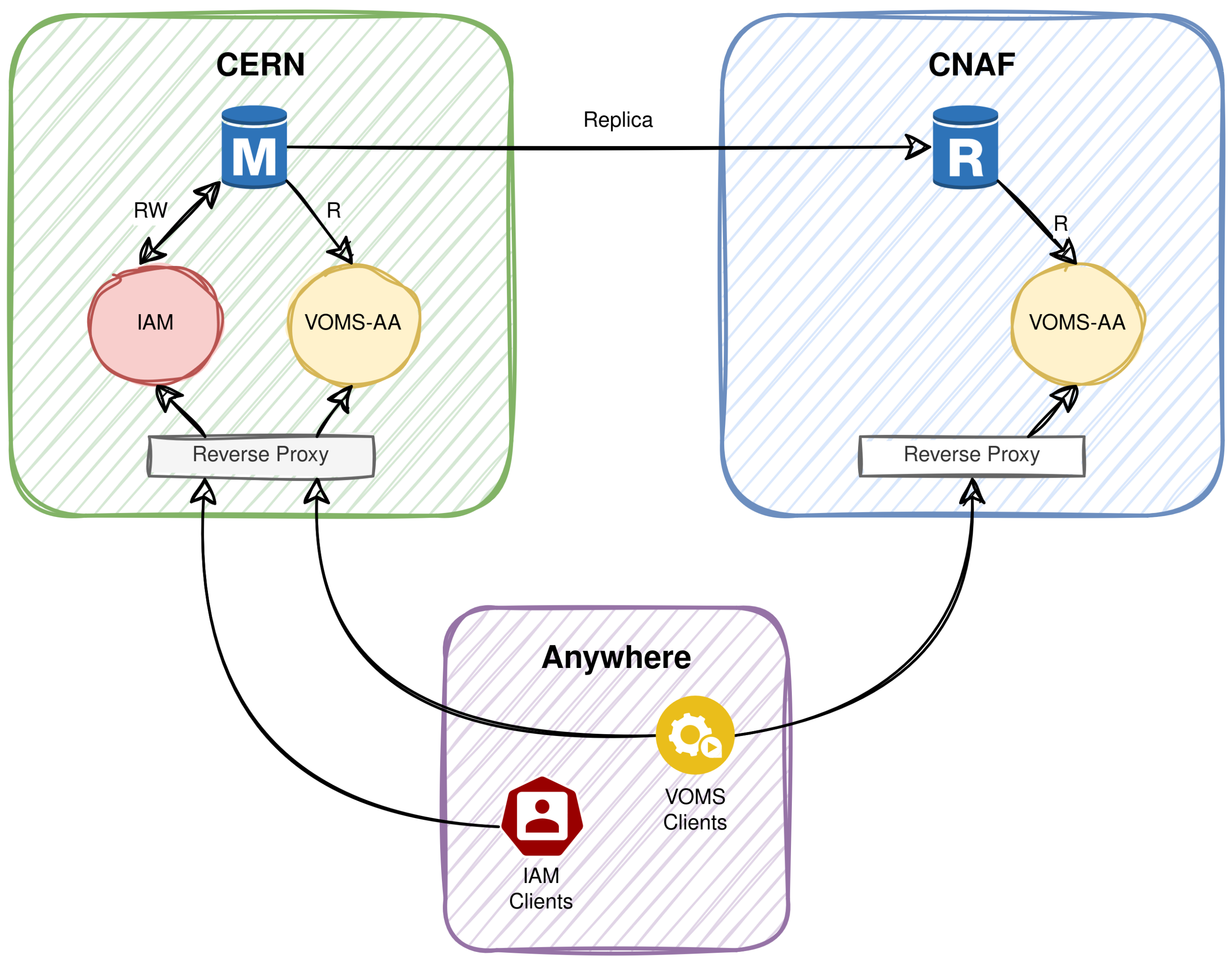
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
terabit

Geographic replication of the VOMS Attribute Authority service

D. Marcato, INFN-LNL, Legnaro (PD), Italy,
F. Agostini, J. Gasparetto, F. Giacomini, R. Miccoli, E. Vianello, S. E. Zotti , INFN-CNAF, Bologna (BO), Italy

WHY?

- VOMS servers provide x509 proxy certificates to access resources based on Virtual Organizations (VO)
- Most VOs are moving to token-based authentication/authorization using IAM
  - Smaller VOs are still using VOMS
  - Both will live together
- VOMS-AA implements the VOMS server interface by using the data from a IAM DB
  - Existing VOMS clients can connect to VOMS-AA seamlessly
- Starting this year legacy VOMS admin servers will be withdrawn at CERN because of VOMS Admin EOL scheduled on June 30th
- Legacy VOMS servers could be deployed with geo-replication
  - VOMS-AA is required to provide the same level of reliability, fault-tolerance and load bearing capacity



HOW?

Using MySQL 8.3 Replication

PRIMARY

```
CREATE USER 'replicator'@'%' IDENTIFIED BY 'pwd' REQUIRE SSL;
GRANT REPLICATION SLAVE ON *.* TO 'replicator'@'%';
```

```
[mysqld]
server-id = 1
log_bin = mysql-bin
binlog_do_db = iam

general_log = 1
general_log_file = /var/log/mysql/primary.log

ssl_ca=/certs/ca-cert.pem
ssl_cert=/certs/server-cert.pem
ssl_key=/certs/server-key.pem
```

REPLICA

```
STOP REPLICA;
CHANGE REPLICATION SOURCE TO
  SOURCE_HOST='db-primary.test.example',
  SOURCE_USER='replicator',
  SOURCE_PASSWORD='pwd',
  SOURCE_SSL=1,
  SOURCE_SSL_CA = '/certs/ca-cert.pem',
  SOURCE_SSL_CERT = '/certs/client-cert.pem',
  SOURCE_SSL_KEY = '/certs/client-key.pem',
  SOURCE_SSL_VERIFY_SERVER_CERT=1;
START REPLICA;
```

```
[mysqld]
server-id = 2
log_bin = mysql-bin
read_only = 1

general_log = 1
general_log_file = /var/log/mysql/replica.log

replicate-do-table=iam.iam_account
replicate-do-table=iam.iam_account_attrs
replicate-do-table=iam.iam_account_authority
replicate-do-table=iam.iam_account_group
replicate-do-table=iam.iam_address
replicate-do-table=iam.iam_authority
replicate-do-table=iam.iam_aup
replicate-do-table=iam.iam_aup_signature
replicate-do-table=iam.iam_group
replicate-do-table=iam.iam_group_labels
replicate-do-table=iam.iam_oidc_id
replicate-do-table=iam.iam_reg_request
replicate-do-table=iam.iam_saml_id
replicate-do-table=iam.iam_ssh_key
replicate-do-table=iam.iam_user_info
replicate-do-table=iam.iam_x509_cert
replicate-do-table=iam.iam_x509_proxy
```

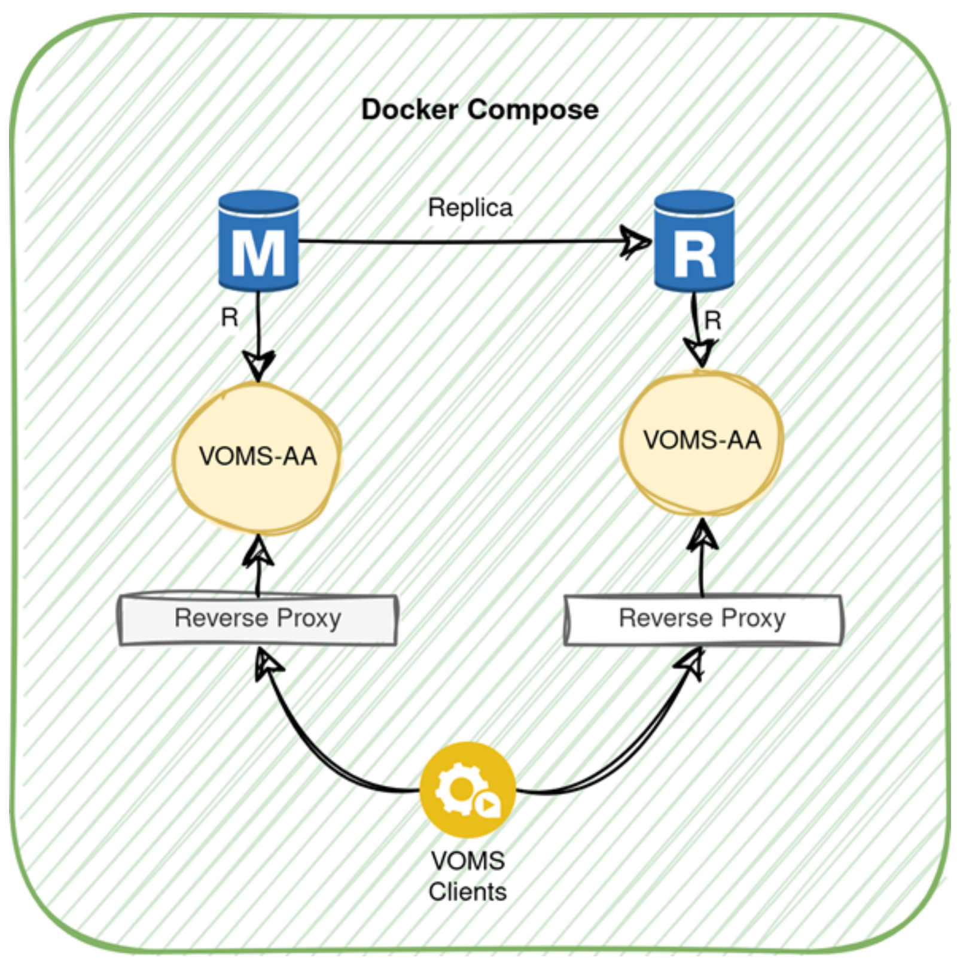
VOMS CLIENT

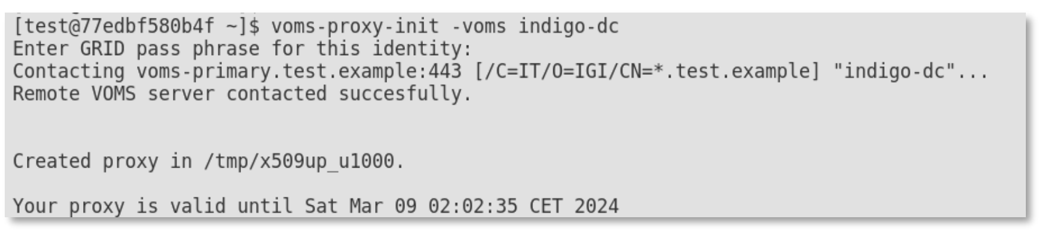
- "voms-primary" "voms-primary.test.example" "443" "/C=IT/O=IGI/CN=*.test.example" "indigo-dc"
- "voms-replica" "voms-replica.test.example" "443" "/C=IT/O=IGI/CN=*.test.example" "indigo-dc"
- "indigo-dc" "voms-primary.test.example" "443" "/C=IT/O=IGI/CN=*.test.example" "indigo-dc"
- "indigo-dc" "voms-replica.test.example" "443" "/C=IT/O=IGI/CN=*.test.example" "indigo-dc"

PROOF OF CONCEPT

- Single docker-compose* with:
  - **trust**: GRID CA certificates plus the igi-test-ca for test certificates
  - **db-primary**: a mysql 8.3 dump of the IAM DB for test environment. The user **test0** has a certificate with DN /C=IT/O=IGI/CN=test0 linked to his account and he also is part of the **indigo-dc** group. A second SQL script creates a replicator user for replica.
  - **db-replica**: read-only replica of db-primary
  - **ngx-primary** and **ngx-replica**: an extension to NGINX, used for TLS termination, reverse proxy and possibly VOMS proxies validation.
  - **vomsaa-primary** and **vomsaa-replica**: the main voms-aa microservices, each connected to their own DB.
  - **client**: it is a single container containing GRID clients (in particular voms-proxy-init) used to query both the primary and replica voms-aa (via ngx).

* Based on the work from F. Agostini

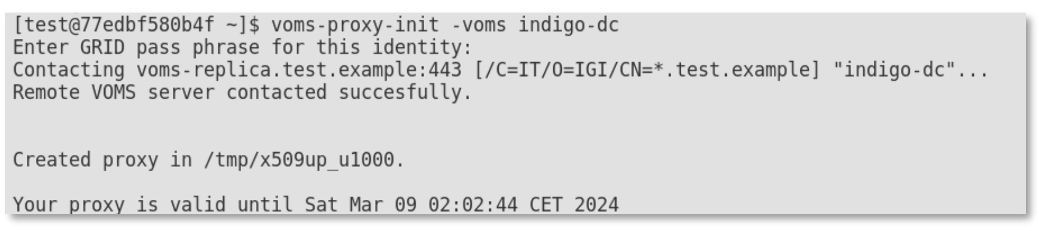




```
[test@77edbf580b4f ~]$ voms-proxy-init -voms indigo-dc
Enter GRID pass phrase for this identity:
Contacting voms-primary.test.example:443 [/C=IT/O=IGI/CN=*.test.example] "indigo-dc"...
Remote VOMS server contacted succesfully.


Created proxy in /tmp/x509up_u1000.

Your proxy is valid until Sat Mar 09 02:02:35 CET 2024
```



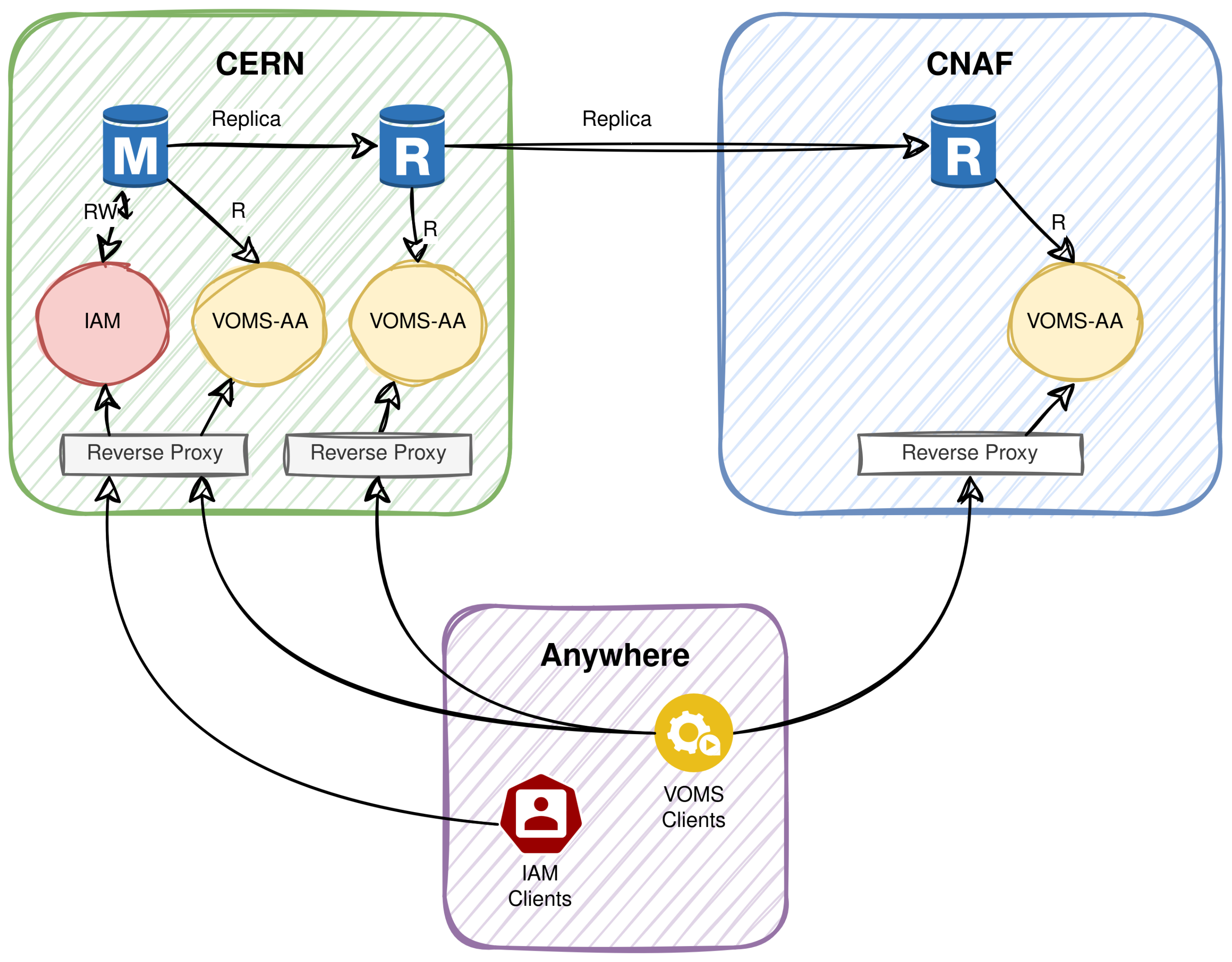
```
[test@77edbf580b4f ~]$ voms-proxy-init -voms indigo-dc
Enter GRID pass phrase for this identity:
Contacting voms-replica.test.example:443 [/C=IT/O=IGI/CN=*.test.example] "indigo-dc"...
Remote VOMS server contacted succesfully.


Created proxy in /tmp/x509up_u1000.

Your proxy is valid until Sat Mar 09 02:02:44 CET 2024
```

ENHANCEMENTS

- All the binary log are sent over the network, including all IAM tables
  - This introduces useless network traffic and potential security problems
  - Use a **double REPLICA** to limit network traffic to the remote site
- Only the VOMS-AA tables are present in the first replica. Its logs are sent over the network but they contain only relevant information
- Run the **VOMS-TESTSUITE** against this setup to validate its functionality
  - Introducing the support for multiple hosts in the voms-testsuite



NETWORKING

We use a few distinct networks, similar to a real scenario:

- **site1-lan** and **site2-lan**: The internal LAN of the two sites. These are used to connect the DB, VOMS-AA and NGINX between them inside the same site.
- **site-to-site-tunnel**: A VPN network or any tunnel network between the two sites, used by db-remote to connect to db-replica.
- **wan**: The NGINX servers are exposed on the public network so that the clients can connect from anywhere.

https://github.com/indigo-iam/iam/tree/voms-replica/compose/voms-replica