Central Banning

Policy/Operations Implications

Sven Gabriel,

sveng@nikhef.nl, Nikhef, EGI-CSIRT

Next Steps

Recap slide: Next steps OMB 18. Dec. 2012

- Agreement on a Central Banning facility from OMB.
- Define procedures for adding and removing a DN from a central ban list.
- Agreement on a Argus deployment.
- A tool for easy download and handling of the central ban lists to be developed.
- **Central Banning Mini Project (CERN/STFC/FOM) seems to get funded**

Policy/Procedures

Define procedures for adding and removing a DN from a central ban list.

- Ban list must only operate on individuals (user DNs).
- Ban list has to be endorsed by IRTF (EGI-CSIRT).
- Service Operations Policy: 9. You should implement the access limitations and banning lists defined centrally by Security Operations and should give them priority over local policies. The site implementation of the central banning service should be configured such that any ban or restore action made by Security Operations is effective within the specified time period."

Argus aware Services

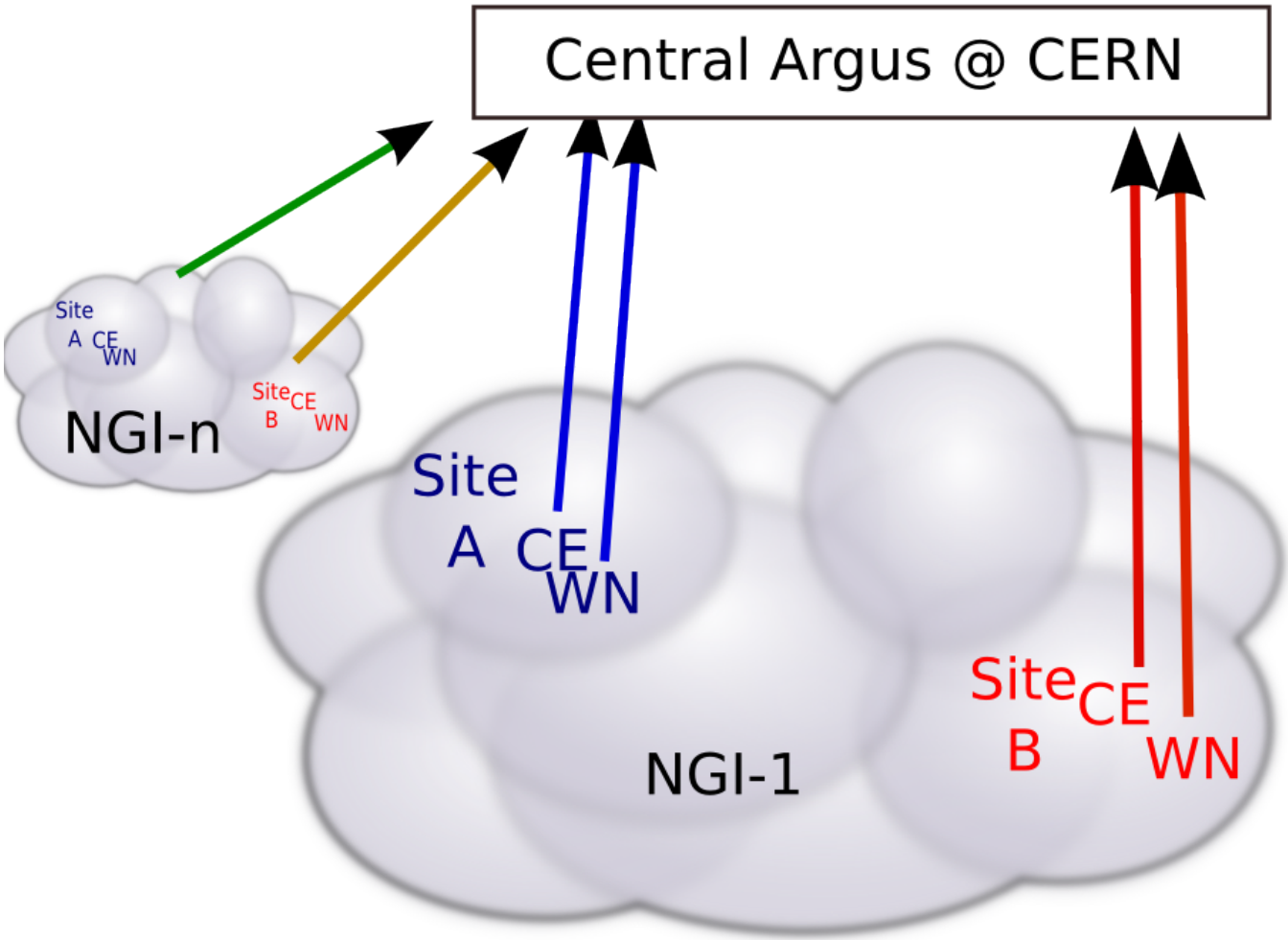
According to release notes almost all glite services are Argus aware

- In production for example at CERN for Cream-CEs, WNs (glexec)
- WMS Argus authZ for access control
- DPM/LFC Support for the DPM/LFC banning engine have been added to the Argus PEP Server.
- dCache gPlazma 2 with ARGUS black listing

Is this tested for example in staged rollout?

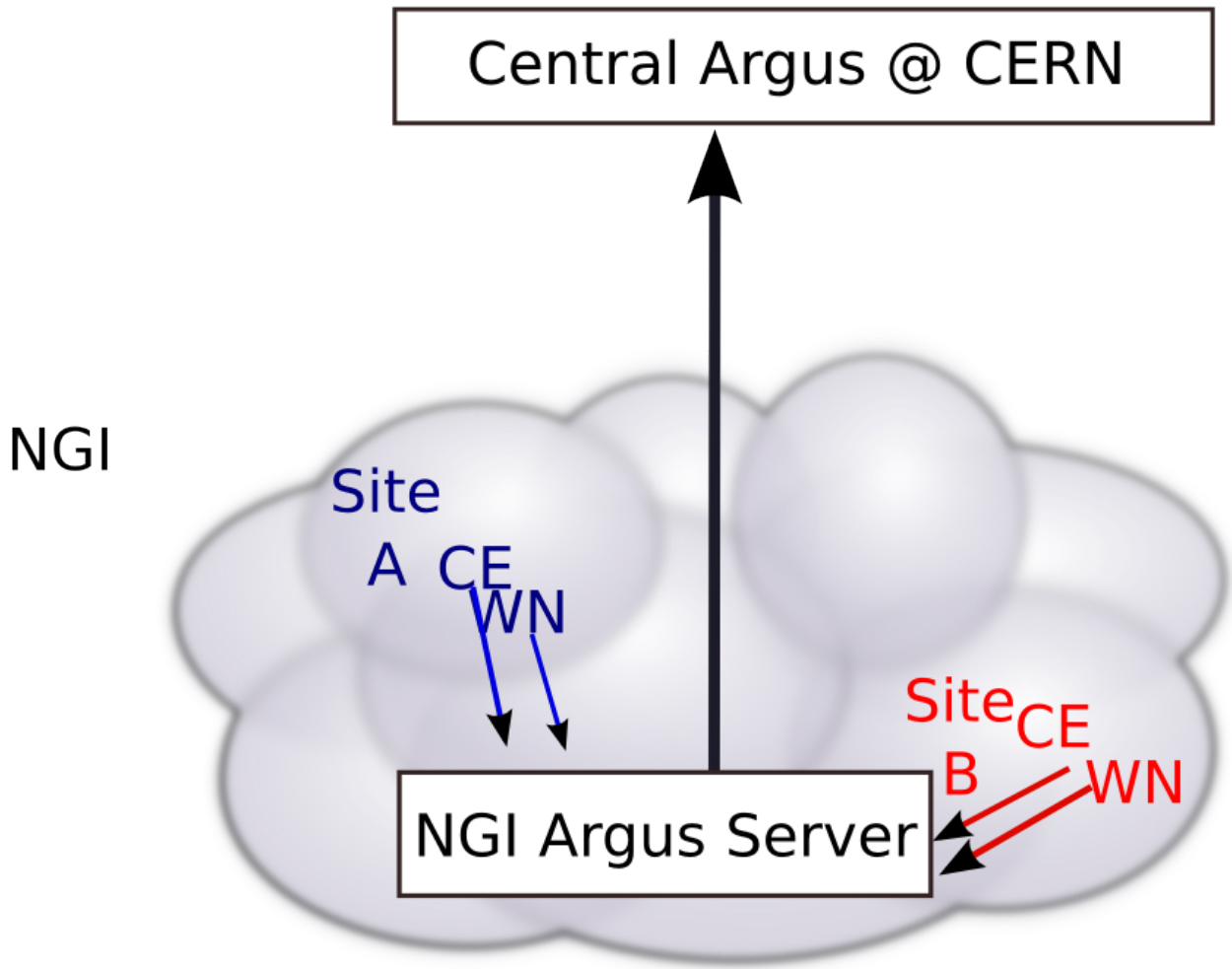
Deployment/Argus

Possible scenarios Only one central Argus instance does **NOT** scale



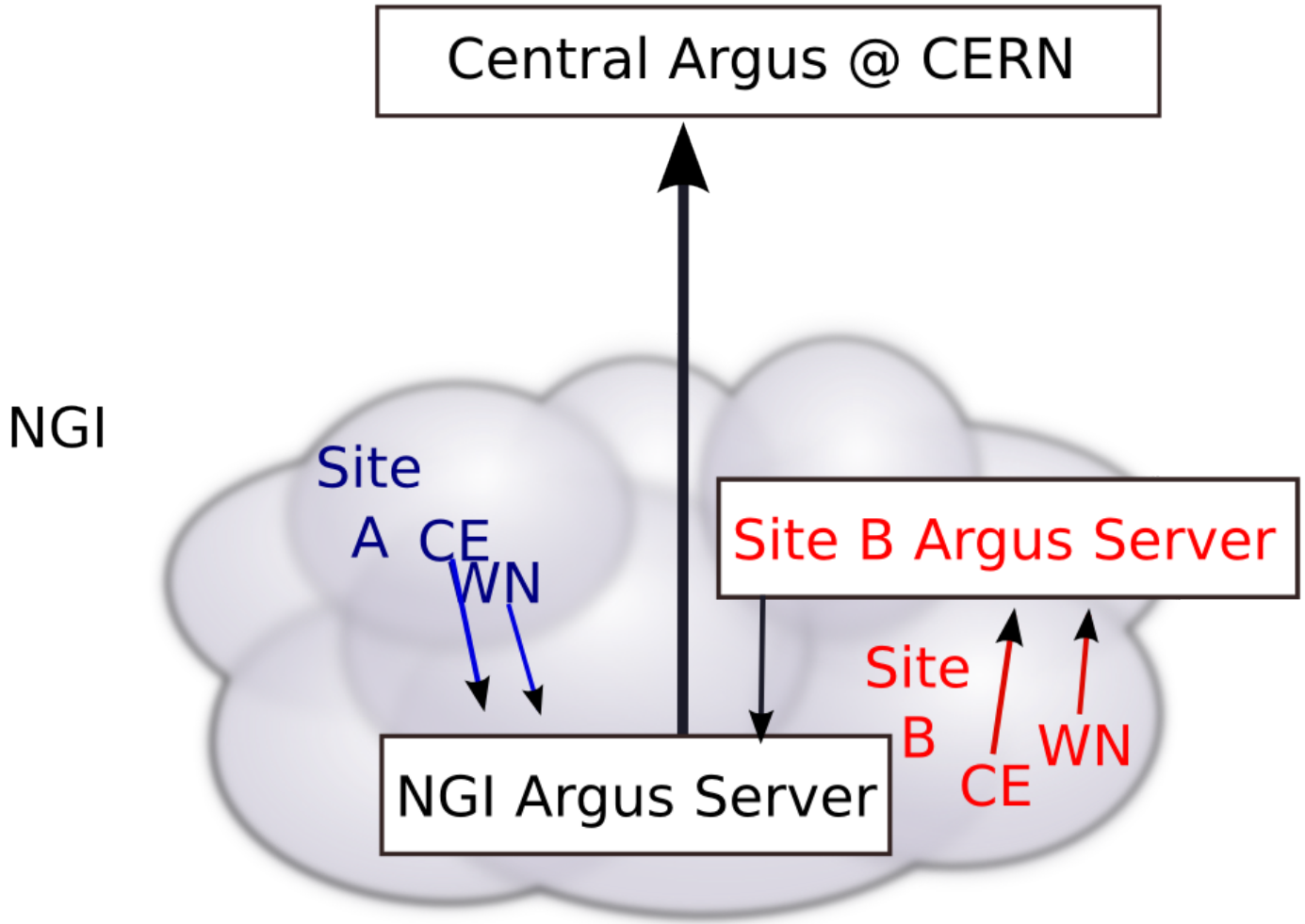
Deployment/Argus

Possible scenarios Minimal Deployment



Deployment/Argus

Possible scenarios More robust/flexible Deployment



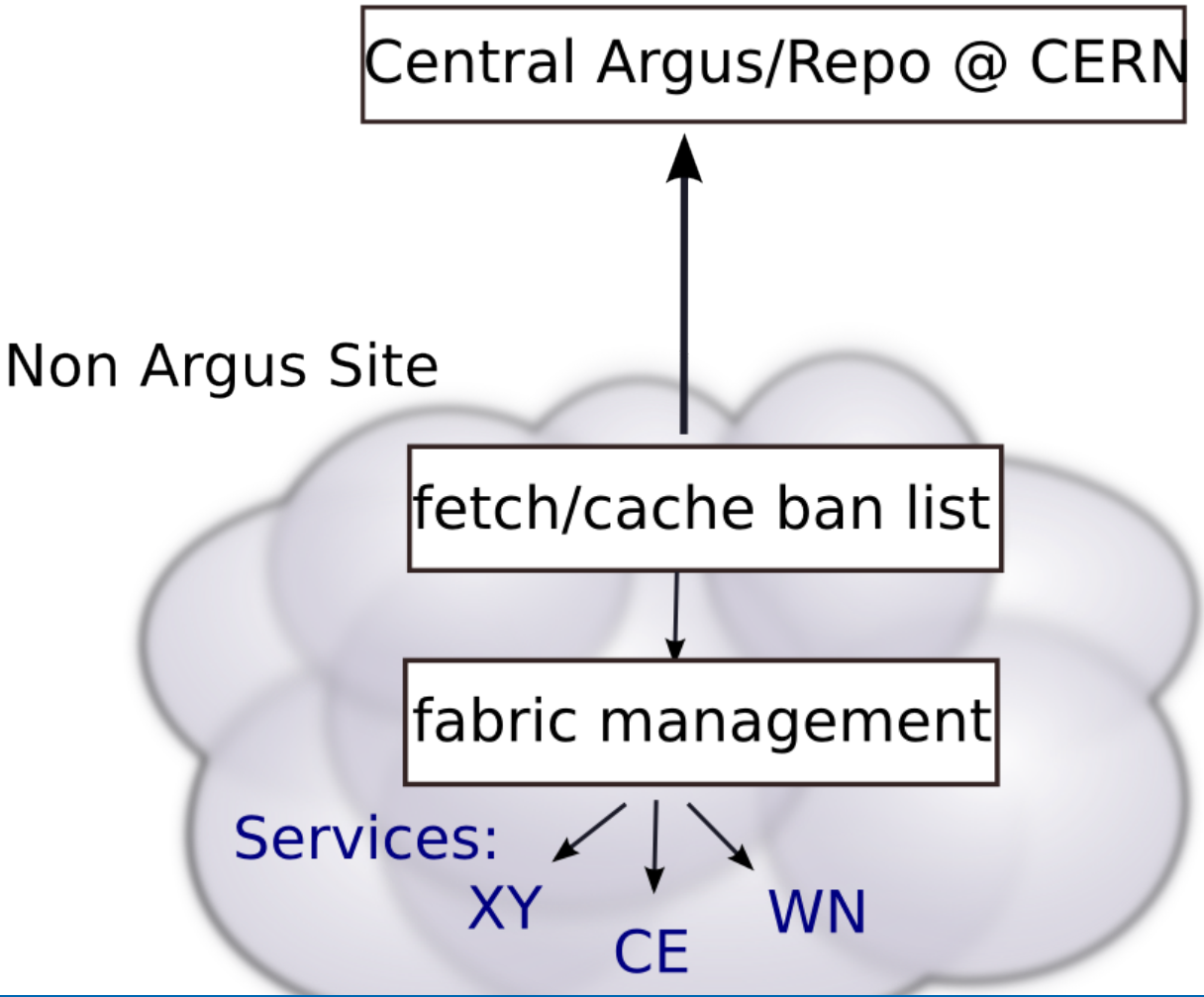
Non Argus services/sites/grids

Non Argus / banning information in plain text file

- peer grids in general do not use Argus.
- ARC-CE is not Argus aware, can consume plain text file.
- Unicore/Argus ?
- Some sites have implemented a banning mechanism in their fabric management.

Non Argus services/sites/grids

Example scenario for fabric-management usage



Technical implementation

Development

- Repository providing emergency suspension information. (CERN)
- Tools that securely download/process the emergency suspension information. (FOM/CERN)
- Interface to GOC-DB that provides role based information on who is allowed to access the emergency suspension information.(STFC/CERN)
- Documentation. (FOM)
- Example Configuration for Caching Service / Quattor Fabric-Management. (FOM)
- Testing. (FOM)