УДК [539.12 + 539.14] : [621.38 + 004.7 + 004.6] (063)
ББК 22.381 я 431 + 22.381.9 я 431 + 32.973.2 – 018 я 431
N91

The contributions are reproduced directly from the originals presented by the Organizing Committee.

Nuclear Electronics & Computing (NEC'2001): International Symposium (18; N91 2001; Varna).

Proceedings of XVIII International Symposium on Nuclear Electronics & Computing (NEC'2001) (Varna, Bulgaria, Sept. 12–18, 2001). — Dubna: JINR, 2002. — 261 p.: ill.

ISBN 5-85165-690-5

The Proceedings of XVIII International Symposium on Nuclear Electronics & Computing (NEC'2001) contain the papers presented at NEC'2001, which was held 12–18 September 2001 (Varna, Bulgaria). The symposium was organized by the Joint Institute for Nuclear Research (Dubna, Russia), European Laboratory for Particle Physics (CERN) (Geneva, Switzerland) and the Institute for Nuclear Research and Nuclear Energy of the Bulgarian Academy of Sciences (Sofia, Bulgaria). The symposium was sponsored by INTAS, UNESCO and Lirex^{BG}.

The symposium was devoted to the problems of detector & nuclear electronics, computer applications for measurement and control in scientific research, triggering and data acquisition accelerator and experiment control systems, information & data base systems, computer networks for scientific research, data & storage management and GRID computing.

Ядерная электроника и компьютинг (NEC'2001): Международный симпозиум (18; 2001; Варна).

Труды XVIII Международного симпозиума по ядерной электронике и компьютингу (NEC'2001) (Варна, Болгария, 12–18 сентября 2001 г.). — Дубна: ОИЯИ, 2002. — 261 с.: ил.

ISBN 5-85165-690-5

Труды XVIII Международного симпозиума по ядерной электронике и компьютингу (NEC'2001) содержат доклады, представленные на «NEC'2001», который проходил с 12 по 18 сентября в г. Варне (Болгария). Симпозиум был организован Объединенным институтом ядерных исследований (Дубна, Россия), Европейской лабораторией физики частиц (CERN) (Женева, Швейцария) и Институтом ядерных исследований и ядерной энергетики Болгарской академии наук (София, Болгария). Спонсорами симпозиума были INTAS, UNESCO и Lirex^{BG}.

Симпозиум был посвящен проблемам детекторной и ядерной электроники, применению вычислительной техники для измерений и контроля, системам сбора данных, системам автоматизации экспериментальных установок, информационным системам и базам данных, проблемам локальных и глобальных коммуникаций, системам массовой памяти и технологии GRID.

УДК [539.12 + 539.14] : [621.38 + 004.7 + 004.6] (063)
ББК 22.381 я 431 + 22.381.9 я 431 + 32.973.2 – 018 я 431

ISBN 5-85165-690-5

CON

EU-DataGrid segment in Russia. Testbed WP6

V. Ilyin[1], N. Kruglov[1], A. Kryukov[1], V. Korenkov[2], V. Kolosov[3], V. Mitsyn[2], L. Shamardin[1], E. Tikhonenko[2].
[1]SINP MSU, Moscow, Russia
[2]JINR Dubna, Russia
[3]ITEP Moscow, Russia

Russia participates in the following work packages of the EU-DataGrid: WP6 Testbed, WP8 HEP Applications. Building of DataGrid infrastructure in Russia started in Moscow region on the base of several institutes (SINP MSU, ITEP, JINR, IHEP and some others). Further development for other regions (St. Petersburg, Novosibirsk) and institutes is under discussion. Main goal for Russian EU-DataGrid segment is to investigate new technologies required for creating Regional center for LHC computing in Russia.

Research directions for the project include

- Data transfer and traffic investigation
  - Investigation of local area links traffic speed and performance with different size of buffering disk server
  - Practical implementation and testing of high-speed site-to-site data replication through Moscow region backbone.
  - Practical implementation and testing of site-to-site data replication Moscow-CERN.
- Investigation of distributive and local data storage
  - The study of feasibility and robustness of disk-based, tapeless data repositories of data, assembled from low cost industrial mass production components; investigation of novel storage technologies.
  - Investigation of the high capacity storage system implementation (tape robots) at the conditions of medium/long range domestic communications structure.
- GRID tools (middleware) in HEP applications
  - Elaboration of elements of cooperative network management for communications, connecting participating institutes.
  - GRID system software tools test in essentially heterogeneous local and wide-area network facilities.
- Research of effectiveness of CPU utilization of production farms (PC clusters)
  - Investigation of effectiveness of CPU utilization and other computer resources during test data production using distributed OO databases.
  - The study of efficiency of local schedulers of batch tasks and their scalabilities and robustness.

Our team participated in EU-DataGrid WP6 Testbed0, which included Globus installation, configuration of GRIS and GIIS servers for both institute and country levels, creation of own DataGrid Certification Authority.

Now we are participating in WP6 Testbed1, which deals with significant computational resources (about 160 Pentium III 1GHz CPUs and 7.5 TB disk space on IDE fileservers) and wide range of used software. The following institutes are participating in this activity: SINP MSU (Moscow), IHEP (Protvino), JINR (Dubna), ITEP (Moscow).

Software environment for Testbed1 is RedHat Linux 6.2 (with kernels 2.2.14-2.2.19), PBS batch system, NFS & AFS file system servers, ObjectivityDB (GDMP 1.1), Globus toolkit 2 ("EDG" distribution), CONDOR batch system on several farms.

Network solution for Testbed1 includes Fast Ethernet (100Mbit) LANs, 400 Mbps interfaces on fileservers, regional and international links up to 1 Gbps.

Russian National GIIS

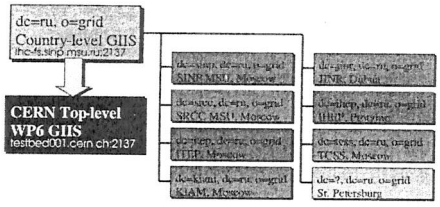

Fig. 1

The configuration of Russian national GIIS is shown on Fig. 1. All institutes participating in the EU-DataGrid setup own institute-level GIIS servers. All institute-level GIIS servers are then registered in Russian National GIIS for the EU-DataGrid, which is installed, and running in SINP MSU, Moscow (ldap://lhc-fs.sinp.msu.ru:2137).

Country-level GIIS is registered in the top-level GIIS server for the Testbed0 which is installed in CERN (ldap://testbed001.cern.ch:2137). GIIS servers use MDS components from Globus Toolkit 1.1.3.

Institutes registered in the country-level GIIS are: SINP MSU (Moscow), SRCC MSU (Moscow), ITEP (Moscow), KIAM (Moscow), JINR (Dubna), IHEP (Protvino). In the nearest future TCSS (Moscow) and several St. Petersburg and Kharkov institutes will setup their GIIS servers and register them in country-level GIIS. SRCC, KIAM and TCSS are not involved in CERN projects, but they are participating in Russian DataGrid project.

Configuration of SINP MSU GIIS server

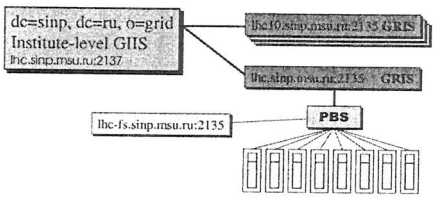

Fig. 2

SINP MSU GIIS server is an example of a "typical" institute-level GIIS server. Its configuration is shown on Fig. 2.

Server receives information from several nodes running Globus 1.1.3 Gatekeeper and GRIS service. One of the nodes with Gatekeeper is a PBS farm interface node, and job submission can be done to PBS system through this node. Information about fork jobmanager queues is published in GRIS and is available in GIIS. Support for the PBS jobmanager in Globus 1.1.3 is incomplete, so there is no information about running jobs on PBS cluster in the GRIS. We are testing some special software written in KIAM for publishing PBS jobs information in GRIS, but tests results are still incomplete.

Certification Authority

Globus Toolkit uses X509v3 cryptography for authentication and encryption, this means that the Certification Authority (CA) is required for operation. WP6 security team decided not to use the Globus.org CA (/C=US/O=Globus/CN=Globus Certification Authority) for EU-DataGrid and to setup local CAs.

The Russian DataGrid CA (/C=RU/O=DataGrid/CN=Russian DataGrid CA) provides Globus X509v3 certificates for Russian DataGrid Testbed community. The CA is located at SINP MSU.

The certificate identifies the individual as a member of the Russian DataGrid Testbed. Russian DataGrid CA issues certificates for Russian institutes, laboratories and individuals participating in EU-DataGrid project. A certificate identifies authenticy of the owner's name, but does not guarantee any rights. Only the local administrator of the resource gives or cancels the permission to use the resource. The Russian DataGrid CA is no the only CA for Russia in the EU-DataGrid project. There can be more CAs for different regions. Russian DataGrid CA uses registration authorities scheme for issuing certificates.

CAs are trusted by lots of people, so we mı
This means that the CA must be hack proof, a
the certificate. In "classical" CA working sch
the certificate requester in some way (by a ph
certificate. This scheme is good for small CA
amount of requests per day we can come to pe
also not the best way for validating the reques

Registration Authority (RA) is a place whe
requesters is performed. We can setup several
this should solve the problems with a "classic
RAs and does not make any validation for the
revocation mechanisms for RAs so that they c
the CA, which again are not validated by the
grid-cert-request program is sent not to the C
example). The administrator validates the req
signs it with his Globus certificate. This signe
checks the signature on the request, and later
other checks. Our implementation of the RA
revocation requests.

The email robot at CA understands not onl
requests that can be used by a RA for certific
renewal requests (generated with grid-cert-rer
several supplementary functions like checkin
certificates with given Distinguished Name o
track on certificate expiration dates and will a
grid-cert-renew (challenge in renew requests

Certificate Revocation Lists

Certificate Revocation Lists (CRLs) are th
Globus Security Infrastructure (GSI). This m
on the hosts running Globus as fast as it is po

All current CRL update solutions are base
These solutions have several problems:

- CRL update frequency on the host oft
  the CA. This causes too frequent CRI
- In future frequent web updates of the
- Signing policies for the CAs are not u

We are now developing the new CRL upd
updating certificates on the Russian DataGric
special notification to all sites, and after this
allows to relinquish the scheduled updates an

Acknowledgments

The work was supported by CERN-INTA

net (100Mbit) LANs, 400 Mbps interfaces
Gbps.

he configuration of Russian national GIIS
own on Fig. 1. All institutes participating
e EU-DataGrid setup own institute-level
servers. All institute-level GIIS servers
ien registered in Russian National GIIS for
U-DataGrid, which is installed, and
ng in SINP MSU, Moscow
://lhc-fs.sinp.msu.ru:2137).
)untry-level GIIS is registered in the top-
GIIS server for the Testbed0 which is
IIS servers use MDS components from

INP MSU (Moscow), SRCC MSU
Dubna), IHEP (Protvino). In the nearest
Kharkov institutes will setup their GIIS
KIAM and TCSS are not involved in
ataGrid project.

er

P MSU GIIS server is an example of a
l" institute-level GIIS server. Its
ıration is shown on Fig. 2.
/er receives information from several
unning Globus 1.1.3 Gatekeeper and
ervice. One of the nodes with Gatekeeper
S farm interface node, and job
sion can be done to PBS system through
le. Information about fork jobmanager
is published in GRIS and is available in
s incomplete, so there is no information
testing some special software written in
it tests results are still incomplete.

tication and encryption, this means that
n. WP6 security team decided not to use
ification Authority) for EU-DataGrid

-Russian DataGrid CA) provides Globus
unity. The CA is located at SINP MSU.
)f the Russian DataGrid Testbed.
itutes, laboratories and individuals
fies authenticy of the owner's name, but
or of the resource gives or cancels the
A is no the only CA for Russia in the
nt regions. Russian DataGrid CA uses

CAs are trusted by lots of people, so we must guarantee "correct" issuing of the certificates. This means that the CA must be hack proof, and only valid real persons should be able to obtain the certificate. In "classical" CA working scheme CA administrator performs the validation of the certificate requester in some way (by a phone call for example) and after that issues the certificate. This scheme is good for small CAs with small amount of requests, but with large amount of requests per day we can come to performance problems. Phone validation of users is also not the best way for validating the requests, direct contact with person is much more secure.

Registration Authority (RA) is a place where "physical" validation of the certificate requesters is performed. We can setup several RAs in the different institutes and divisions and this should solve the problems with a "classical" CA. CA administrator in this case trusts to the RAs and does not make any validation for the requests signed by a RA. We can also implement revocation mechanisms for RAs so that they can send signed certificate revocation requests to the CA, which again are not validated by the CA Administrator. Not the request generated using grid-cert-request program is sent not to the CA but to the RA (division administrator for example). The administrator validates the request using direct contact with the requester and signs it with his Globus certificate. This signed request is then emailed to the CA. The CA checks the signature on the request, and later CA administrator issues the certificate without any other checks. Our implementation of the RA uses Globus certificates for signing certificate and revocation requests.

The email robot at CA understands not only certificate requests, but also special "revoke" requests that can be used by a RA for certificate revocation. Our CA also supports certificate renewal requests (generated with grid-cert-renew program). CA email robot can also perform several supplementary functions like checking certificate validity, obtaining old issued certificates with given Distinguished Name or serial number. In future the email robot will keep track on certificate expiration dates and will automatically send renew challenge strings for grid-cert-renew (challenge in renew requests is currently ignored).

Certificate Revocation Lists

Certificate Revocation Lists (CRLs) are the only way to check the validity of the certificate in Globus Security Infrastructure (GSI). This means that for the best security we must update CRLs on the hosts running Globus as fast as it is possible.

All current CRL update solutions are based on scheduled web update from the CA web sites. These solutions have several problems:

- CRL update frequency on the host often does not match the CRL generation frequency at the CA. This causes too frequent CRL updates or CRL expiration problems.
- In future frequent web updates of the CRLs can cause big load of the CA web servers.
- Signing policies for the CAs are not updated automatically.

We are now developing the new CRL update scheme, which uses notification messages for updating certificates on the Russian DataGrid hosts. When the CA issues a new CRL it sends a special notification to all sites, and after this software on the sites downloads the new CRL. This allows to relinquish the scheduled updates and to update CRLs only when it is really required.

Acknowledgments

The work was supported by CERN-INTAS grant 00-0440.

Conclusions

All grid information services created in Russia were successfully tested during EU-DataGrid WP6 Testbed0 and showed adequate level of services and performance. Russian EU-DataGrid segment is now prepared for the next step – Testbed1, which includes job submission tests using grid tools. Russian DataGrid Certification Authority started issuing certificates that are accepted in all EU-DataGrid member institutes. Solutions used in the Certification Authority showed good scalability and proper security level.

CMS Computing Activities in R
Plans

O.Kodolova[1], *E.T.*

1 - Skobeltsyn Institute of Nuclear Physics, M
Nuclear Research, Du

A number of Russian leading nuclear phy
manufactories and plants participate in the cc
Large Hadron Collider (LHC, CERN): ATLAS
Russian investments into the LHC project can

In order to provide a full-range participati
projects at the running phase of the accelerato
nize a computing support for these experiment

During last several years Russian institutes
on a creation of Russian Regional Centre for sto
LHC) has been created [1]. At this moment t
prototype of such a distributed center in Russi

During last two years several institutes pa
Theoretical and Experimental Physics (ITEP)
clear Physics (SINP MSU) in Moscow, the
(JINR, Dubna) and the Institute of High Ene
dev Phisics Institute (LPI, Troitsk) worked in
activities on a creation of a RCC-LHC prototyp
a proper software environment have been creat
gional Computing Center of Moscow State Uni
for a RCC-LHC prototype). As it can be seen
at the four Russian institutes with a disk spac
tape library with a capicity of 10 TB. Since Se
resources will be increased significantly: by mo
space.

Nowdays these clusters of a prototype of R(
for testing of a current CMS software and for a
on a generation of simulated physical data of
a common CMS data base at CERN. For exa
at RCC-LHC during CMS Monte-Carlo events
Fig. 2). It constituted a 19% of a total amount
at all CMS institutes.

As the Grid technologies will be used for
of RRC-LHC and an integration into the glo
we participate in the EU DataGrid project i
Application) Working Packages. By summer thi
on global tests of DataGrid technologies has be