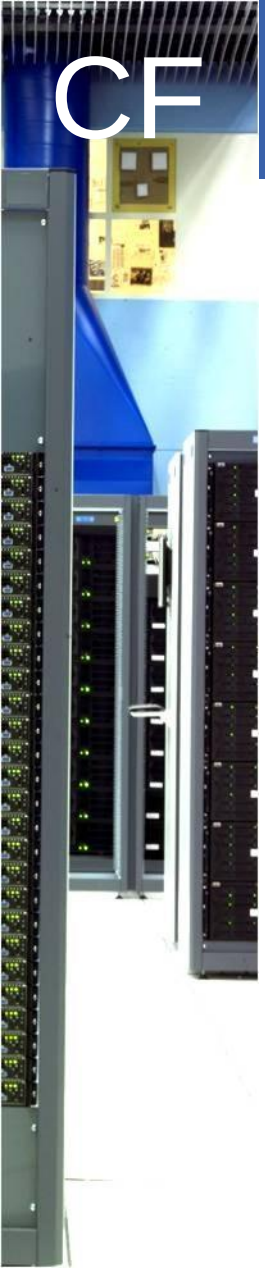


SINDES-2

Secure Information Delivery System

Version 2

Authors: Jan Dudziec

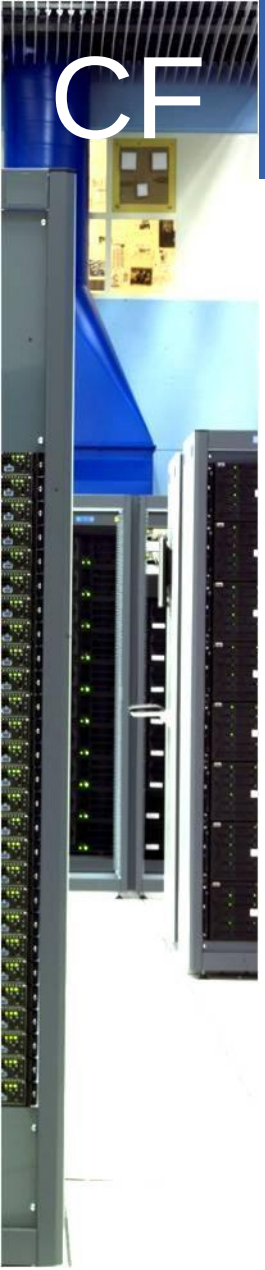
Ivan Fedorko

Speaker: Véronique Lefébure

CERN-IT-CF/ASI

Hepix Vancouver October 2011

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

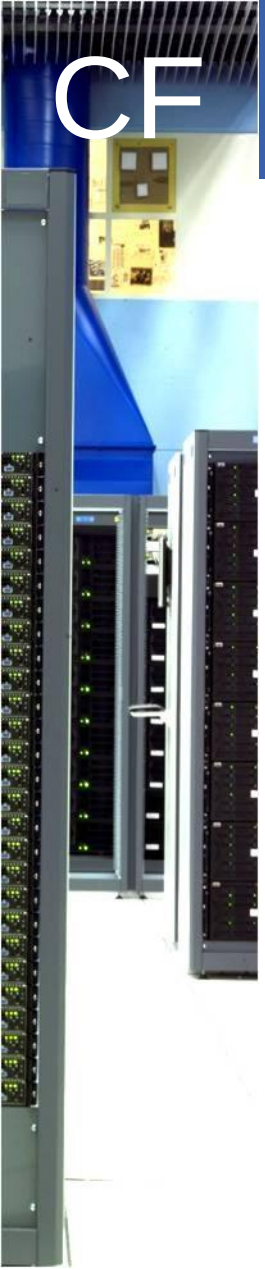


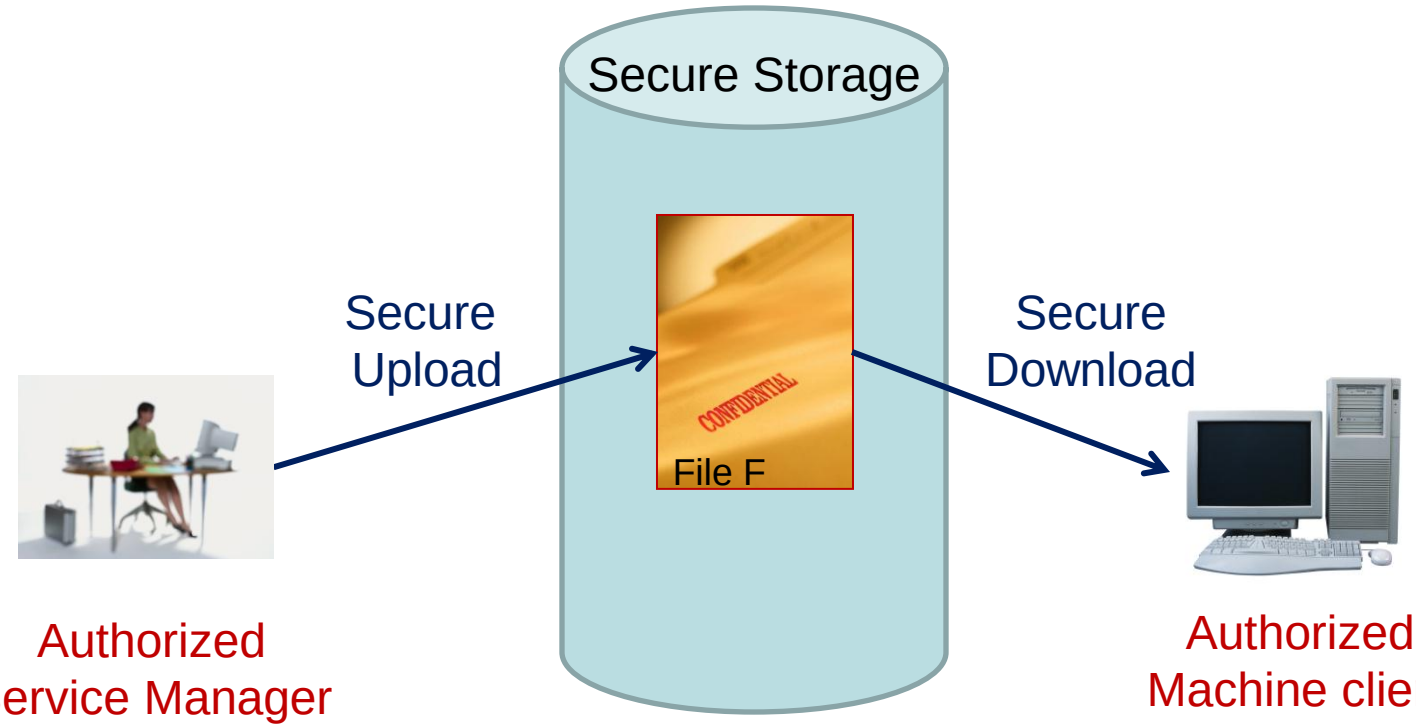
Outline

- Needs
- From SINDES-1 to SINDES-2
- Functionalities
- Architecture
- Differences with SINDES-1
- Project Status

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

Needs



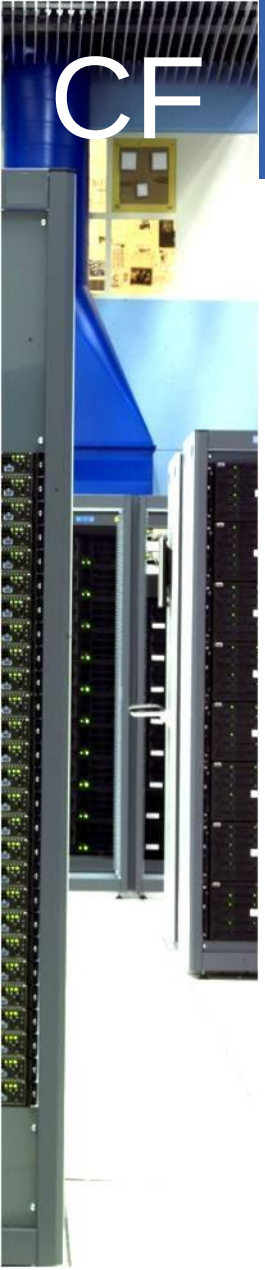


+ Flexible File Management

~100

~10000

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



From SINDES-1 to SINDES-2

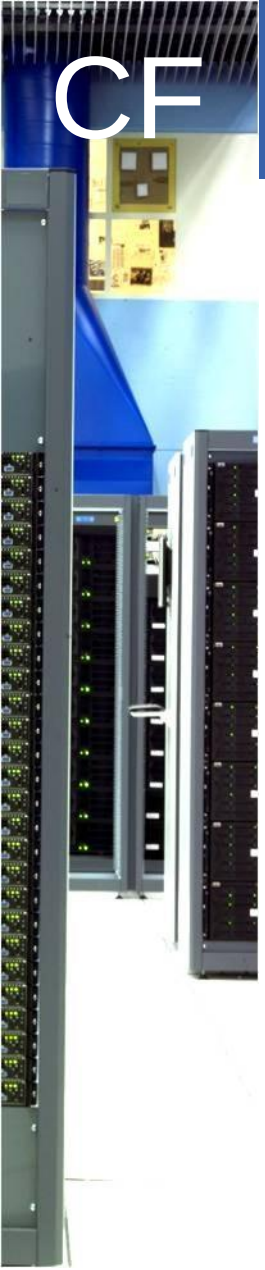
CERN IT Department

- SINDES-1
  - Developed and used at CERN since 2005
  - Also used outside CERN
  - Now old and un-maintained code
  - Need for more flexibility in terms of
    - File manipulation
    - Privilege management

→ SINDES-2

  - Implemented from scratch

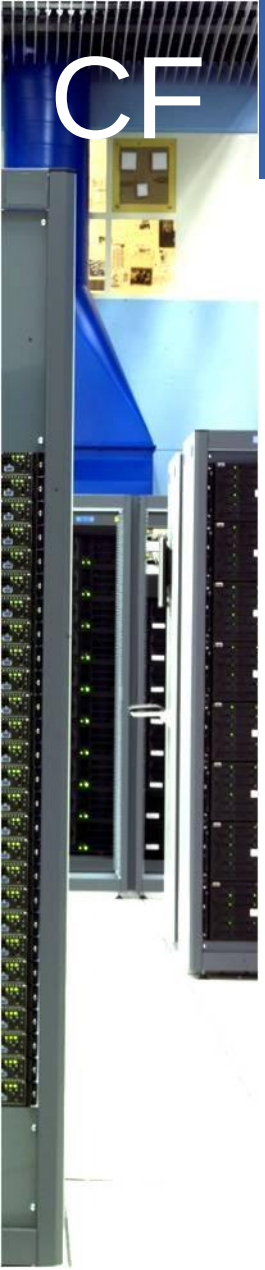
CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it



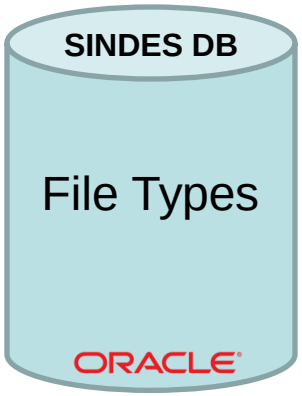
Functionalities

- Management of Privileges
  - Service Manager Privileges
  - Machine Clients Privileges
- Secure File handling
  - Storage
  - Upload
  - Download
- File Management
  - Versioning
  - Deletion

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

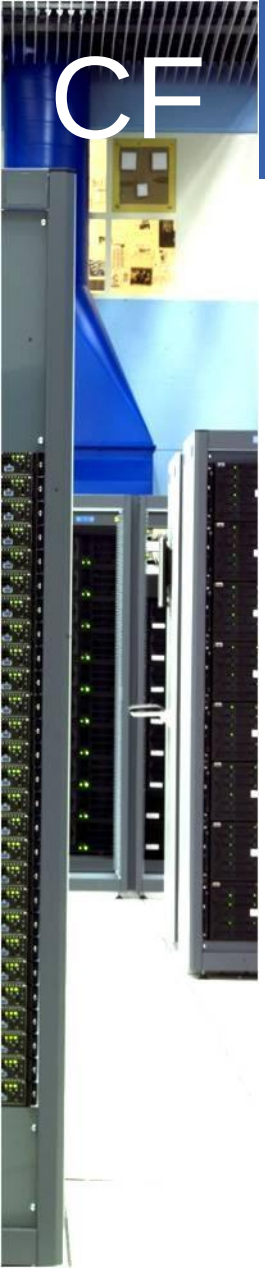


Files



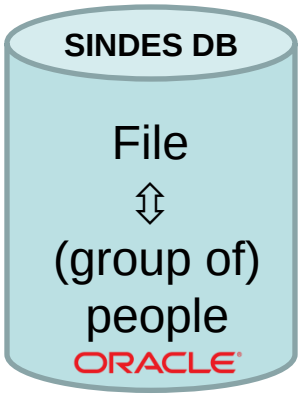
- Types:
  - Examples:
    - Grid certificate
    - Password file
    - /etc service configuration file
    - …
  - Defined by the SINDES administrator
    - can be different between sites
- Storage:
  - Flat file structure on a secure server
  - `.tar.gz` format
- Versioning:
  - SVN

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



Service Manager Privileges

CERN IT Department



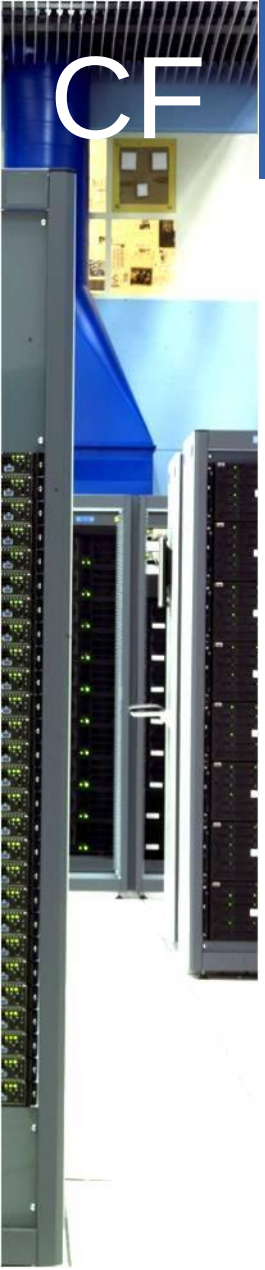
Action:

for a file F, a Service Manager defines

- What is the set of machines that need file F
- Which group of people can upload, update, delete file F

- Authentication
  - **Kerberos**
- Authorization
  - Specialized **Authorization Library**
    - Defined API: `is_user_privileged($target,$user) return 0/1`
    - Can interface to site databases (CMDB) or/and to “e-groups”,…
  - Example @CERN:
    - Sindes “power” user, or
    - Member of a group, or
    - Root user or “responsible” of all machines in the set

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

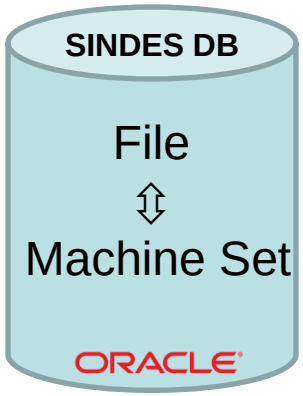


Machine Client Privileges

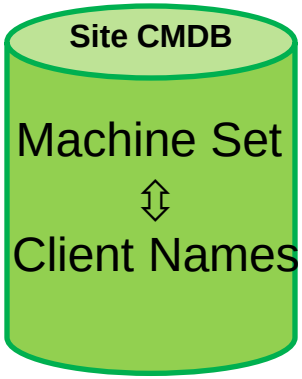
CERN IT Department

A file F can be mapped to

- A set of individual machines
- And/or to a set of (sub-)clusters of machines

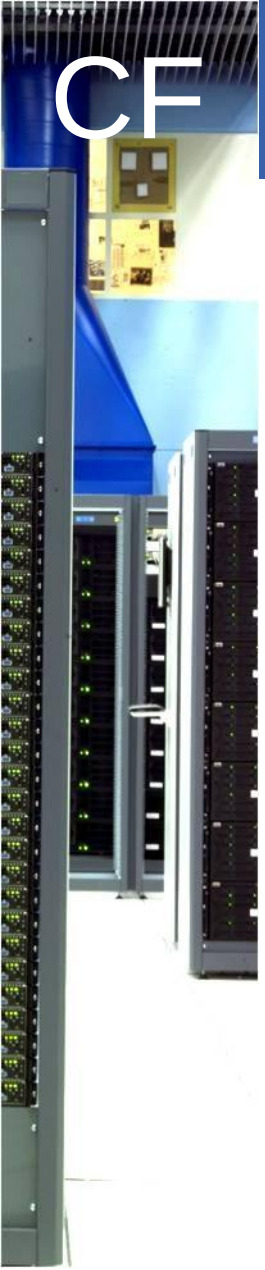


- Authentication:
  - **Kerberos**
- Authorization
  - Specialized **Authorization Library**
    - Defined API: `is_node_privileged($target,$node) return 0/1`
    - Interfaces to site databases describing the machine hierarchy




```
-Cluster1
 -subclusterA
  -host1
  -host2
 +subclusterB
 -host3
+cluster2
```

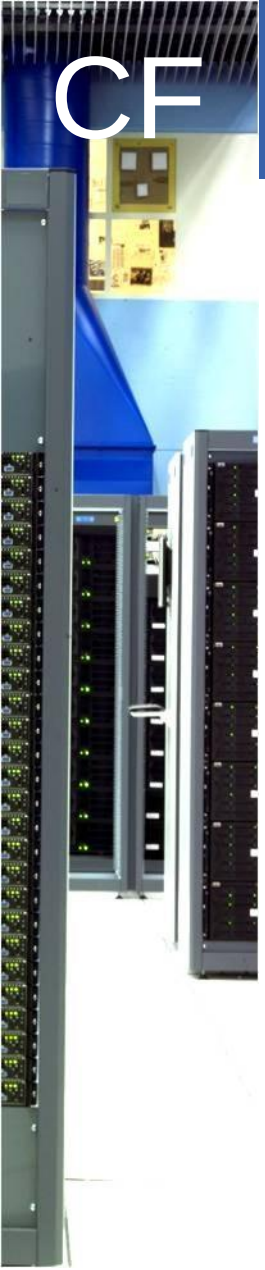
CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it



Roles in SINDES-2

	Enter new file Types	Declare Targets	Read/download files	Update/upload files
Administrator	☑	☑	☑	☑
“Power” user	☒	☑	☒	☒
End-user (Service Manager)	☒	☑ If authorized	☑ If authorized	☑ If authorized
Machine client	☒	☒	☑ If authorized	☑ If authorized

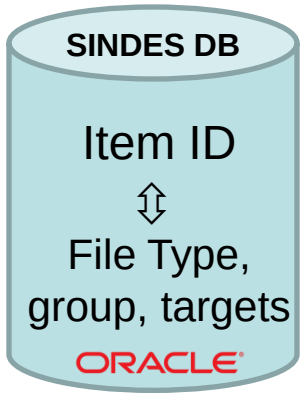
CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it

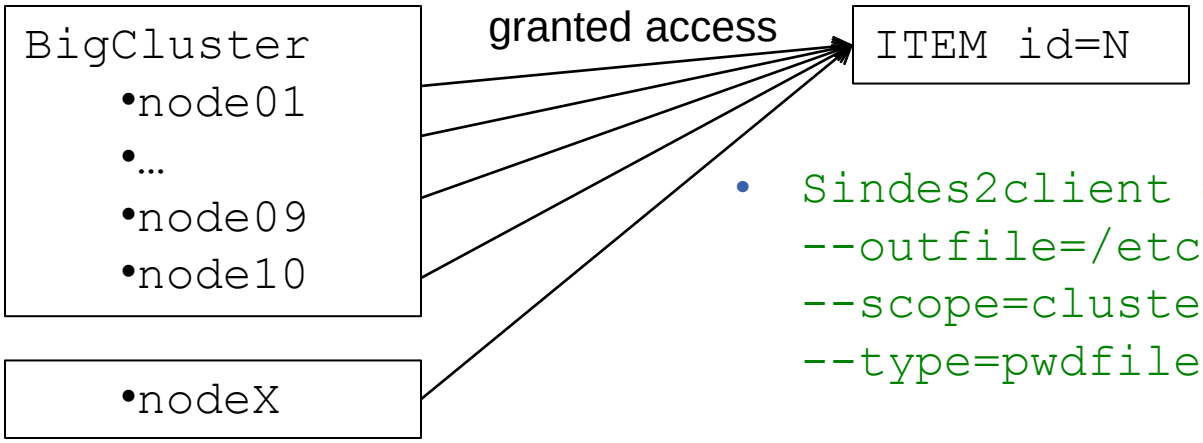


sindes2client cli

- sindes2client **create**
  --type=pwdfile
  --group=SMGroup1
  --user-upload=1
  --node-upload=0
  --add_target=cluster:BigCluster
  --add_target=node:nodeX

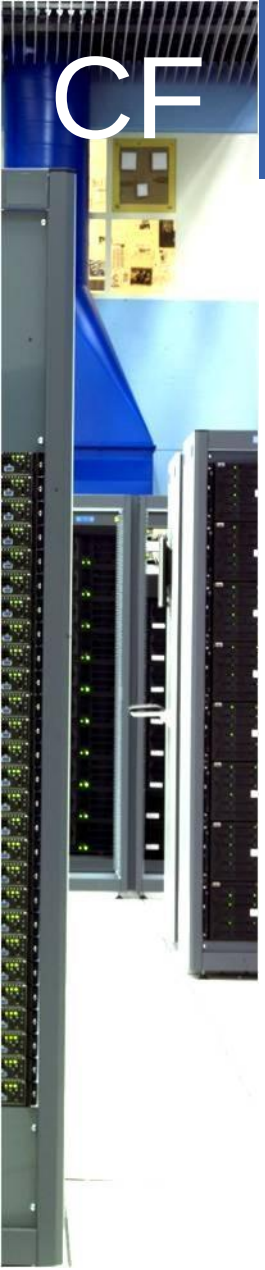
- Sindes2client **upload**
  --infile=mysecretfile --id=N





- Sindes2client **download**
  --outfile=/etc/pwd
  --scope=cluster
  --type=pwdfile

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



sindes2client cli (cont'd)

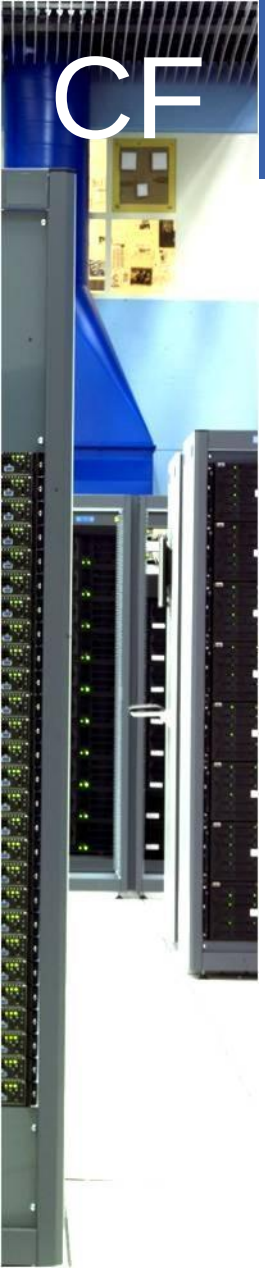
CERN IT Department

- Sindes2client **upload**
  --infile=mysecretfile**2** --id=N

→Item ID
•version 1
•version 2

- Sindes2client **download**
  --outfile=/etc/pwd
  --scope=cluster
  --type=pwdfile
  [--**version**=1 or 2] default=last version

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



sindes2client cli (cont'd)

- sindes2client **info** --id=N

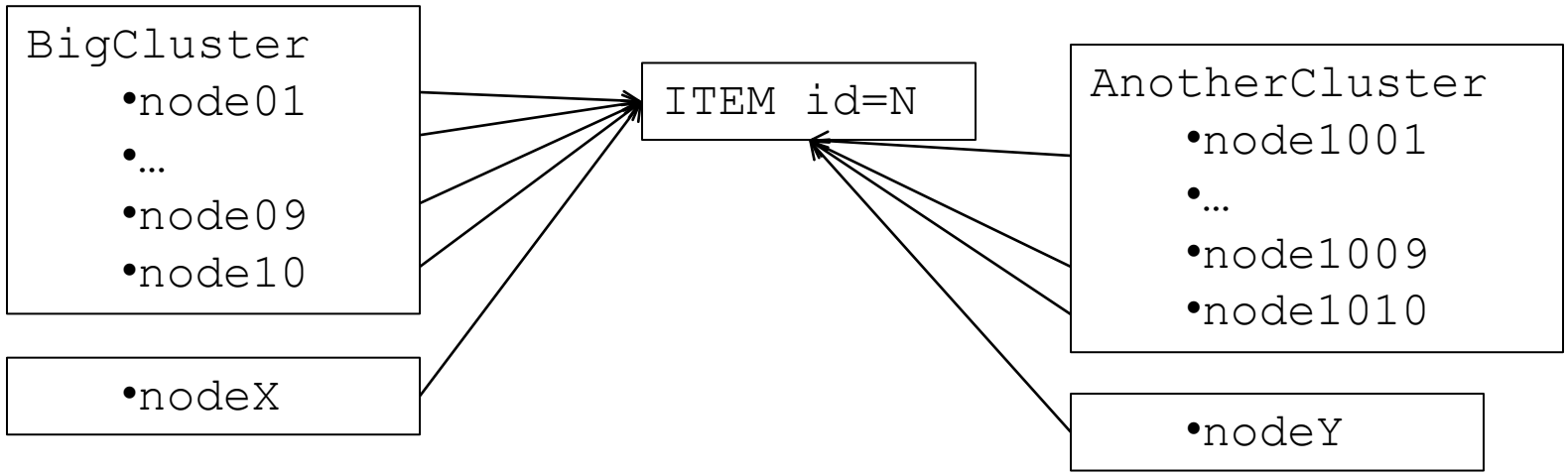
```
* Item
      - id:           N
      - owner:        vero
      - group:        SMGroup1
* Type:
      - name:         pwdfile
* Dates:
      - added:        10-OCT-11 01.44.57.000000 PM
      - modified:     12-OCT-11 03.10.32.000000 PM
* Privileges:
      - can user upload:     yes
      - can node upload:     no
* Targets:
      - cluster:BigCluster
      - node:nodeX
* Versions:
      -1 uploaded by user vero on 10-oct-11
      -2 uploaded by user vero on 12-oct-11
```

- sindes2client **info** --type pwdfile --scope cluster
  --target BigCluster

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

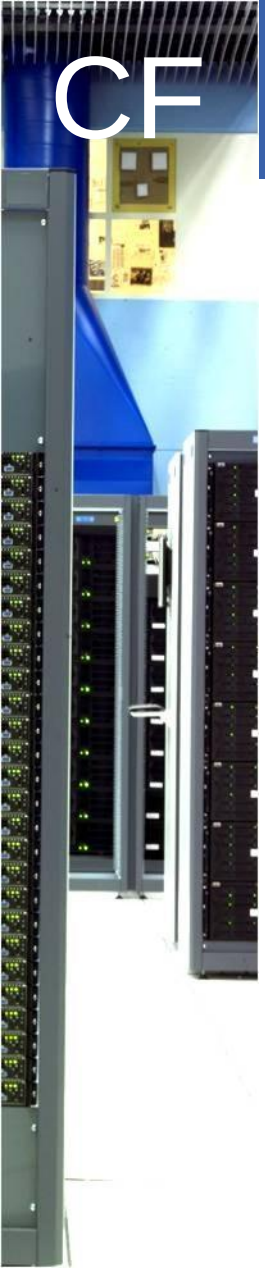
sindes2client cli (cont'd)

- sindes2client **modify** --id=N
  --add_target cluster:AnotherCluster
  --add_target node:nodeY



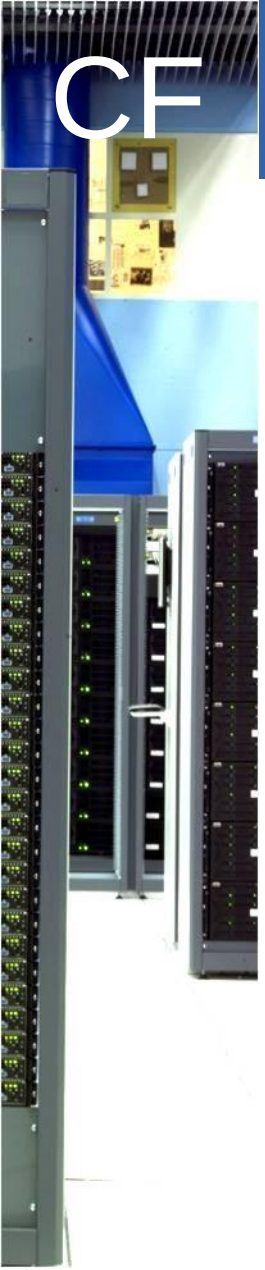
- sindes2client **modify** --id=N
  --del_target node:nodeX

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



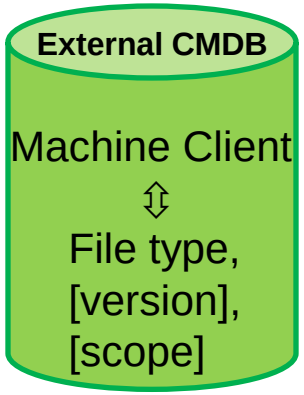
File Scope Shadowing

- Item ID=1 Type pwdfile
  - target = cluster:Cluster1
- Item ID=2 Type pwdfile
  - target = node:NodeX
    - If NodeX is part of Cluster1:
      - →Item 2 takes priority on Item 1 if scope is undefined at download time
- Validation at target creation time



File download by the machine

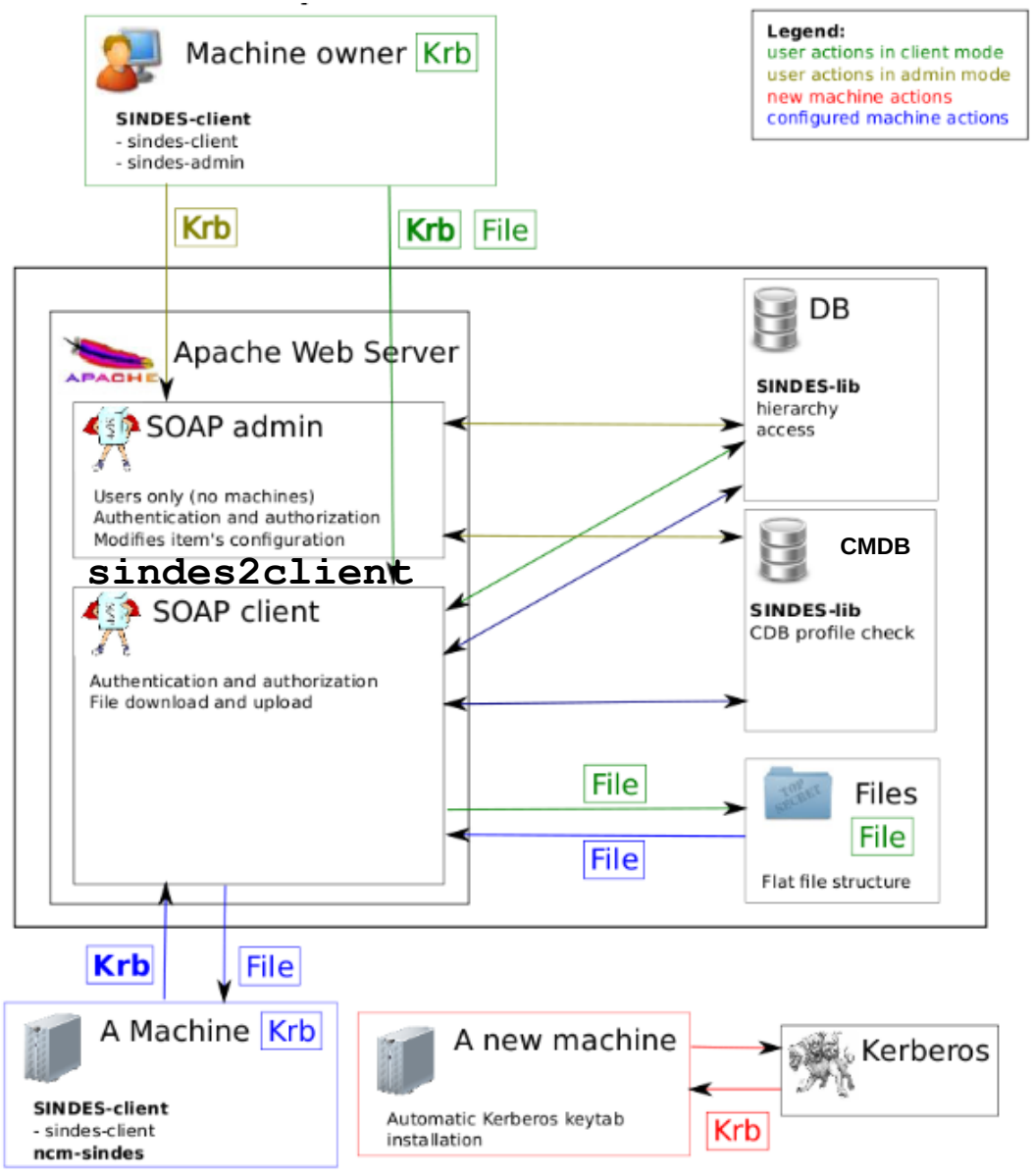
- Which files does machine M need to download ?
  - Defined in CMDB



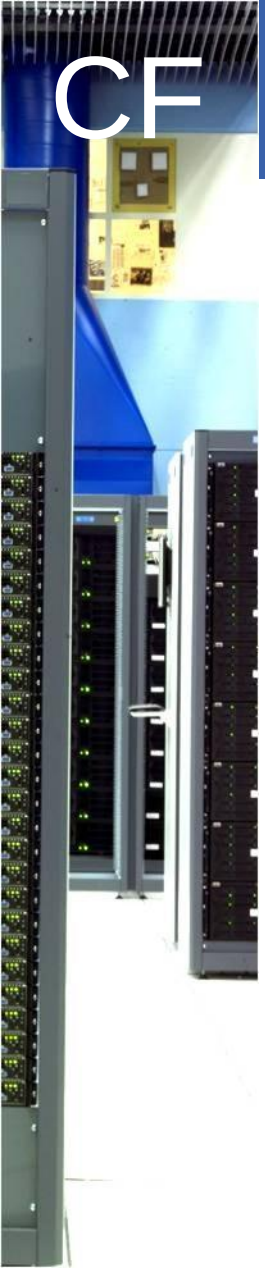
  - Shadowing is possible
- How to download them ?
  - Quattor context: `ncm-sindes2`
    - Calls the "`sindes2client download`" command

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

Global Architecture



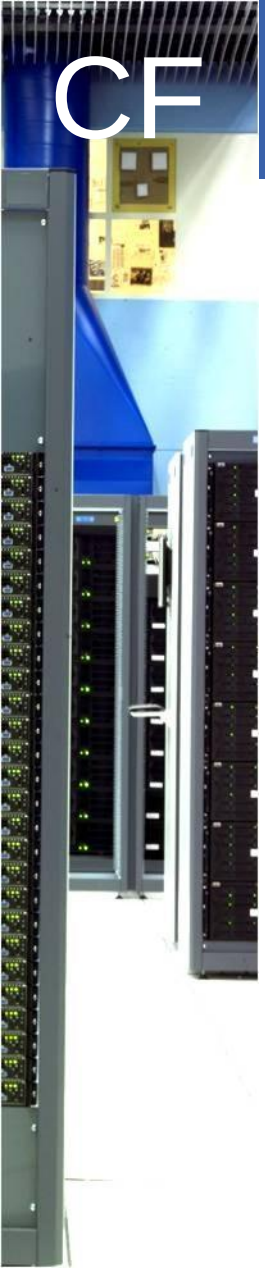
CERN IT Department
CH-1211 Geneva 23
Switzerland
www.cern.ch/it



Comparison with Sindes-1

	SINDES v1	SINDES v2	
Status	In production since 2005	Under test	
Authentication of users	Kerberos	Kerberos	
Authentication of machines	SINDES CA	Kerberos	new
Authorization of users	Local “sindes” user and Site CMDB	Site CMDB & SINDES DB	
Authorization of machines	Site CMDB	Site CMSDB & SINDES DB	new
File upload	Only end-users	Machines & end-users	
File download	Only machines	Machines & end-users	new
File scopes	Cluster/node	Any pre-defined scope	new
File versioning	none	SVN	new
#lines	~10000	About 3x less	new

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

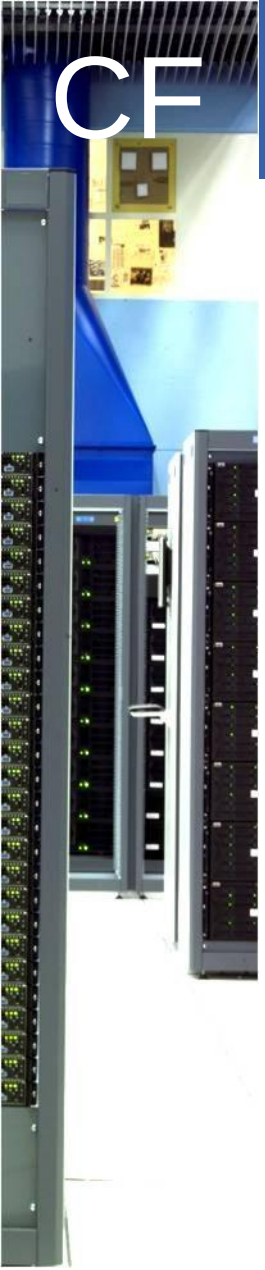


Migration from S1 to S2

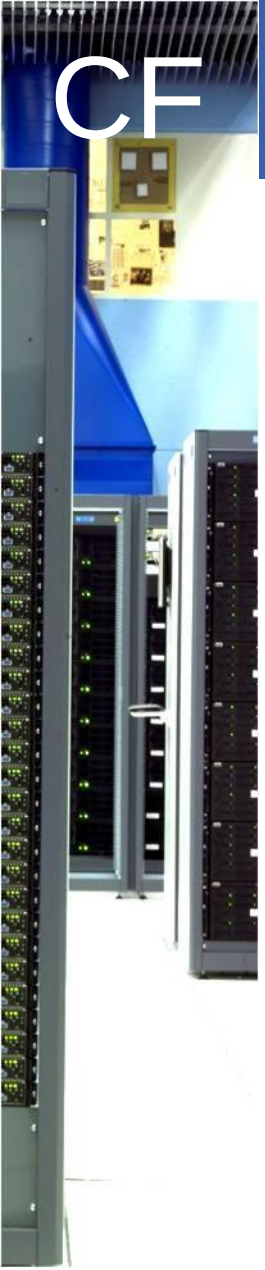
- By end of 2011:
  - One non-critical cluster to be managed with Sindes-2
- During 2012:
  - Migration of all clients

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

Source

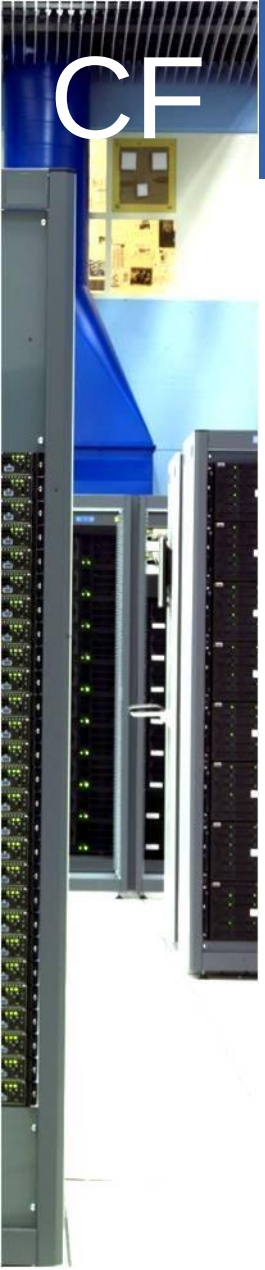


- Currently on CERN SVN
- Documentation to come
- Will be published on the Quattor SourceForge repository, under the Apache2 licence (see http://quattor.org)
  - But is CMDB (Quattor) independent



Conclusion

- SINDES-2
  - Solves file management issues
  - Can be used for non-quattor-managed machines
  - Uses standard Apache web server, SOAP and Kerberos
    - Ease of maintenance
  - Is modular: Authentication and Authorization modules are plug-in's
    - Libraries can be used by other applications
  - Code reviewed by our Computer Security team



Acknowledgements

CERN IT Department

- Main author:
  - Jan Dudziec
- Supervisor:
  - Ivan Fedorko
- Security review and advice:
  - Sebastian Lopienski and the CERN Computer Security Team
- Kerberos expertise:
  - John Heffermen
- Ideas, advice, feedback:
  - CERN IT colleagues and Experiments VO users

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