УДК 004.415.2:004.75

КОМПЛЕКСНА СИСТЕМА ТЕСТУВАННЯ ВЗАЄМОДІЇ РЕСУРСІВ У НАЦІОНАЛЬНІЙ ГРІД-ІНФРАСТРУКТУРІ

Є.А. Слюсар

Київський національний університет імені Тараса Шевченка
01601, м. Київ, вул. Володимирська, 64,
тел.: (44) 259 0247; факс (44) 526 1214; e-mail: slu@grid.org.ua

Розглянуто існуючі підходи до тестування та моніторингу грід-ресурсів у глобальних грід-інфраструктурах та запропоновано власну архітектуру автоматизованої системи тестування грід-ресурсів, що включає в себе локальні, зовнішні та колективні тести. Реалізовано прототип такої системи для тестування ресурсів української національної грід-інфраструктури.

Analysis of monitoring tools of global-scale grid infrastructures is conducted. Architecture of automated testing system is introduced, providing local, external and collective grid-resource testing techniques. A prototype implementing the proposed architecture was developed and applied to Ukrainian national grid-infrastructure.

Вступ

Грід – це географічно розподілена інфраструктура, що надає можливість побудувати на основі поєднаних через Інтернет суперкомп'ютерів та обчислювальних кластерів єдине інтегроване середовище для високопродуктивних обчислень, шляхом об'єднання та розподілу спільного доступу до ресурсів різних типів – процесорів, довготривалої і оперативної пам'яті, сховищ і баз даних, доступ до яких користувач може отримати з будь-якої точки незалежно від місця свого розташування. Грід-технології та так звані хмарні обчислення мають багато спільного, та є відображенням єдиної ідеї – динамічне виділення ресурсів для задач користувачів на вимогу чи автоматично по мірі необхідності. Грід-технології виникли раніше та більш орієнтовані на вирішення наукових задач, що потребують великих обчислювальних ресурсів, тоді як хмарні обчислення орієнтовані на швидке обслуговування клієнтів застосування користувача та масштабування ресурсів у процесі його роботи. Спільна риса полягає у тому, що користувач працює із єдиним загальним інтерфейсом, що приховує внутрішні деталі інфраструктури, такі як фізичне розміщення серверів чи їх системне програмне забезпечення. Так, грід-інфраструктура визначає без втручання користувача найбільш оптимальне джерело даних та знаходить якнайкраще, за певним набором критеріїв, місце для запуску відповідної програми на вузлах, що простоюють [1].

Для реалізації такої інфраструктури у грід-технологіях використовують специфічну програмну архітектуру. Вона забезпечує необхідний проміжний рівень абстракції між користувачами і службами грід-середовища та різноманітними програмними та апаратними компонентами, на основі яких будуються грід-ресурси. Таке програмне забезпечення отримало назву *middleware*, аналогічно до того, як цей термін застосовується, наприклад, у технологіях Java 2 Enterprise Edition. У світі активно розробляються такі пакети програмного забезпечення проміжного рівня для побудови грід-інфраструктур як Nordugrid Advanced Resource Connector (ARC), gLite, UNICORE та Globus Toolkit. Інтероперабельність різних пакетів забезпечується завдяки використанню загальних стандартів протоколів взаємодії між компонентами, які розробляються організацією Open Grid Forum.

Грід-інфраструктура – це динамічне середовище, до якого можуть додаватися та вилучатися як ресурси так і користувачі. Для того, щоб вчасно виявляти підключення нових ресурсів та вилучення існуючих, а також вести облік наявних зайнятих та вільних ресурсів, у межах грід-інфраструктури має функціонувати *інформаційна система*. Вона являє собою набір програмних служб та протоколів обміну даними, що слугують для публікації, оновлення, пошуку та обліку мета-даних, які описують усі ресурси наявні в інфраструктурі.

Інфраструктура зберігання даних у грід-середовищі забезпечує прозорий доступ до розподілених сховищ даних. Серед основних компонентів визначають каталоги даних, власне елементи зберігання даних та служби реплікації даних. Каталоги даних ставлять у відповідність кожному імені файлу в своїй ієрархічній структурі одне або декілька посилань на елементи зберігання, що містять відповідні дані – репліки файлу. Для підвищення надійності та швидкості доступу, служби реплікації слідкують за кількістю доступних реплік та створюють нові у разі необхідності.

Пакетне виконання обчислювальних завдань в грід-інфраструктурі реалізується за допомогою служб обчислювального елемента. Ця служба встановлюється на вхідному вузлі кластера та забезпечує постановку завдань із грід-інфраструктури у локальну чергу, а також подальший моніторинг стану цього завдання із відображенням стану у інформаційній системі. Для вибору обчислювального елемента із необхідними характеристиками використовується служба посередника ресурсів, що постійно завантажує дані із інформаційної системи та використовує їх для визначення найбільш оптимального за параметрами і поточним станом кластера та найближчих до нього реплік вхідних даних для кожного окремого завдання [2].

Грід-інфраструктура являє собою складну багатоагентну систему взаємодії, географічні масштаби якої

можуть охоплювати цілі континенти та навіть всю Земну кулю, кількість ресурсних центрів може складати сотні, а кількість окремих служб – тисячі одиниць [3]. Прикладами таких грід-систем є European Grid Infrastructure (EGI) та Worldwide LHC Computing Grid (WLCG). Також слід зазначити, що грід-система є децентралізованою за своєю суттю, тому всі наявні ресурси перебувають в адміністративному підпорядкуванні різних суб'єктів, що запроваджують свої власні політики використання цих ресурсів. Суб'єктами цих політик виступають не індивідуальні користувачі, а *віртуальні організації* – динамічні об'єднання людей із різних установ та навіть країн, створені для вирішення певних наукових, технічних та інших задач. Кожна віртуальна організація самостійно погоджує доступ до певних ресурсів безпосередньо із їх власниками [4]. Так, для інфраструктури WLCG визначені віртуальні організації, кожна з яких відповідає окремому експерименту на Великому адронному колайдері.

Проблеми існуючих підходів до моніторингу грід-інфраструктур

Задля вчасного виявлення проблем у функціонуванні грід-ресурсів у великих інфраструктурах застосовується трирівнева система організації ресурсів. Найнижчою ланкою виступають окремі *грід-сайти* – набір інтернет-вузлів та грід-служб на них, що перебувають під єдиним керуванням та обслуговуються певною установою. Зазвичай, грід-сайти мають у своєму складі хоча б один обчислювальний елемент та елемент зберігання даних. Наступним рівнем є регіональні *операційні центри*, що представляють сайти грід-інфраструктури на національному рівні. В складі таких центрів зазвичай працюють центральні каталоги ресурсів та даних, а також системи тестування та моніторингу. Так, в Україні на базі Інституту теоретичної фізики ім. М.М. Боголюбова НАН України створено Базовий координаційний центр, на який покладено функції операційного центру для Українського національного гріду. На найвищому рівні знаходиться глобальний операційний центр, що обслуговує центральні бази даних грід-сайтів та каталоги даних, а також служби обліку використання ресурсів. Інформація із регіональних систем моніторингу імпортується до центральної системи, де потім обчислюються показники доступності та надійності окремих вузлів та служб.

Моніторинг стану грід-ресурсів здійснюється шляхом виклику регулярних тестів, за допомогою яких перевіряється коректність роботи служб цих грід-ресурсів. Самі тести являють собою сценарії, що для виконання своїх задач спираються на утиліти командного рядка компонентів інтерфейсу користувача, які входять до програмного забезпечення проміжного рівня. Інфраструктура моніторингу може бути як централізованою, так і частково децентралізованою. Розглянемо підходи до організації моніторингу, що були використані у глобальних грід-інфраструктурах.

Так, у грід-інфраструктурах Enabling Grids for E-sciencE (EGEE) та LCG застосовувалась централізована система Site Functional Tests (SFT), що отримувала список грід-сайтів та їх ресурсів із статичної центральної бази даних топології грід-інфраструктури – Grid Operations Centre (GOCDB) [5]. Тести запускались із окремо виділених вузлів, розміщених у лабораторії CERN, а результати відображались на відповідному веб-порталі. Система дозволяла тестувати лише обчислювальні елементи та сховища, побудовані за допомогою програмного забезпечення gLite. В подальшому розвитку система еволюціонувала та отримала нову назву – Site Availability Monitoring (SAM). Нова система містила більше сценаріїв-сенсорів та дозволяла тестувати каталоги даних, центральні каталоги ресурсів інформаційної системи, а також посередники ресурсів. Але обидві системи мали ряд суттєвих недоліків:

- адміністратори сайтів не мали можливість вручну запланувати виконання тестів, що пришвидчило б процес відлагодження конфігурації грід-ресурсів;
- для визначення точок входу та інших необхідних для тестів параметрів грід-ресурсів система спиралась лише на статичну інформацію із центральної бази даних топології, зміни до якої мали вноситись адміністраторами грід-сайтів вручну; динамічні мета-дані, що публікувались у інформаційній системі, до розгляду не брались;
- надмірна централізація системи – проблеми зв'язку між лабораторією CERN та серверами грід-сайтів могли призводити до провалювання тестів, а вихід з ладу самих серверів тестування міг призвести до відмови системи моніторингу усієї грід-інфраструктури.

В процесі еволюції інфраструктури EGEE у EGI було впроваджено нову систему моніторингу на основі програмного забезпечення Nagios та механізмів обміну повідомленнями ActiveMQ між вузлами системи. Пакет Nagios – це де-факто стандартне відкрите рішення для моніторингу будь-яких інформаційних систем, що має готовий інструментарій для керування запуском тестів та розмежування привілеїв користувачів. Адміністратори грід-сайтів отримали можливість самостійно запланувати разові запуски тестів для служб на своїх сайтах. До складу системи, окрім сценаріїв-сенсорів, входить агрегований постачальник топології – Aggregated Topology Provider (ATP), що формує список вузлів і служб для тестування та групує їх за приналежністю до грід-сайтів, спираючись на відомості не тільки із глобальної бази даних топології, а й із динамічних джерел, таких як каталоги ресурсів інформаційної системи та портал статистики [6]. Завдяки механізму обміну повідомленнями, інфраструктура моніторингу тепер є розподіленою та більш відмовостійкою, оскільки вузли моніторингу можуть дублюватися на усіх рівнях. На найвищому рівні запущено декілька так званих супер-Nagios серверів, що географічно рознесені та використовуються для моніторингу самої інфраструктури тестування, а саме – виконують тести серверів регіонального рівня. На регіональному рівні, зазвичай в масштабах країни, також може бути запущено декілька відповідно настроєних сервери моніторингу, що перевіряють стан грід-сайтів свого регіону та надсилають повідомлення про зміну стану служб до регіонального та центрального

операційних порталів. Адміністратори грід-сайтів мають можливість інсталювати власні вузли моніторнгу, що перевіряють лише їх власний грід-сайт, проте це потребує виділення окремого сервера. Основний недолік полягає в тому, що тести, незалежно від того з якого сервера вони були запущені, є зовнішніми та перевіряють лише вхідні інтерфейси грід-служб. Адміністратори не мають можливості перевірити автоматизованими засобами коректність конфігурації своїх грід-ресурсів, а також зв'язок грід служб із низькорівневими компонентами. Другий суттєваий недолік полягає в тому, що у такій системі перевіряється лише взаємодія вузла системи тестування та відповідних служб грід-ресурсів, що перевіряються. Лише в окремих випадках у процесі тестування використовуються декілька обраних сторонніх грід-ресурсів та постулюється, що вони вже перевірені та функціонують нормально. Ці сторонні ресурси обслуговуються командою системи моніторингу на загальному рівні та включають центральний каталог файлів, тестовий елемент зберігання даних та посередник ресурсів. Така архітектура системи тестування не дозволяє перевірити взаємодію грід-ресурсів регіону між собою, що є досить типовим сценарієм використання грід-інфраструктури в цілому [7].

В українській національній грід-інфраструктурі, на відміну від інфраструктур EGI та WLCG, відсутні жорсткі вимоги до операційного середовища грід-ресурсів. Це ускладнює розробку та впровадження системи автоматизованого тестування, оскільки тести мають коректно відпрацьовувати на різних версіях програмного забезпечення проміжного рівня, операційної системи, тощо. Український грід-сегмент первинно був побудований на основі програмного забезпечення ARC [8], тоді як у європейських грід-інфраструктурах здебільшого використовується gLite. Це обумовило більше покриття тестами системи EGI SAM Nagios саме грід-сервісів, побудованих із використанням gLite, порівняно із грід-сервісами на основі ARC. Тому набір тестів для пакету ARC потребував розширення та додаткової стандартизації, зокрема введення спеціальних середовищ виконання, які дозволяли б перевіряти певні аспекти роботи обчислювального елемента [9].

Критерії та етапи тестування

Проаналізувавши переваги та недоліки існуючих систем тестування та моніторингу грід-інфраструктур, та врахувавши специфіку українського грід-сегменту, можемо сформулювати загальні критерії тестування грід-ресурсів, що дозволили б найбільш повно діагностувати взаємодію компонентів програмного забезпечення Nordugrid ARC, як в межах одного обчислювального кластера чи грід-сайта, так і між різними грід-сайтами. Критерії можна згрупувати у три етапи тестування:

- локальне тестування окремих грід-ресурсів;
- зовнішнє тестування окремих грід-ресурсів;
- колективне тестування взаємодії грід-ресурсів в межах національної грід-інфраструктури.

На кожному етапі запускається певний набір тестів, що послідовно перевіряють критерії функціонування відповідного сервісу. Перехід до наступного етапу здійснюється лише після того, як всі тести попереднього етапу успішно пройдено. Грід-ресурс вважається працездатним, коли він успішно виконує всі тести всіх етапів.

Локальне тестування. Локальні тести виконуються безпосередньо на вузлі, де встановлено серверна частина ARC. Тести даного етапу були розроблені для того, щоб адміністратори грід-вузлів отримали можливість самостійно їх викликати та вносити зміни до конфігурації пакету перед тим, як відкрити грід-сайт для зовнішніх тестів. Деякі тести потребують доступу до утиліт локальної системи керування ресурсами та аналізують системні файли конфігурації, а отже принципово не можуть бути запущені зовнішнім чином через грід-інтерфейси.

Тести локальної конфігурації. Серія тестів складається із трьох тестів і спрямована на перевірку основного файлу конфігурації пакету ARC та його середовища виконання.

Перевіряється коректність синтаксису – структура файлу, допустимі блоки та директиви, їх параметри. Цей тест дозволяє діагностувати механічні помилки при створенні та редагуванні цього файлу адміністратором грід-вузла. З огляду на те, що універсальні шаблону такого файлу надто загальні та не дозволяють автоматизувати його створення, більшість директив вноситься адміністратором вручну.

Далі виконується семантична перевірка файлу конфігурації. Перевіряється наявність блоків опису черг виконання локальної системи керування ресурсами та ресурсів зберігання даних, а також наявність відповідних блоків реєстрації описаних ресурсів у центральних каталогах ресурсів національної грід-інфраструктури. Додатково перевіряється наявність блоків налаштування доступу для користувачів віртуальних організацій. У кожному блоку перевіряється адреси VOMS-серверів для отримання списків користувачів відповідної ВО.

Останній тест із даної серії виконує перевірку існування та повноваження доступу до усіх файлів та каталогів, вказаних у файлі конфігурації, а також деяких стандартних каталогів, що не налаштовуються або приймаються за замовчуванням. Перевіряється наявність усіх необхідних виконуваних модулів та бібліотек власне як для пакету ARC, так і його залежностей. Також перевіряється наявність сценаріїв запуску служб пакету ARC, а також їх реєстрація для автоматичного запуску при старті системи.

Тести локального планувальника. Оцінюється коректність роботи локальної системи керування ресурсами обчислювального кластера, а саме можливості запуску та контролю виконання грід-завдань.

Тип локальної системи керування визначається із файлу конфігурації служб грід-ресурсу, проаналізованого на попередньому кроці. Перевіряється наявність вказаних у ньому черг для завдань, а також наявність стандартних утиліт керування завданнями для вказаної системи (наприклад, qsub для системи PBS) та можливість виклику цих утиліт із контексту облікових записів користувачів, призначених для виконання грід-

завдань. Проблеми такого класу неможливо діагностувати за допомогою зовнішніх тестів,а вирішення їх зазвичай вимагає внесення змін до конфігурації локальних служб обчислювального кластера і може бути здійснене лише локальним адміністратором.

У ході наступного тесту на кластер направляється тестове завдання та перевіряється функціональність засобів керування та моніторингу, а саме операції отримання відомостей про стан завдання, його призупинення, поновлення та повне скасування виконання. У разі виникнення проблем, локальний адміністратор може побачити повідомлення про помилки безпосередньо у процесі виконання команд, а також у журналах системи керування.

Тести середовища виконання завдань. Серія тестів спрямована на перевірку конфігурації робочих вузлів кластера, де будуть виконуватися грід-завдання.

На вузлі, де встановлено службу обчислювального елемента, перевіряється наявність файлів конфігурації стандартних середовищ виконання для грід-завдань, що дозволяють використовувати клієнтські утиліти пакету ARC, отримати доступ до проксі-сертифіката завдання та використовувати його для авторизації при зверненні до віддалених служб. Наявність цих середовищ виконання є необхідною умовою для проходження зовнішніх тестів.

Для перевірки доступу до мережі до черги ставиться локальне завдання, яке виконує з'єднання із зовнішнім сервером. Перевіряється наявність доступу до мережі із контексту грід-завдання та можливість встановлювати вихідні сеанси зв'язку до зовнішніх серверів. Наявність доступу до мережі також є необхідною умовою для проходження зовнішніх тестів, оскільки вони виконують обмін із сервером автоматизованої системи тестування.

Зовнішнє тестування грід-ресурсу. Для запуску зовнішніх тестів використовується автоматизована система тестування, що дозволяє запускати тести як автоматично так і на вимогу адміністратора грід-сайту. Для проведення тестів використовуються стандартні засоби інтерфейсу користувача командного рядка пакету ARC. Реалізація такої системи має містити веб-інтерфейс та набір сценаріїв, що власне запускають та контролюють виконання тестів. Зовнішні тести дозволяють перевірити роботу грід-ресурсу з точки зору інших грід-сервісів та користувачів, оскільки система тестування розміщується на окремому вузлі і, на відміну від локальних тестів, не має доступу до внутрішніх служб та вузлів грід-сайту, що перевіряється.

Для того, щоб отримати доступ до обчислювального елемента чи елемента зберігання даних через грід-інтерфейс, необхідно мати так званий проксі-сертифікат – короткострокову делегацію від діючого сертифіката користувача чи служби, що був виданий центром сертифікації національної грід-інфраструктури. Адміністратор автоматизованої системи тестування визначає яким чином має отримуватись така делегація. Існує два стандартних підходи до вирішення цієї проблеми:

- використання так званого сертифіката робота, що передбачає зберігання приватного ключа прямо на вузлі системи тестування та генерації короткострокової делегації так само, як і для звичайного користувача грід-інфраструктури;
- отримання короткострокової делегації на підставі політик довгострокової делегації, що завантажується та періодично оновлюється адміністратором системи тестування на окремому сервері служби делегацій MyProxy.

Другий спосіб є більш складним для реалізації, проте є більш захищеним порівняно з першим. У разі несанкціонованого проникнення на вузол системи автоматизованого тестування, у першому випадку зловмисник отримає копію приватного ключа і зможе генерувати необмежену кількість делегацій та виконувати несанкціоновані дії над іншими грід-ресурсами. У другому ж випадку, зловмисник отримає копію лише короткострокової делегації і зможе отримати доступ до грід-ресурсів лише на термін дії цієї делегації, який зазвичай становить декілька годин [10].

Тести інформаційної системи спрямовані на перевірку коректності функціонування служби інформації грід-ресурсу та її реєстрації у каталогах ресурсів.

Перший тест із серії двох тестів виконує запит на отримання відомостей про грід-ресурс за допомогою протоколу LDAP із використанням стандартних утиліт. Цей протокол становить основу інформаційної системи пакетів ARC та gLite. При цьому вимірюється час відгуку сервера та перевіряється, що він знаходиться у допустимих межах. Із наданих сервером даних визначається набір служб, що підтримуються грід-ресурсом. Ці служби будуть перевірятися у наступних тестах. Зокрема, визначається адреса GridFTP-інтерфейсу.

Другий тест перевіряє наявність та коректність реєстрації грід-ресурсу в каталогах вищого рівня. Це буде гарантувати те, що усі грід-сервіси та користувачі, що використовують ті ж самі каталоги ресурсів, зможуть отримати відомості про стан грід-ресурсу та скористатись ним за наявності доступу. Із каталогів ресурсів за допомогою стандартного запиту отримується список усіх зареєстрованих грід-ресурсів. Перевіряється, що всі служби, описані у LDAP-відгуку із попереднього тесту зареєстровані у каталогах вищого рівня та регулярно підтверджують свою наявність. Відомості про ресурси у каталогах мають фіксований час життя і у випадку, коли реєстрацію грід-ресурсу не було вчасно поновлено, запис про нього видаляється.

Тест функціонування GridFTP-інтерфейсу. Унікальність програмного забезпечення проміжного рівня Nordugrid ARC полягає в тому, що протокол GridFTP використовується як для доступу до сховищ даних, так і для направлення завдання на виконання. Це дозволяє запускати служби обчислювального елемента та сховища на одному вузлі, використовуючи спільний інтерфейс. У ході тесту виконується звернення до служби GridFTPd

грід-ресурсу, що тестується. При цьому використовується проксі-сертифікат певного користувача або служби в залежності від налаштувань вузла системи автоматизованого тестування, що був отриманий перед початком тестування. Перевіряється авторизація користувача та отримання списку файлів у кореневому каталозі, як у активному, так і у пасивному режимі обміну протоколу FTP. Також перевіряється сертифікат грід-вузла та його відповідність до імені вузла у системі DNS, що є стандартною вимогою інфраструктури безпеки грід (Grid Security Infrastructure, GSI).

Тести запуску завдання призначені для перевірки функціонування власне служби обчислювального елемента, а також середовища виконання грід-завдання на кластері, що використовується даною службою.

Простий тест запуску завдання спрямований на перевірку середовища виконання завдання, а також коректності взаємодії служби обчислювального елемента із локальною системою керування ресурсами. У сценарії тестового завдання представлені перевірка доступу до сторонніх серверів, а також затримка виконання на 5 хвилин. Із вузла системи автоматизованого тестування проводиться моніторинг стану завдання з моменту його направлення на грід-ресурс до повного завершення виконання або доки не сплив час, виділений на виконання тесту. В останньому випадку тест не зараховується. Після завершення завдання його вихідні файли завантажуються на сервер системи тестування та аналізуються. У разі виявлення помилок при виклику стандартних команд та при доступі до мережі тест не зараховується. Для проходження цього тесту завантаженими кластерами необхідною вимогою є виділення резервації невеликої кількості обчислювальних ядер під тестові завдання з грід-інфраструктури у локальному планувальнику ресурсів кластера.

Повний тест запуску завдання направлений на перевірку функціонування грід-шлюзу обчислювального елемента та засобів інтерфейсу користувача пакету ARC на робочому вузлі. В описі завдання, що направляється на обчислювальний елемент, містяться директиви для підключення стандартних середовищ виконання, а також посилання на вхідні та вихідні файли, що вказують на зовнішні сервери та каталоги даних. Перевіряється можливість програмного забезпечення грід-шлюзу звертатись до зовнішніх серверів. У сценарії завдання міститься звертання до зовнішніх серверів, із використанням проксі-сертифікату завдання, який має надаватись через стандартне середовище виконання. Системою автоматизованого тестування проводиться моніторинг стану завдання та аналізується вихідні файли після його завершення. Перевіряється коректність налаштування стандартних середовищ виконання та можливість доступу до зовнішніх серверів із контексту завдання.

Тест елементу зберігання даних. Для доступу до GridFTP-інтерфейсу, як і у попередніх тестах, використовується проксі-сертифікат. Під час тесту з вузла елемента зберігання даних отримується список файлів та каталогів, відбувається завантаження файлу випадкового вмісту з сервера системи тестування та знову отримується список файлів. Перевіряється видимість нового файлу в списку файлів сховища та можливість завантаження даних. На наступному кроці файл отримується з сховища на сервер системи тестування та порівнюється з вихідним файлом. Перевіряється можливість отримання файлів із сховища та відсутність спотворень вмісту файлу, що можуть виникнути, наприклад, через невірне перетворення CR/LF у текстових файлах. На останньому кроці файл видаляється із сховища.

Колективне тестування взаємодії грід-ресурсів. За допомогою колективних тестів перевіряється взаємодія певного грід-ресурсу із іншими службами у складі національної грід-інфраструктури. Такі тести дозволяють виявити проблеми, що пов'язані із відсутністю зв'язку між певними вузлами, які можуть мати місце навіть при доступності цих вузлів із вузла системи тестування безпосередньо. Взаємодія двох обчислювальних елементів, а також обчислювального елемента та сховища є основою декількох стандартних сценаріїв використання грід-інфраструктури, які відображено у відповідних тестах.

Тест направлення та керування завданням із одного ресурсу на інший дозволяє перевірити коректність роботи інтерфейсу командного рядка клієнтської частини програмного пакету Nordugrid ARC, що викликається у контексті грід-завдання. За допомогою стандартних засобів відбувається направлення завдання на інший кластер із авторизацією за проксі-сертифікатом поточного завдання. Таким чином перевіряється доступність служб зовнішнього кластера із контексту завдання на грід-ресурсі, що тестується. Також перевіряється коректність конфігурації клієнтської частини пакету ARC на робочих вузлах. Зовнішній обчислювальний елемент обирається із списку грід-ресурсів, що успішно пройшли всі тести. У випадку, коли такий список порожній, колективні тести не виконуються. Система автоматизованого тестування формує цей список динамічно та публікує за відповідною адресою, звідки він завантажується сценарій грід-завдання.

Тест направлення завдання, що використовує результати іншого завдання відображає типовий сценарій використання грід-інфраструктури. На грід-ресурс, що перевіряється, направляється завдання, в описі вхідних файлів якого вказані вихідні файли іншого завдання, що завершилось на іншому кластері. Перевіряється коректність взаємодії грід-шлюза обчислювального елемента грід-ресурсу, що тестується, із грід-шлюзом віддаленого обчислювального елемента. Описаний спосіб взаємодії відображає такі сценарії використання грід-інфраструктури як перезапуск довготривалого розрахунку з контрольної точки або подальший аналіз попередньо згенерованих даних.

Тест тристоронньої передачі даних між сховищами. Протоколи доступу до сховищ даних SRM та GridFTP дозволяють здійснювати обмін даними між сховищами оминаючи клієнтський вузол (метод тристоронньої передачі – third party transfer). Такий тест відображає сценарій перекачування великих об'ємів даних між сховищами у процесі їх реплікації для підвищення доступності цих даних чи для прискорення доступу до них із обчислювальних елементів, розташованих близько від задіяних сховищ. На вузлі системи

автоматизованого тестування запускаюся відповідні клієнтські утиліти пакету ARC та інструментарію Globus, що відправляють запит на одне із сховищ на отримання файлу, а на інше – на передачу файлу. При цьому передача відбувається безпосередньо між сховищами, а клієнтські утиліти слугують лише для початкового налаштування такого сеансу, керування ним та авторизації доступу. При зверненні до служб елемента зберігання даних використовується проксі-сертифікат, аналогічно до попередніх тестів. Файли даних для проведення цього тесту попередньо генеруються на вузлі системи автоматичного тестування, а потім завантажуються на одне із сховищ. Після завершення тристоронньої передачі відповідний файл отримується із іншого сховища та порівнюється із оригіналом на вузлі системи тестування.

Реалізація прототипу системи автоматизованого тестування

Прототип автоматизованої системи тестування ресурсів було реалізовано на базі обчислювального кластера Київського національного університету імені Тараса Шевченка. До складу реалізованого прототипу системи тестування входить набір сценаріїв для побудови веб-інтерфейсу мовою PHP, набір shell-сценаріїв, які реалізують тести, та допоміжна утиліта для отримання сертифіката вузла, реалізована мовою C.

Вищеописані критерії та тести реалізовано у сценаріях тестування мовою Bash з використанням стандартних UNIX-утиліт, засобів інтерфейсу командного рядка пакетів Nordugrid ARC та Globus Toolkit. Так, локальне тестування представлене наступними сценаріями, що можуть бути викликані адміністратором грід-ресурсу самостійно:

- тест файла конфігурації;
- тест локального грід-середовища;
- тест локального запуску завдання.

Зовнішні та колективні тести запускаються за допомогою веб-інтерфейсу системи тестування та можуть виконуватися паралельно для кожного грід-ресурсу в фоновому режимі. Стан процесу тестування кожного ресурсу відображається на головній сторінці веб-інтерфейсу (рис. 1). Під час виклику утиліт інтерфейсу командного рядка пакету Nordugrid та будь-яких інших довготривалих операцій застосовується обмеження за часом виконання операції 30 секунд. Процедуру запуску кожного тесту оформлено у вигляді окремого сценарію, що викликається загальною оболонкою у контексті фонового завдання. У прототипі реалізовано наступні сценарії тестів:

- тест інформаційної системи грід-ресурсу та реєстрації у каталогах;
- тест сертифіката грід-вузла;
- тест GridFTP-інтерфейсу вузла;
- простий тест запуску грід-завдання на обчислювальному елементі;
- тест запуску грід-завдання із віддаленим завантаженням вхідних та вихідних даних;
- тест віддаленого запуску завдання із віддаленими даними;
- перевірка обміну даними із елементом зберігання даних;
- колективний тест віддаленого запуску грід-завдання із результатами іншого завдання як вхідні дані;
- колективний тест направлення нового завдання на грід-ресурс із контексту поточного завдання;
- тест тристоронньої передачі даних між елементами зберігання даних.

Загальний сценарій-оболонка також відповідає за виклик допоміжних сценаріїв для отримання тимчасової делегації та кінцевого форматування результатів серії тестів для її відображення у веб-інтерфейсі. Результати роботи кожного сценарію запуску тестів записуються до журналу, який потім форматується для більш зручного відображення у веб-інтерфейсі. Приклад такої сторінки із протоколом перевірки грід-ресурсу показано на рис. 2.

Список грід-ресурсів, що перевіряються автоматизованою системою тестування, задається у конфігураційному файлі у формі декларації масивів мови PHP:

```
$celist = array(
      "a30a71dc-9d63-4ba2-bc39-282d16039120" => array(
            "name" => "IPM",
            "ce_host" => "grid.ipm.lviv.ua",
      ),
      ...
);
$selist = array(
      "f821cf2f-76cd-4b70-8fa3-6f5525665fa9" => array(
            "name" => "KNU_1",
            "se_name" => "pub:arc.univ.kiev.ua"
      ),
      ...
);
```

Кожен грід-ресурс має унікальний ідентифікатор у формі GUID, який використовується у системі для зберігання динамічних відомостей про стан тестів. Для обчислювальних елементів вказується ім’я вузла, а для сховищ даних – назву сховища в інформаційній системі. Всі інші відомості про грід-ресурси, такі як адреса

GridFTP-інтерфейсу, отримуються системою тестування автоматично під час тесту інформаційної системи грід-ресурсу. Це значно спрощує додавання нових грід-ресурсів та загальне обслуговування системи автоматизованого тестування.

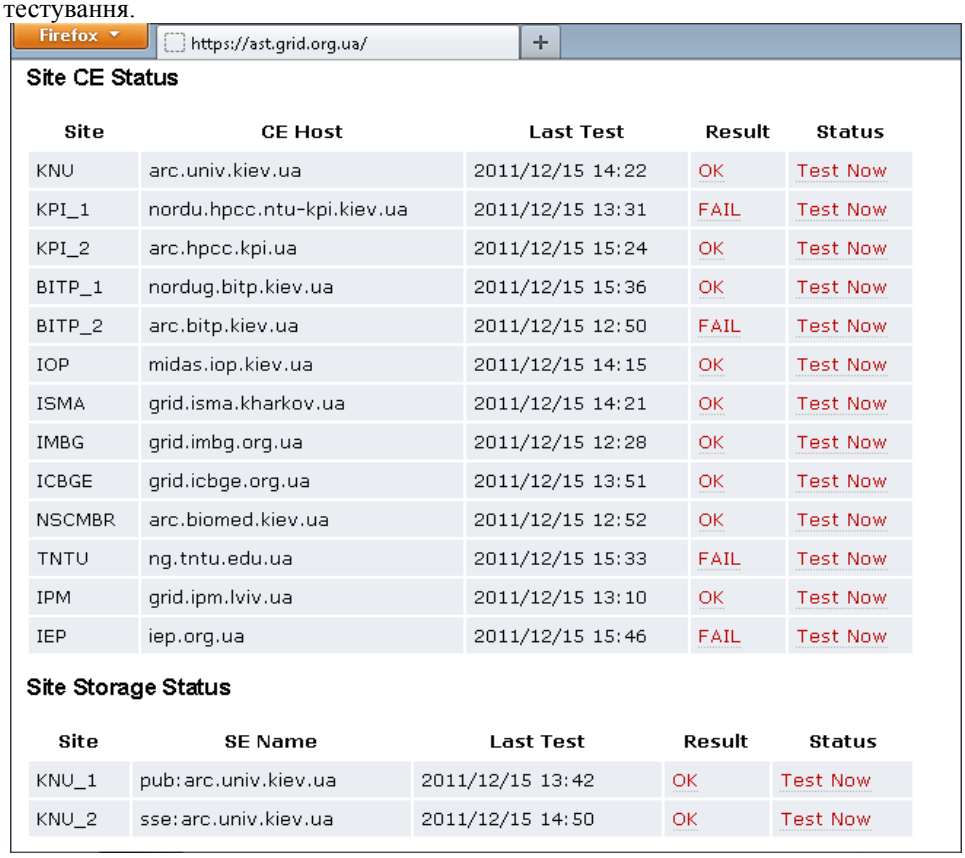

Рис. 1. Головна сторінка веб-інтерфейсу прототипу системи автоматизованого тестування

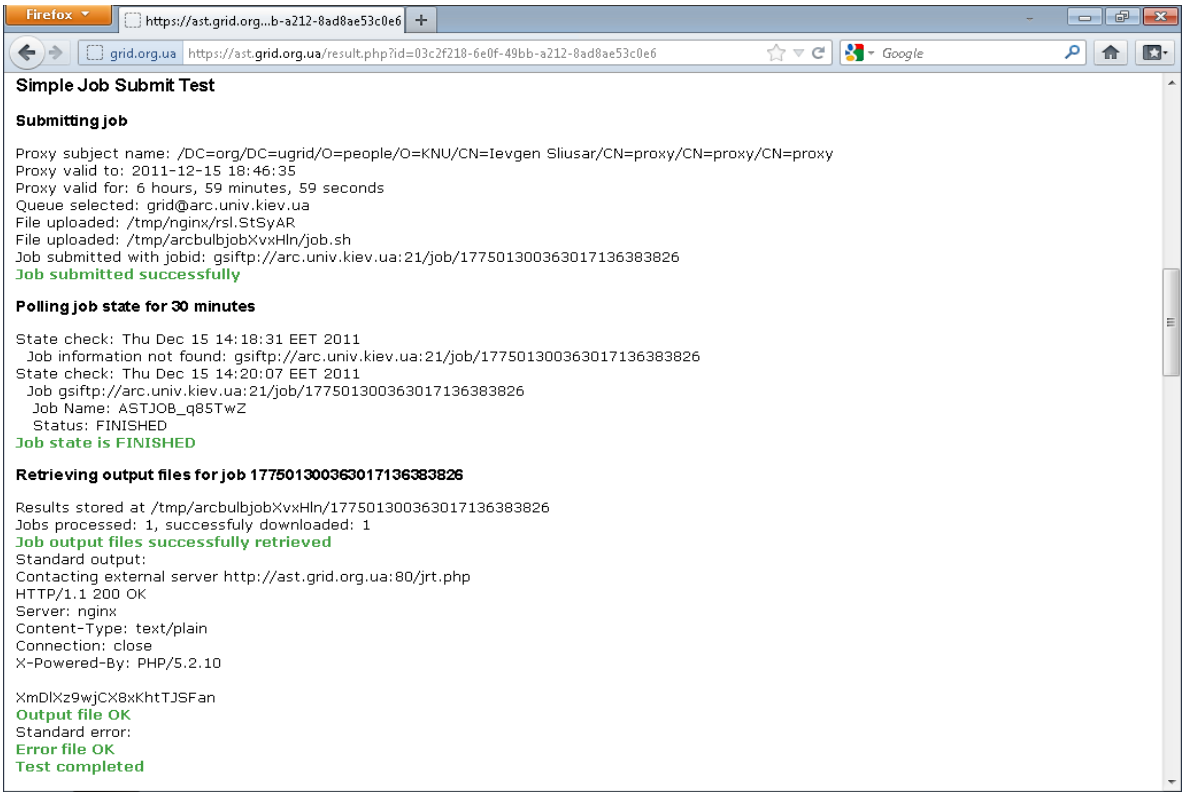

Рис. 2. Сторінка протоколу перевірки грід-ресурсу прототипу системи автоматизованого тестування

Висновки

Здійснено детальний аналіз можливостей та механізмів роботи існуючих засобів тестування та моніторингу грід-ресурсів у складі глобальних грід-інфраструктур, у ході якого було оцінено застосовність стандартних рішень до українського національного грід-сегменту. У зв'язку із функціональною обмеженістю існуючих рішень та великим розмаїттям операційних середовищ кластерів національного грід-сегменту, було запропоновано власну архітектуру системи автоматизованого тестування грід-ресурсів.

Унікальною особливістю запропонованої архітектури є запровадження тестів колективної взаємодії грід-ресурсів, що відповідають типовим сценаріям використання грід-інфраструктури. До переваг також слід віднести наявність локальних тестів, що дозволяють перевірити роботу внутрішнього операційного середовища та системи керування ресурсами обчислювального кластера.

Реалізовано прототип автоматизованої системи тестування, який базується на використанні стандартних технологій, таких як PHP та UNIX Shell. Реалізовано базові функції запропонованої архітектури, необхідні для моніторингу функціонування грід-ресурсів в українській національній грід-інфраструктурі.

Представлений прототип системи автоматизованого тестування може бути застосований для моніторингу інших грід-інфраструктур, побудованих із використанням програмного забезпечення проміжного рівня Nordugrid ARC, а окремі його компоненти можуть бути інтегровані до інших систем автоматизованого тестування для збільшення покриття тестами функціональності грід-ресурсів.

1. *Foster I., Kesselman C.* The Grid, Blueprint for a New computing Infrastructure. – Morgan Kaufmann Publishers, Inc., 1998.
2. *Демичев А., Ильин В., Крюков А.* Введение в грид-технологии. – 2007. http://www.sinp.msu.ru
3. *EGI-InSPIRE* Project Metrics – http://www.egi.eu/projects/egi-inspire/metrics
4. *Foster Ian, Kesselman Carl, Tuecke Steven.* The Anatomy of the Grid – Enabling Scalable Virtual Organizations // International Journal of Supercomputer Applications. – 2001. – Vol. 15. – P. 2001.
5. *Novak Judit, Nyczyk Piotr, Vidic Valentin.* Monitoring in EGEE // EGEE/SEEGRID Summer School. – Budapest, 2006.
6. *Service* Availability Monitoring. End-to-end service monitoring for computing grids. – https://tomtools.cern.ch/confluence/display/SAMWEB
7. *Aeschlimann Andres.* Multi Level Monitoring Overview. – 20 Jun 2011, CERN Public TWiki, EGEE Support Activity 1. https://twiki.cern.ch/twiki/bin/view/EGEE/MultiLevelMonitoringOverview
8. *Ellert Mattias.* Advanced Resource Connector middleware for lightweight computational Grids // Future Gener. Comput. Syst. – 2007. – Vol. 23, N. 1. – P. 219–240.
9. *Бойко Ю.В., Зинов'єв М.Г., Судаков О.О., Свістунов С.Я.* Український академічний Грід: досвід створення й перші результати експлуатації // Математичні машині і системи. – 2008. – Випуск 1. – С. 67–84.
10. *Novotny J., Tuecke S., Welch V.* An Online Credential Repository for the Grid: MyProxy // Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10), IEEE Press. – August 2001. – P. 104–111.