Управление вычислительным комплексом: вопросы безопасности и конфиденциальности

Т.С. Кушнир

ЗАО «Т-Сервисы», Москва

На данном этапе развития современных вычислительных комплексов существует проблема создания унифицированного, эффективно использующего ресурсы и предоставляющего гибкие настройки безопасности и конфиденциальности управляющего программного обеспечения. Всякий раз при построении нового большого суперкомпьютера, задача выбора ПО для управления и мониторинга решается практически с нуля. Особенно это актуально для компаний, предоставляющих машинное время в аренду, поскольку ни бесплатного, ни коммерческого комплексного пакета ПО такого класса пока не существует.

С точки зрения эффективности использования, имеется несколько вариантов решения задачи мониторинга, управления узлами и компонентами суперкомпьютера, создания и управления очередями заданий. Что касается вопросов безопасности суперкомпьютеров, их решение либо не происходит вообще (нет обеспечения безопасности/конфиденциальности), либо всё сводится к разграничению доступа к файлам и данным на уровне пользователей операционной системы, назначению прав доступа к хранилищам и иным компонентам суперкомпьютера, а передача всех данных по открытым каналам происходит с шифрованием данных (используя технологию SSL). Такой подход, в частности, в среде Linux не избавляет от следующих ситуаций (если не вносить модификацию в исходные тексты ядра и утилит ОС):

1. практически любой пользователь может узнать кто, когда и какое время использует узлы суперкомпьютера;
2. практически любой пользователь может узнать, кто в данный момент находится на управляющем узле суперкомпьютера и какие процессы запускает, какие программы использует (при наличии нескольких управляющих узлов – только на том, на который пользователь вошёл);
3. при определённых навыках, пользователь может узнать что, кем и где запущено на вычислительных узлах суперкомпьютера (только в том случае, если разграничение доступа на узлы суперкомпьютера сделано стандартным для ОС Linux способом);
4. при использовании стандартных коммерческих вычислительных пакетов на суперкомпьютере, практически любой пользователь может получить доступ к временным данным других пользователей (только в случае, если сам пользователь не позаботится о сохранности своих данных).

Помимо названных, существует ещё несколько ситуаций, в которых возможна утечка конфиденциальной информации при работе на «стандартном» суперкомпьютере под управлением ОС Linux.

В данном докладе будет сформулирован набор требований к ПО, устанавливаемом на вычислительном комплексе. Особое внимание при этом будет уделено вопросам безопасности и конфиденциальности данных пользователей.