УДК 004.75

САЛЬНІКОВ А.О.,
БОЙКО Ю.В.

ВИРІШЕННЯ ПРОБЛЕМ ІНТЕГРАЦІЇ ВІРТУАЛЬНИХ ОРГАНІЗАЦІЙ НА ПРОВАЙДЕРАХ РЕСУРСІВ В УКРАЇНСЬКОМУ НАЦІОНАЛЬНОМУ ГРІД-СЕГМЕНТІ

В роботі проведено аналіз існуючих проблем інтеграції віртуальних організацій (ВО) в українському національному грід-сегменті (УНГ) та показано ключові обмеження провайдерів ресурсів. Запропоновано методики вирішення проблем масштабованості, гнучкості та цілісності політик, відокремлення ВО. Виконано успішне впровадження методик на трьох кластерах УНГ.

Contemporary virtual organizations (VO) integration problems in Ukrainian National Grid (UNG) has been analyzed. Key limitations of UNG resource providers are shown. Techniques for solving the problems of scalability, policy flexibility and integrity as well as VO separation are proposed. Successful deployments of proposed methods are conducted on three UNG member clusters.

1. Вступ

Грід-обчислення це різновид розподілених обчислень, що орієнтовані на використання ресурсів світового масштабу, зазвичай із застосуванням високопродуктивних обчислювальних кластерів [1]. За останні роки грід набуває все більшого розповсюдження та розвитку як в світі в цілому (Європейська грід-інфраструктура – EGI [2]), так і в Україні зокрема (Український національний грід – УНГ [3]).

Побудова грід-інфраструктури, EGI чи УНГ, є лише фундаментом для вирішення ресурсоємних задач. Головною метою координованого доступу до ресурсів є вирішення реальних наукових завдань динамічними групами людей з різних установ, в так званих *віртуальних організаціях* (ВО). Дослідження кожної ВО напрямлені на вирішення певної наукової задачі.

Обмін обчислювальними потужностями чи простором зберігання даних, з боку провайдерів ресурсів має чітко визначати до яких сервісів надається доступ, кому і за яких умов. Множина користувачів та/або установ що визначається такими правилами і є віртуальною організацією [1].

Головна спільна риса, що характерна для всіх учасників віртуальної організації – вирішення одного класу проблем, а відповідно і використання одного класу обладнання та/або прикладного програмного забезпечення. Спільний клас задач диктує однакові вимоги до сервісів грід-інфраструктури що будуть використані, процесорного часу для виконання розрахунків, обсягів та критеріїв зберігання даних.

Такі вимоги можуть принципово відрізнятися для різних ВО, проте одна й та сама ВО чітко висуває вимоги до грід інфраструктури. Саме тому одиницею з якою працює провайдер ресурсів, як елемент загальної грід-інфраструктури, є віртуальна організація [4]. Цей підхід надає можливість гнучкого налаштування локального планувальника ресурсів обчислювального елементу для гарантії процесорного часу, чи конфігурації квот на елементі зберігання згідно домовленостей з тією чи іншою ВО. Відповідно, договір з провайдерами ресурсів відбувається на рівні ВО, а не окремих користувачів.

2. Проблеми інтеграції ВО на провайдерах ресурів в УНГ

Інфраструктура УНГ історично побудована децентралізованим чином без чіткої координації. Розвиваючись, нові обчислювальні кластери під'єднувались до УНГ встановлюючи базову поставку програмного забезпечення проміжного рівня Nordugrid ARC [5] доступну на час інсталяції.

Конфігурація грід на обчислювальних кластерах при таких інсталяціях обмежувалась лише базовими сервісами рівня ресурсів: обчислювальним елементом (CE) та локальною інформаційною системою грід-ресурсу (GRIS) [6]. Конфігурація обчислювального елементу також залишалася базовою, з використанням так званої *класичної авторизації*. Ключові властивості класичної авторизації це [7]:

- використання локальних облікових записів та файлів відповідності;
- механізми авторизації замикає на собі операційна система;

- грід-сервіси не проводять додаткових перевірок для розмежування прав доступу.

На більшості провайдерів УНГ застосовані тривіальні налаштування класичної авторизації – використання єдиного облікового запису для будь-якого учасника будь-якої ВО. Списки учасників ВО формуються атоматично завдяки використанню сервісу VOMS. Переважну більшість українських ВО обслуговує VOMS сервер КНУ [8], проте використання сервісу обмежено лише оновленням списків користувачів.

Використання такого підходу має ключові обмеження для інтеграції ВО:

- Масштабованість: кожна зміна політики доступу для учасника ВО потребує змін на кожному провайдері ресурсів;
- Гнучкість політик: вбудовані засоби контролю політик операційної системи можуть бути недостатньо гнучкими для підтримки внутрішньої структури ВО грід-сервісами;
- Цілісність: вбудовані засоби контролю політик операційної системи можуть відрізнятися на різних провайдерах ресурсів;
- Відокремлення ВО: прив'язка до ВО відбувається виключно за DN користувача, і не може коректно працювати в випадку участі одного користувача в декількох ВО.
- Безпека: завдання різних користувачів різних ВО мають змогу отримати доступ до файлів та процесів всіх грід-завдань через роботу від імені одного локального облікового запису.

В результаті таких обмежень конфігурації провайдерів ресурсів в УНГ, не відбувається розділення роботи різних ВО, не кажучи вже про підтримку внутрішньої структури ВО. Відповідно залишаються неврахованими особливості вимог прикладного програмного забезпечення кожної ВО, якій надаються ресурси. Це призводить до *відсутності ефективного планування завдань, що веде до простою національних обчислювальних ресурсів.*

Більш того серед близько 30-ти учасників УНГ лише одиниці слідкують за оновленнями програмного забезпечення проміжного рівня грід та проводять роботи з розгортання чи забезпечення підтримки нових сервісів. Таким чином сьогодні стоїть *проблема неінтероперабельної роботи* інфраструктури: помилки в роботі та несумісність різних версій програмного забезпечення, практично повна відсутність підтримки роботи з сервісам рівня кооперації грід.

Через збільшення активності використання інфраструктури такими ВО як moldyngrid, networkdynamics та medgrid, насьогодні проблема інтероперабольності гостро стоїть перед УНГ. Роботи з вирішення проблем координованої роботи інфраструктури закладено в державну цільову науково-технічну програму впровадження і застосування грід-технологій на 2009–2013 роки. В рамках програми створено координаційний комітету, який проводить роботи по встановленню регламенту роботи як провайдерів ресурсів так і віртуальних організацій в Україні.

Проте навіть за інтероперабельної роботи, для вирішення проблем масштабованості, гнучкості, цілісності та відокремлення роботи ВО на провайдерах ресурсів необхідні методики, що дозволять систематизувати підхід до інтеграції ВО. Розробка та впровадження таких методик є завданням даної роботи.

3. Засвідчення участі в ВО

Класична авторизація не враховує фактор участі користувача в ВО. Ідентифікація користувача вказує тільки на його унікальне ім'я (DN) за яким неможливо однозначно визначити приналежність до ВО [7]. В той час ефективне розділення ресурсів (резервацій чи приорітезації обчислювальних потужностей, квот елементів зберігання) потребує механізмів визначення такої інформації.

Методом, що дозволяє провести ідентифікацію приналежності до ВО є засвідчення за допомогою сервера VOMS [9]. На сьогодні роботу з VOMS підтримують всі проекти по розробці програмного забезпечення проміжного рівня грід. Служба VOMS є невід'ємною складовою EMI та IGE.

Методика засвідчення участі в ВО будується на розширенні проксі-серти-фікатів делегації користувача. Учасник ВО, за допомогою утиліти для створення делегації, звертається до серверу VOMS з запитом щодо засвідчення параметрів участі в ВО. VOMS сервер створює сертифікат атрибутів (Attribute Certificate – AC) [10], який містить перелік прав доступу учасника відповідно до інформації в базі даних. Такий AC засвідчується цифровим підписом серверу VOMS та передається клієнту користувача, що

додає АС як розширення до базової делегації [9]. Грід-сервіси, що підтримують таке розширення зможуть працювати з параметрами доступу ВО, в той час як інші реалізації будуть ігнорувати таке розширення і працювати спираючись на класичну авторизацію.

Параметри участі в ВО відображено в повному імені атрибутів користувача (Fully Qualified Attribute Name, FQAN). В АС міститься перелік FQAN всіх атрибутів, засвідчення яких вимагалось в запиті користувача. FQAN має наступний формат:

```
/VO[/group[/subgroup(s)]][/Role=role][
/Capability=cap]
```

4. Методики інтеграції ВО на провайдерах ресурсів

Метод засвідчення участі в ВО за допомогою сертифікату атрибутів дозволяє грід-сервісам на провайдері ресурсів отримати інформацію як про участь ВО, так і особливості участі відповідно до внутрішної структури.

Права доступу учасника відображені виключно в FQAN, та можуть змінюватись адміністратором ВО через інтерфейс керування VOMS [8]. Сервіси що не потребують запуску окремих процесів від імені користувача (наприклад елемент зберігання чи каталог файлів) для забезпечення виконання політики доступу використовують FQAN безпосередньо. Якщо необхідно виконати запуск процесів (наприклад обчислювальний елемент чи інтерактивний вхід) необхідне надання відповідності користувача ВО локальному обліковому запису ОС від імені якого буде запущено цільовий процес.

Програмне забезпечення проміжного рівня Nodrugrid ARC, що використовується в УНГ, не містить штатних засобів надання локальних облікових записів в залежності від FQAN учасника в ВО [5].

З поставкою програмного забезпечення gLite проекту EGI використовується інфраструктура Site Access Control (SAC) [11].

Використання бібліотек SAC для Nodrugrid ARC дозволить визначити єдині політики доступу у випадку одночасної роботи сервісів різного програмного забезпечення проміжного рівня (в тому числі авторизації на елементах зберігання, тощо).

Розглянемо методики інтеграції ВО на провайдерах ресурсів з використанням інфраструктури SAC в застосуванні до Nodrugrid ARC.

4.1. Відокремлення ВО. Виходячи з проведеного вище аналізу випливає, що для розділення доступу різних ВО, відповідні їм облікові записи мають бути різними. Більш того, для підвищення ефективності роботи провайдера ресурсів є необхідність розділяти роботу різних учасників однієї ВО для:

- відокремлення роботи (виконання задачі одного учасника не може випадково чи навмисно завадити виконанню завдання іншого);
- надання різних прав доступу в залежності від FQAN учасника;
- забезпечення “справедливого” (fair share) розділення ресурсів (сервіси операційної системи не пов’язані з роботою грід повинні розрізняти завдання різних учасників, щоб уникнути монопольного використання ресурсів).

Відокремлення ВО є особливо важливим для роботи віртуальних організацій, які орієнтовані на обробку захищених приватних даних. За статичного підходу до відповідності користувачів, що використовується в Nodrugrid ARC, при реалізації відокремлення виникає проблема масштабування: учасники додаються та видаляються із віртуальних організацій незалежно від провайдерів ресурсів, що ускладнює процес керування відповідністю до системних облікових записів.

Для вирішення проблеми масштабування необхідно використовувати динамічно розподілені ресурси облікових записів – *пули користувачів* (від англ. pool – сукупність об’єктів). Локальний обліковий запис ставиться у відповідність до ідентифікації користувача динамічно, за допомогою механізму оренди [12]. Для ідентифікації використовується DN учасника разом з VOMS FQAN. Таким чином при засвідченні участі в ВО, користувачеві ставиться у відповідність обліковий запис із пулу, що відповідає даній ВО. Для однієї ВО можуть існувати декілька пулів, а відповідність обліковим записам відбувається в залежності від групи, ролі чи атрибутів учасника. Розміри пулів визначаються кількістю та функціями ресурсів провайдера та локальними політиками використання ресурсів.

Забезпечуючи розподіл за обліковими записами на рівні операційної системи, пули не обмежують архітектуру грід-сервісів, які в свою чергу можуть додатково визначати права доступу безпосередньо використовуючи VOMS AC делегації.

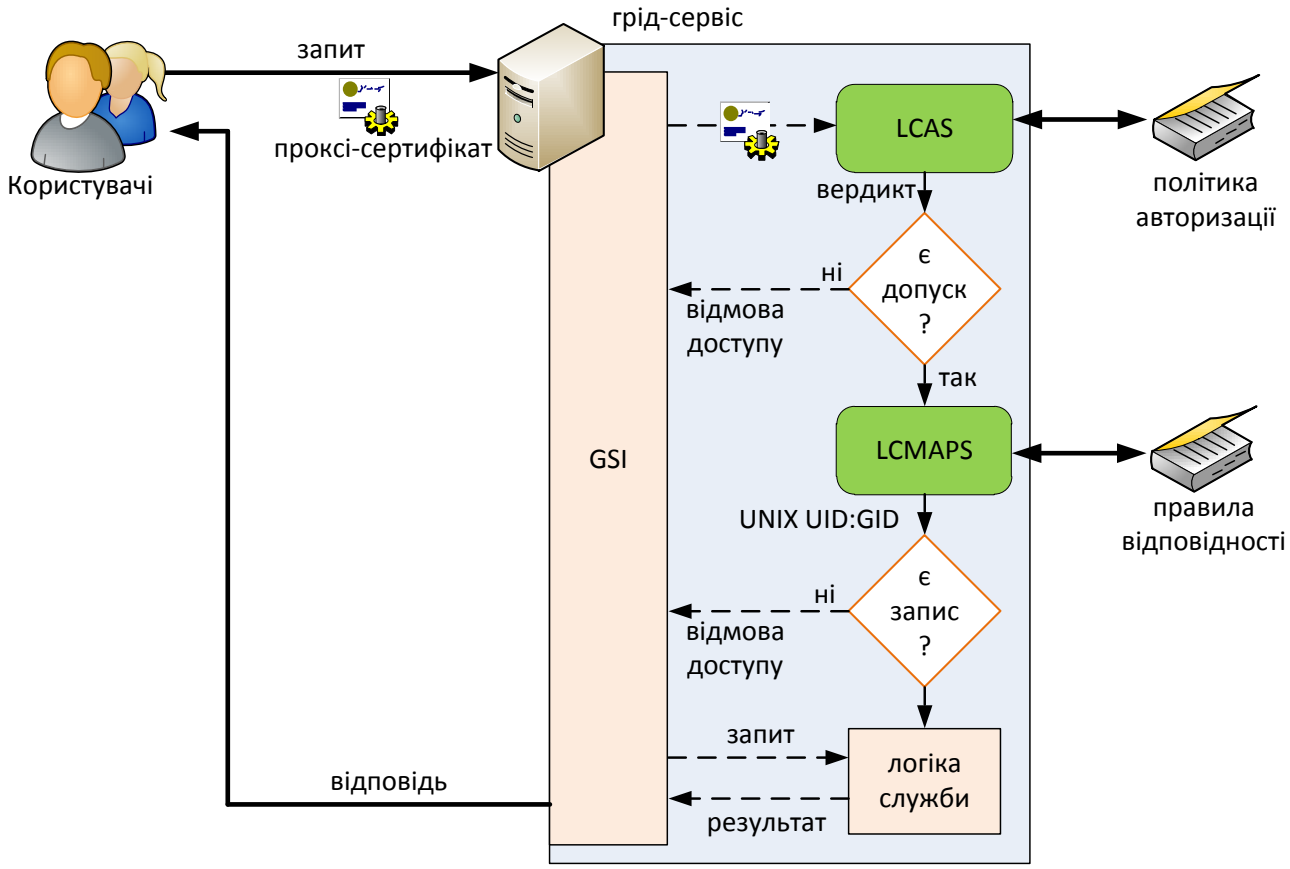

Рис. 1.Схема алгоритму взаємодії GSI з бібліотеками LCAS/LCMAPS

4.2. Цілісність та гнучкість політик за допомогою SAC. Site Access Control – це інфраструктура бібліотек та сервісів локальної авторизації, що надає механізми реалізації політик доступу до грід-ресурсу та забезпечує відповідність грід-користувачів локальним обліковим записам [**Ошибка! Источник ссылки не найден.**].

Бібліотеки LCAS та LCMAPS інфраструктури SAC представлені набором незалежних підключених програм.

Local Centre Authorization Service (LCAS) – бібліотека для реалізації механізмів контролю доступу на сервісах грід. Вона являє собою набір методик прийняття рішення про успішну авторизацію чи заборону доступу.

Local Credential MAPping Service (LCMAPS) – бібліотека для реалізації механізмів присвоєння локальних повноважень (таких як UID облікового запису) для грід-завдань, що виконуються на локальних фабрикатах.

На рисунку 1 зображено схему алгоритму взаємодії GSI з бібліотеками LCAS/LCMAPS. Використання інструментарію LCAS для забезпечення політики авторизації разом з LCMAPS для створення правил відповідності забезпечує локальну авторизацію грід-сервісів та дозволяє ефективно працювати з сертифікатами атрибутів VOMS завдяки відповідним підключеним програмам SAC.

Всі підключені програми LCMAPS розділяють на два типи: *модулі присвоєння (acquisition)* та *модулі забезпечення виконання (enforcement)*. Модулі присвоєння призначені для збору інформації щодо надання повноважень для кожного запиту, які присвоюються модулями забезпечення виконання [12].

Для Nodrugrid ARC було створено зовнішні застосування що викликають LCAS та LCMAPS. Відповідно до алгоритму роботи (рис. 1) LCAS приймає бінарне рішення щодо надання чи відхилення доступу. Зовнішньому застосуванню передається DN користувача та шлях до файлу з проксі-сертифікатом. LCAS перевіряє цифровий підпис серверу VOMS та використовує перевірку доступу відповідно до конфігурації. Код повернення використовується для прийняття рішення.

Приклад конфігурації LCAS для реалізації контролю доступу за VOMS AC наведено на рис. 2.

```
pluginname=lcas_voms.mod,\
pluginargs="-vomsdir /etc/grid-security/vomsdir/ \
     -certdir /etc/grid-security/certificates/ \
     -authfile /etc/grid-security/voms-user-mapfile
```

Рис.2. Лістинг конфігураційного файлу LCAS для роботи з VOMS AC

```
"/moldyngrid/modelling/Role=production" .mdgmodprod
"/moldyngrid/Role=VO-Admin" .mdgadm
"/testbed.univ.kiev.ua" .tb
```

Рис.3. Фрагмент лістингу файлу voms-user-mapfile

Директорія `vomsdir` містить публічні сертифікати серверів VOMS які обслуговують ВО, що підтримуються; `certificates` містить сертифікати довірених кореневих центрів сертифікації грід. Файл `voms-user-mapfile` містить список FQAN, які допущені до використання ресурсу (рис. 3).

В наведеній конфігурації будуть допущені всі засвідчені учасники ВО testbed.univ.kiev.ua та учасники групи modelling з роллю production чи роллю VO-Admin ВО moldyngrid. Другий параметр не використовується LCAS, проте необхідний для використання цього ж файлу бібліотекою LCMAPS.

Винесення рішення щодо авторизації на ресурсі в LCAS дозволяє змінювати політику доступу без переконфігурації самого сервісу.

Nodrugrid ARC виконує присвоєння локальних повноважень (операції setuid та setgid) за допомогою вбудованих засобів, проте для присвоєння використовуються лише механізми класичної авторизації [5]. Виклик LCMAPS з окремої підключеної програми не може виконати зміну повноважень в батьківському процесі. Тому для роботи з Nodrugrid ARC необхідно забезпечити передачу визначених повноважень від LCMAPS.

Аналогічно до виклику LCAS, виконуваній програмі передається DN користувача та шлях до файлу з проксі-сертифікатом. Програма виконує виклик LCMAPS, конфігурація якого не повинна використовувати модулі забезпечення виконання. Отримані значення локальних повноважень передаються до Nodrugrid ARC який і виконує необхідне присвоєння.

Приклад конфігурації LCMAPS для Nordugrid ARC наведено на рис. 4.

Конфігураційний файл визначає наступні операції:

- good – викликає модуль забезпечення виконання, що нічого не робить;
- vomsextract – викликати базовий модуль роботи з VOMS, що обробляє VOMS AC розширення делегації користувача з використанням VOMS API та зберігає ідентифікацію VOMS в структурах даних LCMAPS для роботи інших підключених програм;
- vomspoolaccount – викликати модуль, який повертає значення UID локального облікового запису з заданого пулу користувачів відповідно до участі в ВО;
- vomslocalgroup – аналогічно до vomspoolaccount, але повернути значення GID;

Відповідно до визначених операцій формується політика присвоєння локальних повноважень:

- виклик vomsextract: якщо знайдено валідне AC розширення викликається модуль vomspoolaccount (визначення UID), інакше робота завершується без забезпечення виконання (good);
- Якщо визначення UID виконано успішно (vomspoolaccount) визначається GID, в протилежному випадку робота LCMAPS завершується (good).
- Після визначення GID (vomslocalgroup) робота LCMAPS завершується (good).

Файли та директорії вказані в конфігурації-містять інформацію щодо прив'язки FQAN до пулу користувачів. Ім'я локального аккаунту з пулу містить номер (наприклад, для ВО moldyngrid імена аккаунтів представлені множиною: `mdg01, mdg02,…, mdg50`). Ім'я складається з базового імені до якого додається порядковий номер. В конфігурації для посилання на пул використовується нотація крапки – зазначається лише базове ім'я, якому передує символ «крапка» (наприклад для посилання на пул для ВО moldyngrid використовується `.mdg`).

```
good = "lcmaps_dummy_good.mod"

vomsextract = "lcmaps_voms.mod"
" -vomsdir /etc/grid-security/vomsdir"
" -certdir /etc/grid-security/certificates"

vomspoolaccount = "lcmaps_voms_poolaccount.mod"
" -override_inconsistency"
" -max_mappings_per_credential 1"
" -do_not_use_secondary_gids"
" -gridmapfile /etc/grid-security/voms-user-mapfile"
" -gridmapdir /etc/grid-security/gridmapdir"

vomslocalgroup = "lcmaps_voms_localgroup.mod"
" -groupmapfile /etc/grid-security/voms-group-mapfile"
" -mapmin 1"

voms:
vomsextract -> vomspoolaccount | good
vomspoolaccount -> vomslocalgroup | good
vomslocalgroup -> good
```

Рис.4. Приклад файлу конфігурації LCMAPS для роботи з Nordugrid ARC

5. Впровадження методик

Описані вище методики були застосовані до обчислювальних кластерів Київського національного університету імені Тараса Шевченка (КНУ), Інституту молекулярної біології і генетики (ІМБіГ) НАН України та Національного наукового центру з медико-біотехнічних проблем (ННЦМБП) при президії НАН України.

Апаратна та програмна архітектура обчислювальних кластерів істотно відрізняється, проте використання описаних методик інтеграції ВО є універсальним механізмом, що дозволяє проводити подальше регулювання ефективного планування відповідно до особливостей програмної архітектури та домовленостей про резервації з кожною ВО. Разом з тим вирішуються зазначені проблеми класичної авторизації.

На кожному провайдері ресурсів, налаштовано роботу Nordugrid ARC з зовнішніми програмами виклику LCAS та LCMAPS. Впроваджено конфігурацію бібліотек яка використовує інформацію з VOMS AC.

На обчислювальному кластері КНУ також функціонують сервіси програмного забезпечення gLite, що використовуються для роботи в інфраструктурі EGI. Ці сервіси також використовують LCAS та LCMAPS, що забезпечує інтероперабельну роботу для ВО незалежно від точки входу.

В створеній конфігурації, для обслуговування нової ВО провайдером необхідно:

- створити новий пул користувачів (або декілька пулів за необхідності підтримки складної внутрішньої структури ВО);
- додати до списків допущених FQAN нові записи відповідно до інформації наданої ВО;
- додати інформацію про сертифікат серверу VOMS, що обслуговує ВО.

Разом з методиками авторизації, запропонований підхід забезпечив індикацію класу виконуваних задач за ідентифікатором групи (GID) пулу користувачів. Це дозволило налаштувати резервації та використовувати прогнозування часу обрахунку локального планувальника, зменшуючи час простою обчислювальних ресурсів зазначених кластерів.

6. Висновки

Було проаналізовано існуючі проблеми інтеграції ВО на провайдерах ресурсів УНГ під керуванням Nordugrid ARC, та сформовано ключові обмеження існуючого підходу: відсутність масштабованості, гнучкості та цілісності політик доступу, разом з проблемами відокремлення роботи різних ВО.

Ефективне планування локальних ресурсів можливе лише за наявності детермінованих вимог до процесорного часу, обсягів та критеріїв зберігання даних, які диктує прикладне програмне забезпечення, що використовується. Тому необхідним є розділення доступу для різного класу задач, а відповідно і для різних віртуальних організацій.

Проблему масштабованості конфігурації вирішено шляхом використання серверу VOMS для динамічного керування FQAN учасників ВО.

Проблему відокремлення роботи різних ВО вирішено за допомогою використання пулів локальних облікових записів, прив'язка до яких відбувається у відповідності до FQAN учасника, який засвідчено сервером VOMS за допомогою використання сертифікату атрибутів.

Цілісність та гнучкість політик досягнуто винесенням рішень авторизації та відповідності локальним обліковим засобам в інфраструктуру SAC, а саме використання бібліотек LCAS та LCMAPS. Взаємодія з сервісами Nordugrid ARC відбувається за рахунок конфігурації без забезпечення виконання.

Методики дозволяють додавати нові ВО чи проводити модифікацію конфігурації та політики доступу без переривання роботи та зміни конфігурації самих грід-сервісів.

Методики були застосовані до обчислювальних кластерів Київського національного університету імені Тараса Шевченка, Інституту молекулярної біології і генетики (ІМБіГ) НАН України та Національного наукового центру з медико-біотехнічних проблем (ННЦМБП) при президії НАН України та дозволили гнучко налаштувати локальне планування ресурсів та підтримку віртуальних організацій УНГ.

Перелік посилань

1. Foster, Ian. The Anatomy of the Grid - Enabling Scalable Virtual Organizations / Ian Foster, Carl Kesselman, Steven Tuecke // International Journal of Supercomputer Applications. – 2001. –Vol. 15. –P. 2001.
2. Infrastructure, European Grid. Towards to sustainable grid infrastructure [online] –http://www.egi.eu/. –2011.
3. Український академічний Грід: досвід створення й перші результати експлуатації / Ю.В.Бойко, М.Г.Зинов'єв, О.О.Судаков, С.Я.Свістунов // Математичні машині і системи. –2008. –Vol. 1. –Pp. 67-84.
4. Foster, Ian. The physiology of the grid: An open grid services architecture for distributed systems integration / Ian Foster. – 2002.
5. Ellert, M. Advanced Resource Connector middleware for lightweight computational Grids / M. Ellert et al. // Future Gener. Comput. Syst. –2007. –Vol. 23, no. 1. –Pp. 219–240.
6. Ukrainian Grid Infrastructure: Practical Experience / Mykhaylo Zynovyev, Sergiy Svistunov, Oleksandr Sudakov, Yuriy Boyko // Proceedings of the 4-th IEEE Workshop IDAACS 2007. – 2007. – September. – Pp. 165-169. – 6-8 September 2007, Dortmund, Germany.
7. The Globus Security Team. Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective [online]. – http://www-unix.globus.org/toolkit/docs/5.0/5.0.0/security/GT4-GSI-Overview.pdf. – 2005. – September. – Version 4.
8. PHP VOMS-Admin project development [online]. – http://grid.org.ua/development/pva/. – 2011.
9. Alfieri R. An Authorization System for Virtual Organizations / R. Alfieri, R. Cecchini, V. Ciaschini et al. // In Proceedings of the 1st European Across Grids Conference, Santiago de Compostela. –2003. –Pp. 13–14.
10. Farrell, S. An Internet Attribute Certificate Profile for Authorization. – RFC 5755 (Proposed Standard). [online] – 2010. – January. http://www.ietf.org/rfc/rfc5755.txt.
11. Site Access Control [online]. – http://www.nikhef.nl/pub/projects/grid/gridwiki/ – 2011.
12. Local Credential MAPping Service [online]. – http://www.nikhef.nl/grid/lcaslcmaps/lcmaps-apidoc/html/ – 2005.