Развитие GRID-сети ВЦ ДВО РАН

Т. С. Шаповалов, А.Ю. Сапронов, А.Г. Тарасов.

В докладе изложен опыт расширения GRID-сети Вычислительного центра ДВО РАН. Доклад охватывает описание GRID-сети, полученной в результате подключения территориально распределённых вычислительных ресурсов научных и коммерческих организаций, показаны проблемы построения подобных сетей и способы их решения, представлены результаты экспериментов работы в GRID-сетях микропроцессоров различных архитектур. Одним из направлений исследований ВЦ ДВО РАН являются распределённые вычисления, осуществляемые на кластерах - машинах с массивно параллельной архитектурой. В ВЦ ДВО РАН спроектированы и внедрены несколько таких установок. Развёрнута инфраструктура по управлению множеством распределённых кластеров (Инфраструктура PKI, web-сервисы для работы пользователей, Globus Toolkit). Выбор Globus Toolkit 4.x (GT) в качестве инструментария для построения каркаса GRID-сети обусловлен его широкой распространённостью и направленностью на соответствие международным стандартам. GT представляет собой открытый, свободно распространяемый сервис-ориентированный (SOA) набор программного обеспечения (ПО) для построения GRID-сетей и сервисов в них. Среди прочего, GT обеспечивает работу базовых служб, таких как безопасная передача данных, аутентификация, сбор и накопление информации о ресурсах, их администрирование. В терминологии SOA-подхода, основной задачей GT является обеспечение работы контейнера web-сервисов, являющихся основой функциональности GRID-сети. GT, обладая модульной и открытой структурой, позволяет добавлять как готовые, так и собственные компоненты в GT-контейнер. Это создаёт возможности географической и архитектурной масштабируемости и расширяемости системы. С другой стороны, географическое распределение компонентов сети накладывает жёсткие требования к безопасности каналов связи и механизмов авторизации составных частей системы (пользователи, узлы, сервисы и ряд других). Как уже было указано, GT удовлетворяет подобным требованиям, обеспечивая безопасность на уровне WS-ресурсов, а также аутентификацию и безопасность транспортного уровня. Особенности работы в рамках GRID-сети вычислительных ресурсов с различной архитектурой были рассмотрены на эксперименте, включающем в себя оценку возможностей ПО для анализа архитектуры системы, планирования и способов создания заданий. Различия систем выражались в архитектуре вычислительных узлов, входящих в сеть (SMP, NUMA), разрядности аппаратного и программного обеспечения, стандартов коммуникаций и коммуникационных библиотек. Для решения задач создания, планирования и распределения вычислительных запросов в соответствии с имеющимися ресурсами использовалась система мета-планирования GridWay и нижележащее программное обеспечение - менеджер управления локальными вычислительными ресурсами TorquePBS, основанный на открытых стандартах POSIX. Эксперимент не был бы возможен без наличия в составе GRID-сети коммерческих организаций, в рамках которых возможно сосредоточение разнородных ресурсов, в то время как для научной организации наличие в своём компьютерном парке многообразия вычислительной техники не является оправданным и целесообразным. Наравне с возможностью получения доступа к таким ресурсам или сервисам необходимо решать вопросы ограничения доступа к ним. При участии в GRID организаций с общим направлением деятельности подобные ограничения могут быть не столь существенны, однако в GRID-сетях с организациями-участниками, большую часть времени преследующих не связанные между собой цели, напротив, необходимо решать такие вопросы. Также необходимо иметь инструменты для учёта использования ресурсов. Упомянутая выше система GridWay при планировании и запуске, опираясь на инфраструктуру подсистемы безопасности GT, позволяет гибко назначать права доступа на запуск заданий в GRID на тех или иных вычислительных узлах. GridWay даёт возможность контролировать выполнение заданий на принадлежащих организации вычислительных мощностях таким образом, что эти ресурсы будут предоставлены узкому кругу лиц, участвующих в экспериментах, в то время как большинству пользователей данные виды ресурсов будут недоступны, несмотря на установленные доверительные отношения посредством общего центра сертификации.