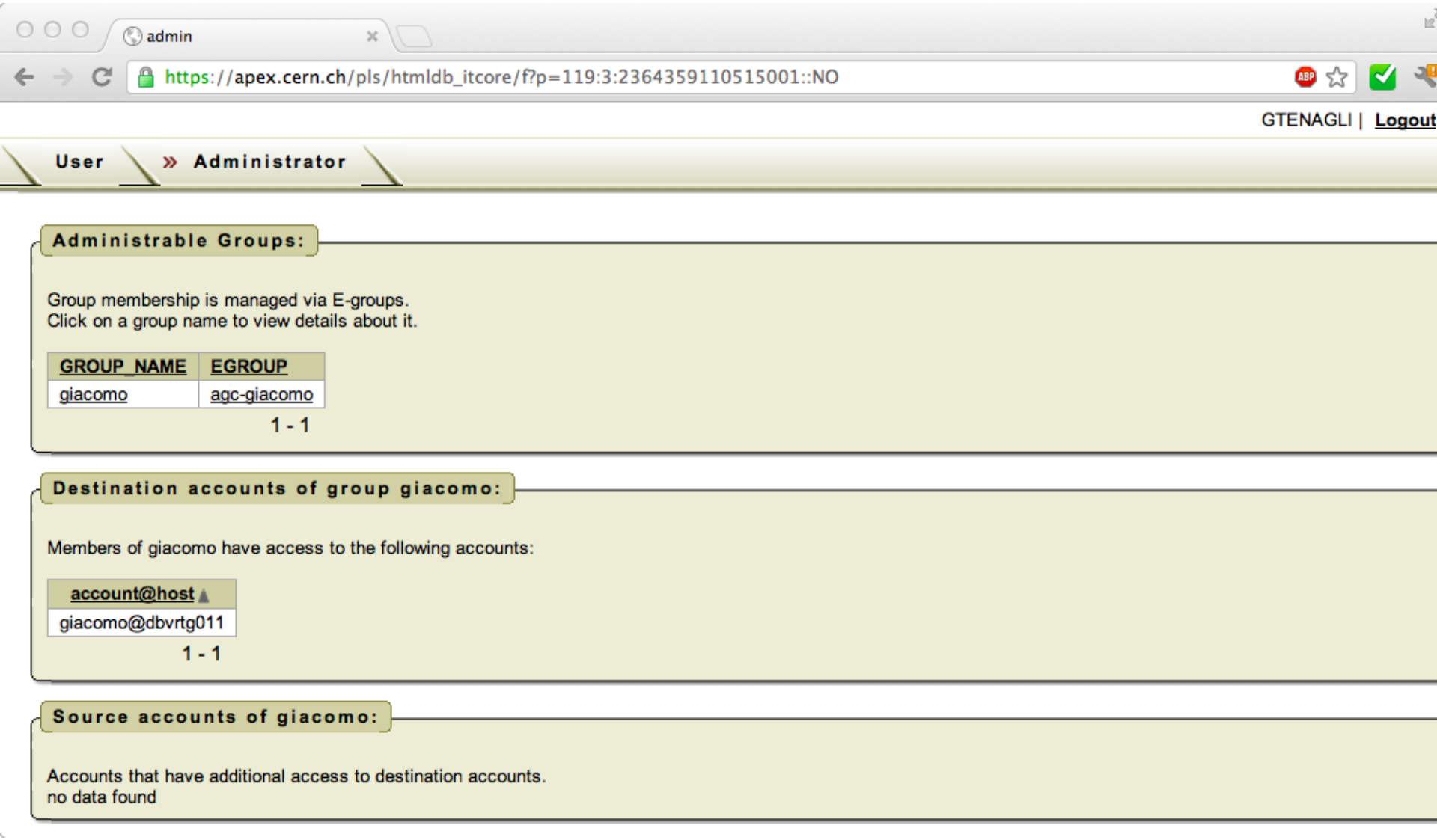
ACCOUNT_NAME	HOSTNAME
edh	dbsrvd243

Interface for Users




https://apex.cern.ch/pls/htmldb_itcore/f?p=119:1:2364359110
» User
Administrator
my Keys:
HOWTO generate a new key
KEY_ID
KEY_CURRENT
KEY_VALUE
2522
1
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA2q
2762
1
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAx8
gtenagli@pchptenaglia
4166
1
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCmMo
jack@airtenaglia
4401
1
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABA
jack@airtenaglia
New key

Interface for Group Admins



Administrable Groups:

Group membership is managed via E-groups.
Click on a group name to view details about it.

GROUP_NAME	EGROUP
giacomo	agc-giacomo

1 - 1

Destination accounts of group giacomo:

Members of giacomo have access to the following accounts:

account@host
giacomo@dbvrtg011

1 - 1

Implementation Details

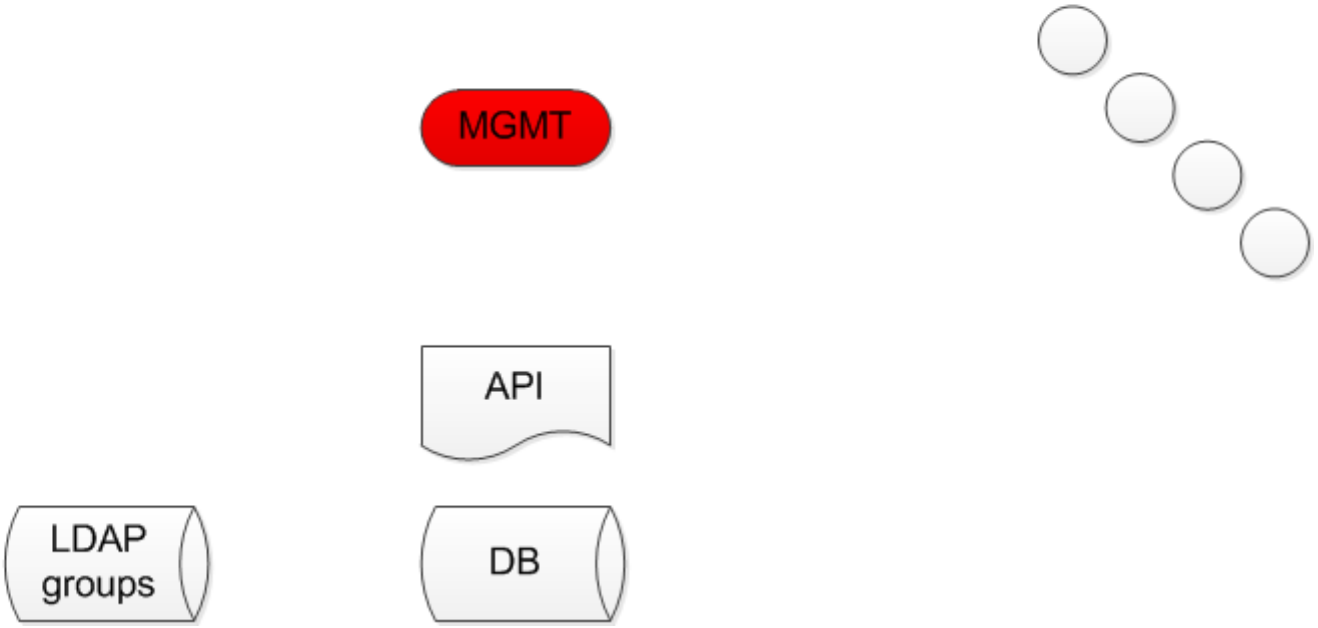
- PL/SQL API, Perl, APEX Application
- Extensive use of Kerberos
  - Service keytab on management host
    - Tested with CERN Security Team
  - Easier for users than SSH keys
- LDAP groups managed by users (“egroups”)

Implementation Details

- Parallel “Access refresh”
- Source accounts
  - Generate private keys on the nodes
- Managed servers pre-seeding
  - Integrated in CMS
- Revoke public key
  - Consistency checks upon refresh

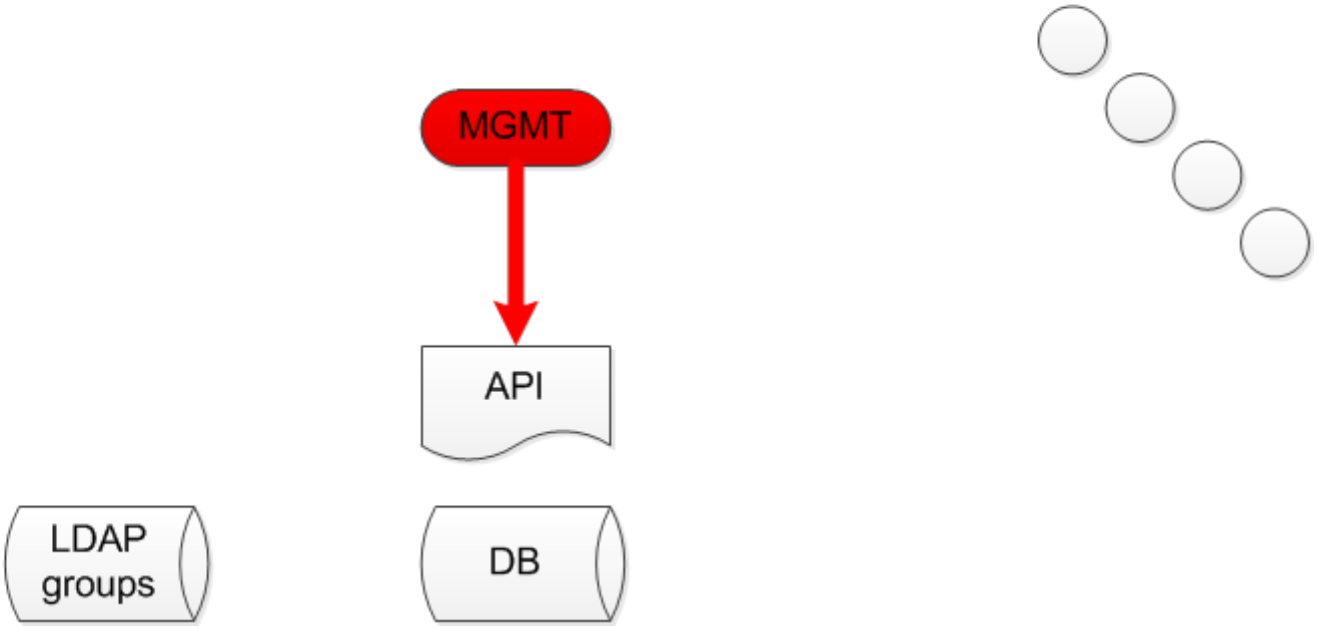
How It Works

Processing accountX@hostY



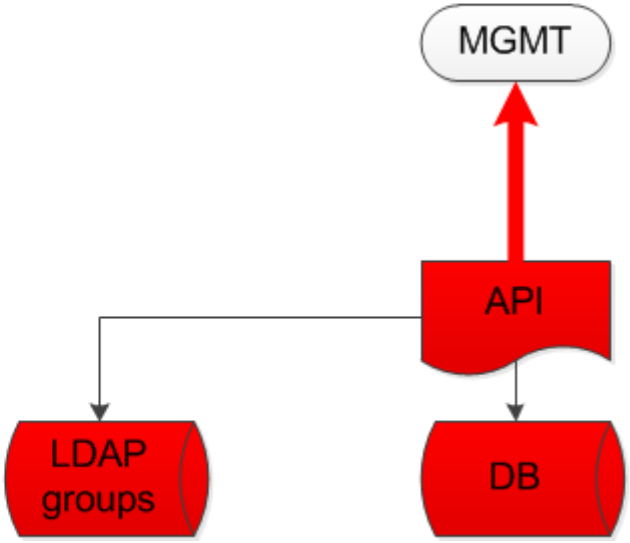
How It Works

Processing accountX@hostY
Get authorised users



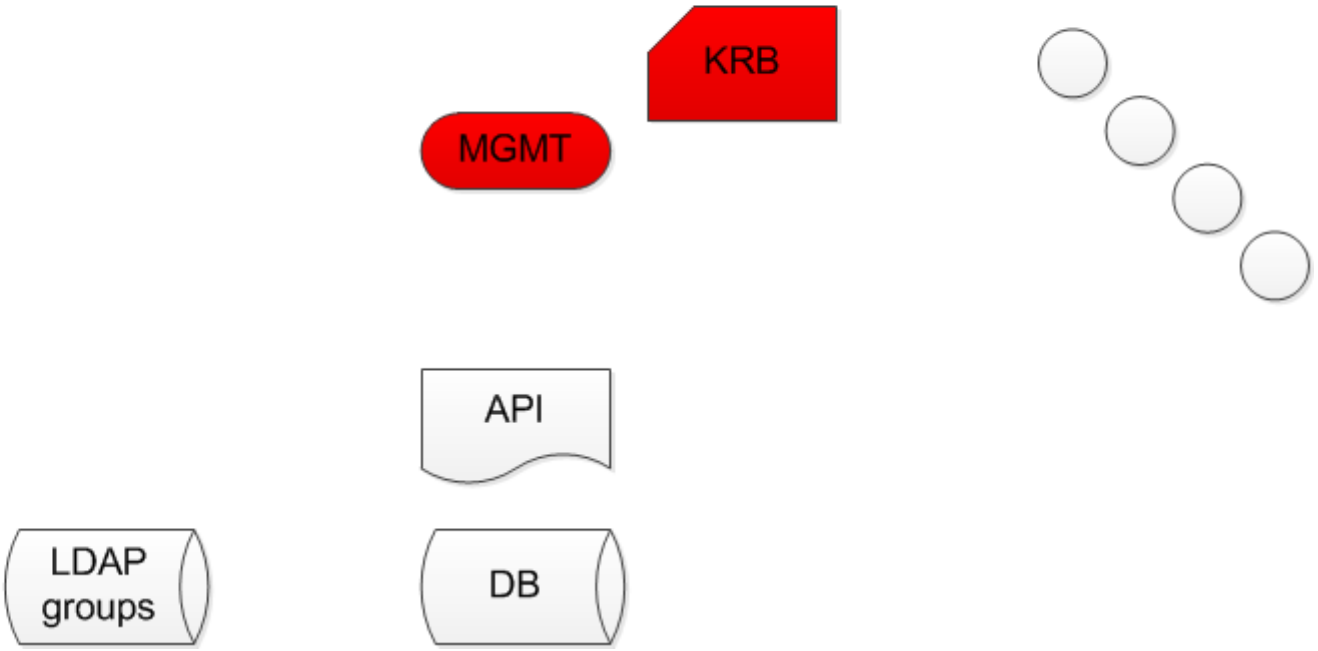
How It Works

Processing accountX@hostY
Get authorised users
Create user list



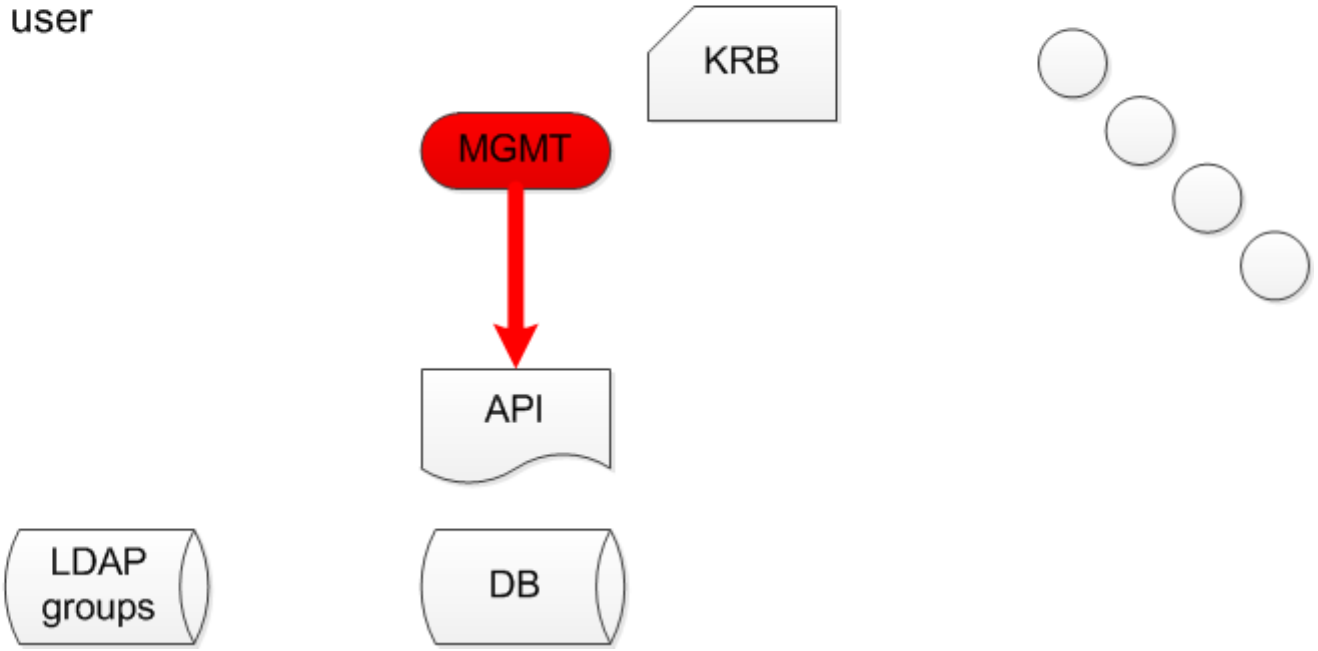
How It Works

Processing accountX@hostY
Get authorised users
    Create user list
Create Kerberos file



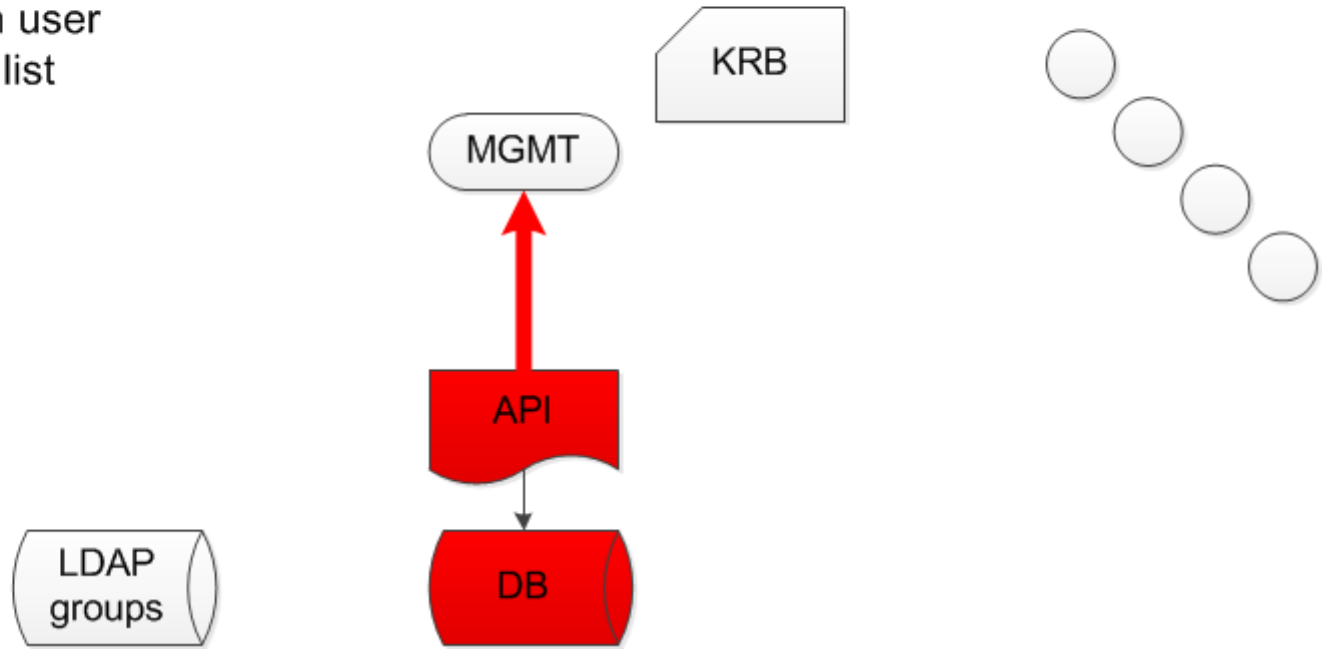
How It Works

Processing accountX@hostY
Get authorised users
    Create user list
Create Kerberos file
Get pubkeys for each user



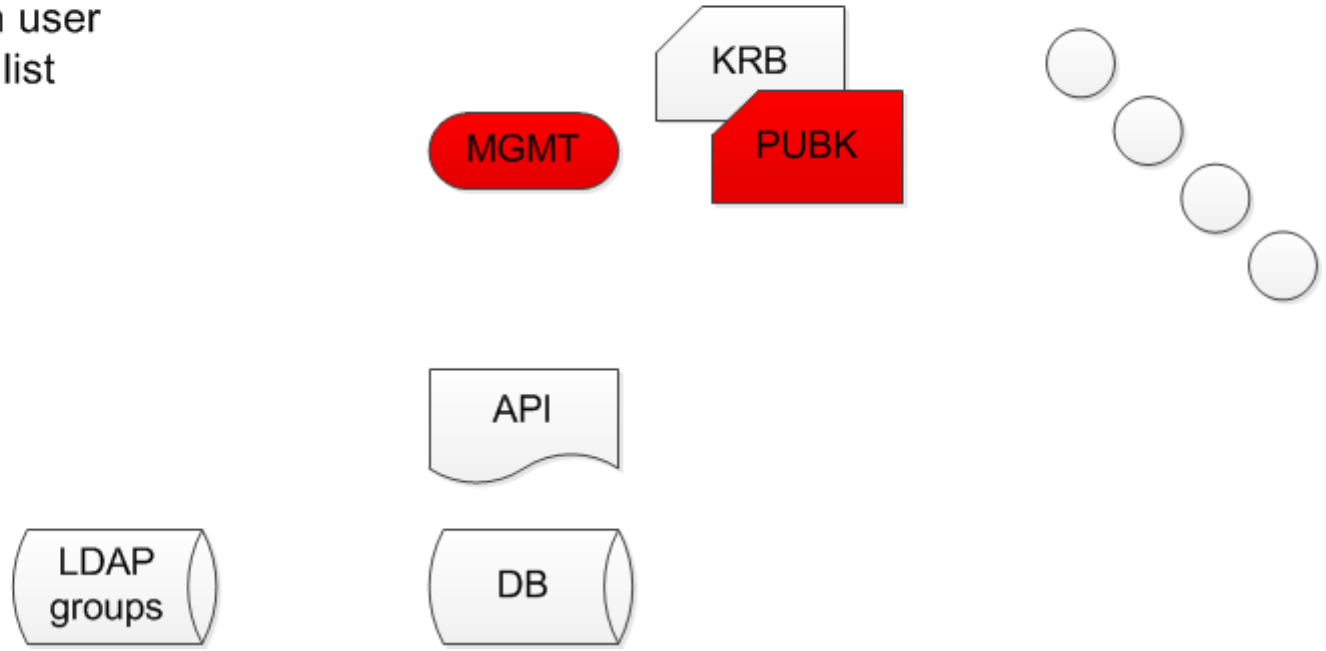
How It Works

Processing accountX@hostY
Get authorised users
    Create user list
Create Kerberos file
Get pubkeys for each user
    Create pubkey list



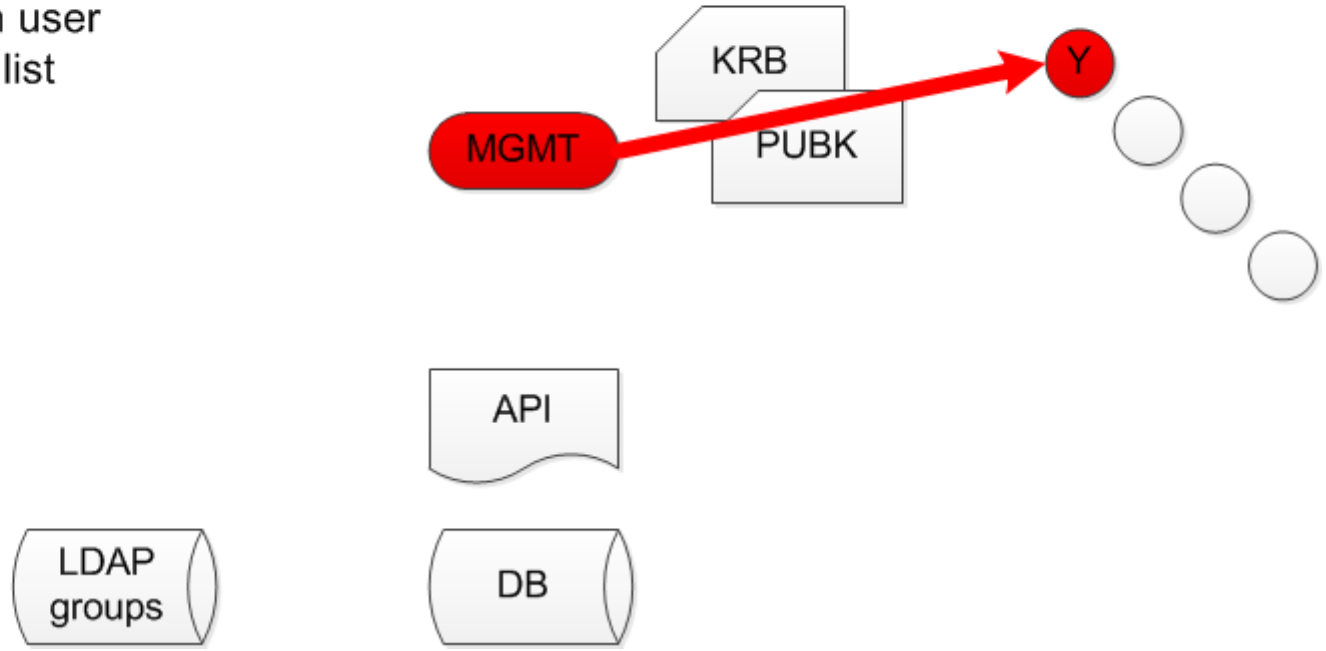
How It Works

Processing accountX@hostY
Get authorised users
    Create user list
Create Kerberos file
Get pubkeys for each user
    Create pubkey list
Create pubkey file



How It Works

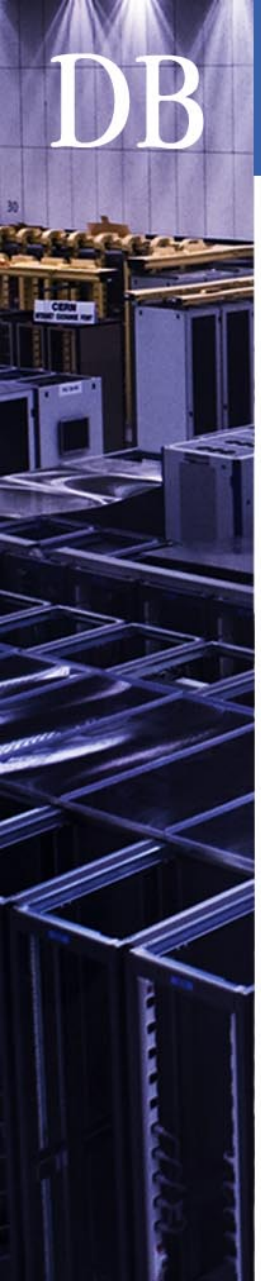
Processing accountX@hostY
Get authorised users
    Create user list
Create Kerberos file
Get pubkeys for each user
    Create pubkey list
Create pubkey file
Ship files to hostY



Current usage

- 500 servers
- 2000 accounts
- 5 teams (developers, DBA, sysadmins)
- 150 groups

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

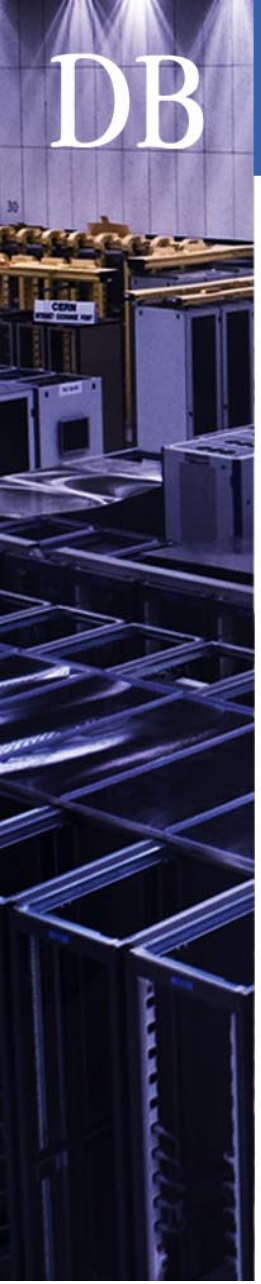


Summary

- DAM helps secure our environment
- Key success factor for 11g migration
- API and source code could be made available to other sites if interested

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

Q&A



Thank you!

Giacomo.Tenaglia@cern.ch

Credits:
Alvaro Gonzalez Alvarez
Andrea Ieri,
Artur Wiecek,
Dawid Wojcik
Jacek Wojcieszuk

CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it