СИСТЕМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ КОМПЬЮТЕРНОЙ СЕТЬЮ «ARAMID-DS»

Алешкин В. А.

ФГУП «РФЯЦ ВНИИЭФ», г. Саров Нижегородской обл.

Современный мир передовых научных технологий сложно представить без высокопроизводительных расчетов, выполняемых средствами многопроцессорных вычислительных комплексов (МВК).

Новые технологические задачи требуют не только наращивания аппаратных мощностей МВК, но и сохранение конфиденциальности обрабатываемой информации. По этим причинам создаются аппаратные и программные решения, позволяющие обеспечивать необходимый режим секретности при работе на МВК. Одним из таких решений является созданный коллективом разработчиков ФГУП «РФЯЦВНИИЭФ» дистрибутив специализированной защищенной операционной системы «Арамид» [1], который удовлетворяет требованиям ФСТЭК России по обработке информации, составляющей государственную тайну.

ЗОС «Арамид» предназначен для организации распределенных высокопроизводительных вычислений, содержащих сведения, составляющие государственную тайну, на супер-ЭВМ предприятий госкорпорации «РосАтом» и Оборонно-промышленного комплекса.

При создании и эксплуатации многопроцессорных вычислительных комплексов важным и моментом является организация системы управления компьютерной сетью.

Управление компьютерной сетью в данном случае представлено тремя основными направлениями:

– непосредственно управление ресурсами домена компьютерной сети – идентификационными данными для пользователей, хостов и сервисов.

– аутентификация или подтверждение подлинности объекта. Данный процесс также актуален для пользователей, хостов и сервисов.

– разграничение доступа. Здесь основными аспектами является управление политиками доступа и привилегиями пользователей.

Таким образом, можно ввести определение: система централизованного управления компьютерной сетью – это распределенная система, позволяющая организовать в рамках многопроцессорного вычислительного комплекса централизованное управление ресурсами домена компьютерной сети.

Основные задачи, которые стоят перед данной системой:

В рамках создания такой системы для ЗОС «Арамид» разработчикам необходимо было решить следующие задачи:

– создание централизованной модели хранения учетных данных вычислительного комплекса;

– предоставление механизмов безопасной идентификации и аутентификации;

– администрирование системы через единый интерфейс;

– реализация технологии «единого входа» пользователей;

– организация управления политиками безопасности;

– интеграция с средствами защиты информации реализованными в защищенной операционной системе «Арамид».

В условиях большого количества узлов, для создания системы централизованного управления идентификационными данными необходимо решить следующие подзадачи. А именно:

– создание единого хранилища для учетных данных – поскольку на каждом узле МВК хранятся собственные учетные записи пользователей, групп пользователей, файлов хостов и т.д.;

– создание централизованной системы идентификации и аутентификации – иначе настройки необходимо выполнять на каждом узле МВК;

– создание единого интерфейса администрирования – при его отсутствии необходимы дополнительные ресурсы для поддержания данных в актуальном состоянии;

– реализация единого поставщика аутентификационных данных – позволяет избежать накапливания учетных записей пользователей и паролей для различных сервисов;

– обеспечение возможности хранения конфигураций сервисов в едином точке – исключает необходимость настраивать сервисы на каждом узле, повторяя одни и те же операции.

А использование на узлах комплекса защищенной операционной системы добавляет к этому списку еще несколько критериев:

– организация централизованного механизма управления политиками безопасности – совместимого с собственной системой разграничения доступа операционной системы «Арамид»;

– разработка механизмов взаимодействия со средствами защиты информации – системное программное обеспечение необходимо адаптировать к работе средств защиты информации.

В начале работ был рассмотрен вопрос использования существующих реализаций систем центра-

лизованного управления компьютерной сетью. Рассмотренные варианты представлены в таблице.

Основные реализации систем централизованного управления компьютерной сетью

Реализация	Недостатки
Microsoft Active Directory	Коммерческий продукт компании Microsoft; закрытая реализация без возможности доработки.
Free IPA	Использование системы разграничения доступа на основе SELinux; большое количество предустановленных политик безопасности.
Open AM	Собственная модель политик безопасности, переход на коммерческую лицензию в новых версиях.
Open LDAP + Kerberos	Сложность конфигурирования и интеграции сервисов, сложность администрирования сервисов.

Кроме того все рассмотренные варианты не имели возможности работы с атрибутами безопасности ЗОС «Арамид» и не имели поддержки СЗИ ЗОС «Арамид».

В связи с этим было принято решение о создание собственной системы централизованного управления компьютерной сетью. Проект получил название «Aramid Directory Service» или «Aramid-DS».

Aramid Directory Service (Aramid-DS) – это система централизованного управления компьютерной сетью в рамках многопроцессорного вычислительного комплекса, реализованная на базе открытых программных решений.

В состав Aramid-DS входят следующие программные компоненты:

– служба каталогов OpenLDAP – обеспечивает централизованное хранение ресурсов домена компьютерной сети (учетные записи, атрибуты безопасности и т. д.);

– система безопасной аутентификации Kerberos – предоставляет протоколы безопасной идентификации и аутентификации, является основой для функционирования технологии «единого входа»;

– служба имен BIND – реализует централизованный механизм управления именами узлов вычислительного комплекса;

– подключаемые библиотеки аутентификации PAM – интегрируют различные механизмы аутентификации, управления учетными записями и сеансами пользователей, предоставляя единый высокоуровневый API;

– утилита системного администрирования политик SUDO – предоставляет возможность назначения административных привилегий для пользователей;

– модуль работы с мандатным окружением – обеспечивает интеграцию сервисов «Aramid-DS» с средствами защиты информации ЗОС «Арамид»;

– утилиты автоматического конфигурирования «Aramid-DS» – набор утилит, которые предоставляют возможность выполнить автоматическую настройку всех сервисов «Aramid-DS»;

– утилиты администрирования– предоставляют единый интерфейс администрирования системы без прямого взаимодействия с сервисами «Aramid-DS»;

– модуль синхронизации сетевых и локальных групп пользователей – механизм централизованное управление системными группами пользователей.

На рис. 1 представлена абстрактная схема функционирования компонентов Aramid-DS:

– обозначено взаимодействие компонентов серверной части «Aramid-DS»;

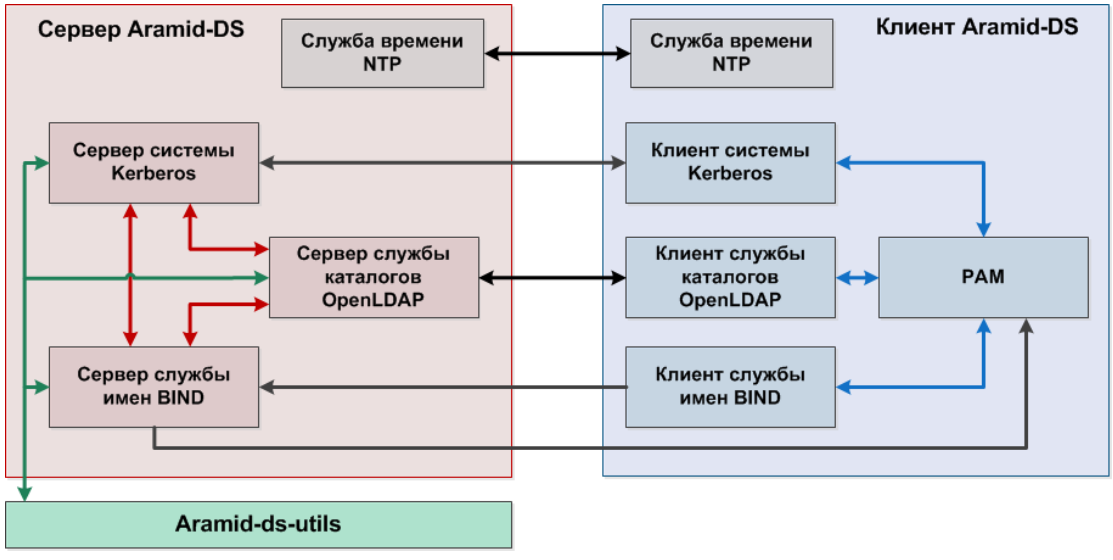

Рис. 1. Абстрактная схема функционирования компонентов Aramid-DS

– представлена модель централизации данных сервисов в службе каталогов OpenLDAP, а также использование сервера имен BIND системой Kerberos;

– сервер и клиент Aramid-DS синхронизированы по времени при помощи протокола NTP, поскольку это одно из необходимых условий работы системы Kerberos;

– обозначено взаимодействие компонентов клиентской части «Aramid-DS». Представлена модель работы набора библиотек PAMc прочими сервисами в составе Aramid-DS;

– обозначено межсерверное взаимодействие компонентов «Aramid-DS». Тут отображено взаимодействие клиентских и серверных частей различных узлов вычислительного комплекса;

– обозначено взаимодействие утилит администрирования с компонентами «Aramid-DS».

Рассмотрим основные функциональные возможности системы централизованного управления компьютерной сетью «Aramid-DS».

1. Централизованное хранение учетных данных

«Aramid-DS» предоставляет механизм централизованного хранения для учетных данных, к которым относятся:

– учетные записи пользователей;
– учетные записи групп пользователей;
– атрибуты безопасности пользователей;
– уровни и категории доступа (MAC);
– хосты и подсети МВК;
– конфигурации сервисов;
– информация о подключаемых носителях;
– политики SUDO.

2. Технология «единого входа» на МВК

Пользователь, выполнив процедуру аутентификации с использованием логина и пароля, получает билет Kerberos, который в дальнейшем используется для автоматического прохождения процедуры аутентификации без необходимости повторного ввода пароля.

Билет используется системой Kerberos для процедуры взаимной аутентификации пользователя и сервиса, которая выполняется при обращение пользователя к сервису. При этом процесс происходит не заметно для самого пользователя. Билет имеет настраиваемый срок действия и изменяемые функциональные ограничения. Схема функционирования для технологии «единого входа» представлена на рис. 2.

3. Автоматическое конфигурирование компонент системы

Конфигурирование компонент системы централизованного управления компьютерной сетью – процесс, требующий серьезных компетенций и знаний, поскольку каждый из компонентов уже является сложной системой, а организация их непосредственного взаимодействия – задача, которая требует глубоких познаний в администрировании системного программного обеспечения.

Система «Aramid-DS» предоставляет механизмы автоматического конфигурирования компонент системного программного обеспечения без специальных знаний и необходимости прямого конфигурирования каждого из компонентов. Администратору достаточно внести изменения в небольшой конфигурационный файл и запустить соответствующую роли узла утилиту.

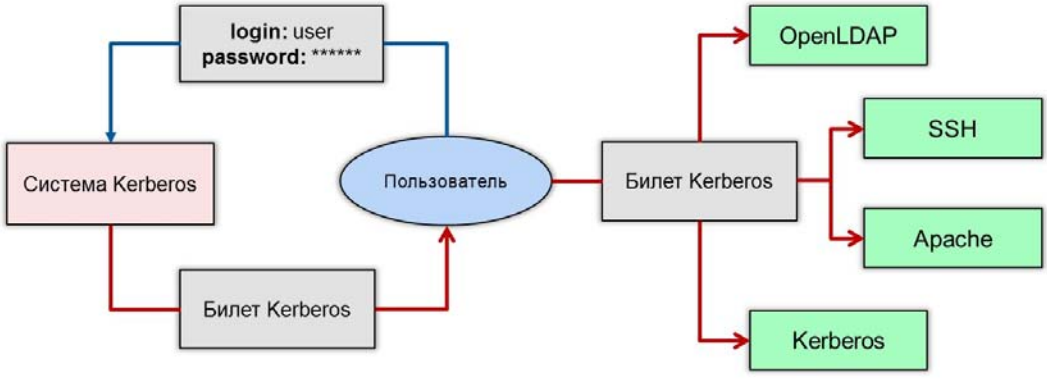

Рис. 2. Функциональная схема технологии «единого входа»

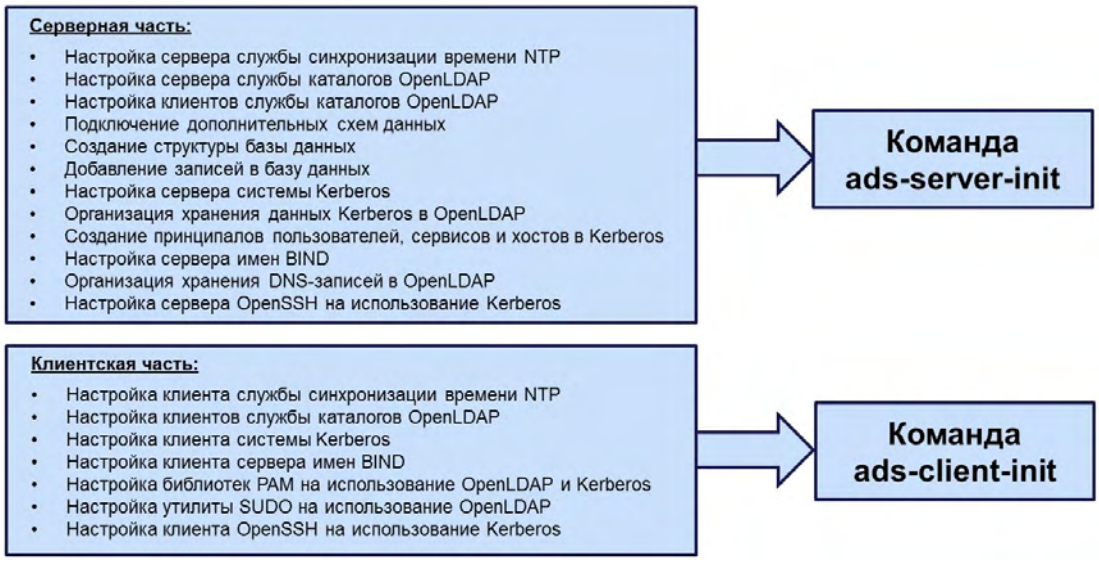

Рис. 3. Пример автоматизации конфигурирования компонент «Aramid-DS»

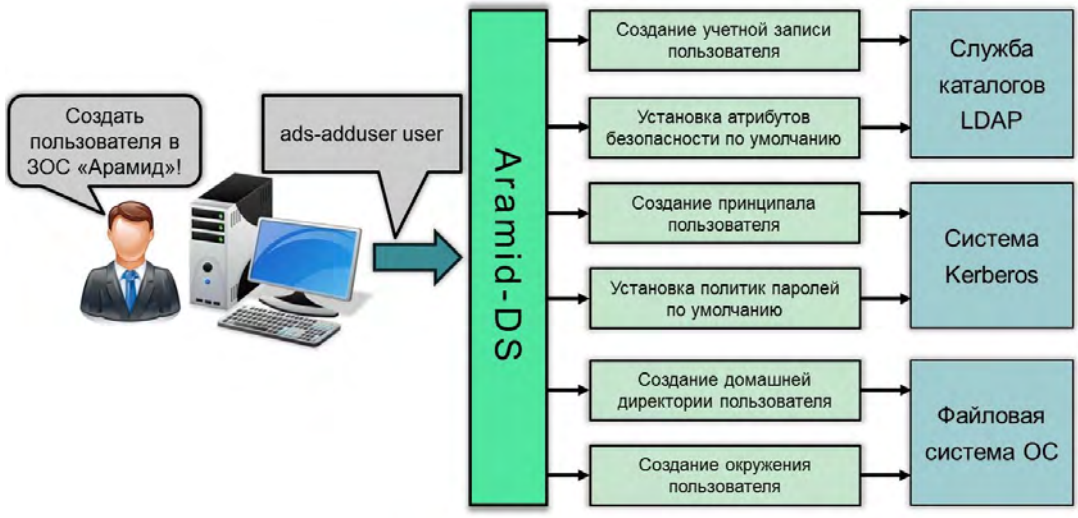

Рис. 4. Пример использования утилит администрирования

На рис. 3 представлен наглядный пример, сколько действий требуется для настройки компонент без использования специальных утилит.

Также в составе «Aramid-DS» входят утилиты, позволяющие выполнить откат изменений в конфигурации компонентов к их первоначальному состоянию.

4. Единый интерфейс администрирования

Специально разработанные утилиты администрирования исключают необходимость взаимодействия с каждым компонентом «Aramid-DS», предоставляя единый интерфейс управления удобный и понятный для пользователя.

Утилиты администрирования «Aramid-DS»предоставляют следующие возможности:

– создание/редактирование/удаление учетных записей пользователей и групп пользователей;

– управление привилегиями пользователей (административными полномочиями;

– создание/удаление категорий доступа, уровней доступа;

– создание/редактирование/удаление политик паролей пользователей;

– добавление/удаление пользователей в группы пользователей пользователе;.

– просмотр информации о пользователях, группах пользователей, хостах и устройствах;

– вывод идентификационной информации пользователей;

– блокировка/разблокировка учетных записей пользователей;

– управление паролями пользователей.

На рис. 4 представлен пример заведения пользователя с использованием консольной утилиты «ads-adduser». На схеме видно, насколько прост синтаксис

Рис. 5. Организация единого пользовательского пространства

утилиты для пользователя и сколько процедур скрывается за выполнением данной утилиты на стороне сервера.

5. Интеграция с web-интерфейсом администратора безопасности

Web-интерфейс администратора безопасности - это графическая интерактивна web-среда, выполняющая в операционной системе «Арамид» централизацию административных и пользовательских сервисов в режиме дистанционного доступа.

Web-интерфейс имеет поддержку «Aramid-DS», обеспечивая возможность визуализации хранящейся в «Aramid-DS» информации, а также предоставляя возможность управления ресурсами компьютерной сети через графический web-интерфейс.

6. Организация единого пользовательского пространства

Система «Aramid-DS» является источником необходимых данных и сервисных возможностей для различных компонент операционной системы «Арамид». Обеспечивая таким образом возможность организации Единого Пользовательского Пространства. На рис. 5 приведены примеры основных функциональных взаимодействий «Aramid-DS» в рамках организации единого пользовательского пространства.

Результатом выполненной работы является создание системы централизованного управления идентификационными данными «Aramid-DS», которая позволяет преодолеть сложности работы с учетными данными на многопроцессорных вычислительных комплексах, а также адаптирована для работы в защищенной операционной системе «Арамид».

Стоит также отметить, что в составе дистрибутива операционной системы «Арамид» успешно пройдены сертификационные испытания и проводится успешное внедрение в составе ЗОС «Арамид» на предприятия госкорпорации «Росатом и предприятия ОПК.

Созданный программный продукт является полноценным инструментом централизованного управления компьютерной сетью, функционирующим на многопроцессорных вычислительных комплексах с обеспечением необходимого режима безопасности.

В планах дальнейших работ по развитию системы централизованного управления компьютерной сетью «Aramid Directory Service» – реализация поддержки сетевых протоколов SAMBA, FTP и VNC, повышение отказоустойчивости за счет репликации сервисов и интеграция с наиболее значимыми аналогичными системами.

Литература

1. Петрик А. Н. Защищенная операционная система «Арамид» для супер-ЭВМ / VIII Форум «Информационные технологии на службе оборонно-промышленного комплекса России» // Сборник тезисов. Екатеринбург, 2019. С. 11.