УДК 004.056 doi: 10.15827/0236-235X.148.461-471 2024. Т. 37. № 4. С. 461–471

Управление пользовательскими заданиями в сети суперкомпьютерных центров с применением федеративной аутентификации

А.В. Баранов [1, 2]✉, Е.Е. Кузнецов [2]

[1] Межведомственный суперкомпьютерный центр РАН, г. Москва, 119334, Россия
[2] Национальный исследовательский центр «Курчатовский институт», г. Москва, 123182, Россия

Ссылка для цитирования
Баранов А.В., Кузнецов Е.Е. Управление пользовательскими заданиями в сети суперкомпьютерных центров с применением федеративной аутентификации // Программные продукты и системы. 2024. Т. 37. № 4. С. 461–471. doi: 10.15827/0236-235X.148.461-471
Информация о статье
Группа специальностей ВАК: 2.3.6
Поступила в редакцию: 20.07.2024 После доработки: 22.08.2024 Принята к публикации: 30.08.2024

Аннотация. Предметом представленного в статье исследования является управление пользовательскими заданиями в распределенной сети научных суперкомпьютерных центров (СКЦ) коллективного пользования. Сеть СКЦ объединяет высокопроизводительные вычислительные системы разной архитектуры, принадлежащие различным СКЦ. Каждый центр самостоятельно определяет политику безопасности и поддерживает собственную базу учетных записей пользователей, что осложняет управление пользовательскими заданиями, в частности, затрудняет оперативное перераспределение заданий между вычислительными системами разных СКЦ. Методология исследования базируется на совмещении двухуровневой иерархической системы управления заданиями и федеративного управления идентификацией, в частности, федеративной аутентификации. В работе предложен новый метод управления пользовательскими заданиями в распределенной сети СКЦ, основанный на федеративной аутентификации. Верхний уровень иерархии управления представлен глобальной очередью, из которой задания распределяются по вычислительным системам распределенной сети СКЦ. Локальные очереди этих вычислительных систем образуют нижний уровень иерархии управления заданиями. Аутентификация и авторизация для каждого задания должны производиться дважды: при постановке в глобальную очередь и при распределении в одну из локальных очередей. Предлагаемый метод учитывает, что за время нахождения в глобальной очереди задание с точки зрения информационной безопасности превращается из объекта в субъект, который заново должен быть авторизован в локальной очереди. Как показано в статье, применение федеративной аутентификации при авторизации пользователей и их заданий позволяет построить простую и безопасную схему управления заданиями в сети СКЦ. Практическую значимость исследования составляют представленный в статье порядок функционирования системы управления заданиями в распределенной сети СКЦ и анализ безопасности такой системы.

Ключевые слова: сеть суперкомпьютерных центров, управление заданиями, очередь заданий, федеративная аутентификация, поставщик услуг, поставщик идентификационных данных

Благодарности. Работа выполнена в МСЦ РАН и НИЦ «Курчатовский институт» в рамках госзадания по теме FNEF-2024-0014

Введение. Формированию единого научно-образовательного пространства информационных технологий в стране придается большое значение. Так, в Межведомственном суперкомпьютерном центре РАН ведутся работы по созданию прикладной цифровой платформы, объединяющей в единую сеть вычислительные ресурсы территориально распределенных *суперкомпьютерных центров* (СКЦ) коллективного пользования в интересах организаций науки, высшего образования и промышленности Российской Федерации [1]. Представленный в [2] метод управления заданиями пользователей в распределенной сети СКЦ основан на двухуровневой организации системы управления. Единицей вычислительной работы в такой системе является задание, включающее параллельную программу для прикладных расчетов, требования к ресурсам и входные данные. Единицей оборудования в составе распределенной сети СКЦ является высокопроизводительная *вычислительная система* (ВС). Для управления отдельной ВС используется *локальная система управления ресурсами* (ЛСУР), действия всех ВС в сети координирует *глобальная система управления ресурсами* (ГСУР). В качестве ЛСУР может выступать любая система управления заданиями (СУППЗ, SLURM, PBS), поступающие в ЛСУР задания могут выполняться только на вычислительных ресурсах локальной ВС. Задания могут быть направлены в ГСУР, которая ведет глобальную очередь. Задания из глобальной очереди допускают обработку на вычислительных ресурсах любой ВС сети. Для распределения заданий из глобальной очереди в очереди ЛСУР могут быть применены различные алгоритмы, в том числе основанные на экономических (аукционных) методах.

Вне зависимости от способа распределения заданий глобальной очереди пользователь (субъект) оставляет после себя объекты – зада-

ния, которые продолжительное время (от нескольких минут до нескольких суток) проводят в глобальной очереди. Прошедшее глобальную очередь задание будет претендовать на вычислительные ресурсы назначенной ему локальной ВС. Однако на момент распределения задания из глобальной очереди в локальную пользователь может потерять право доступа к ресурсам назначенной ВС или исчерпать квоту. Фактически за время нахождения в глобальной очереди задание из информационного объекта превращается в субъект, который в том числе должен быть авторизован в СКЦ на уровне планирования локальных ресурсов.

В работе [2] была предложена децентрализованная автоматизированная система управления заданиями и ресурсами в распределенной сети СКЦ. Авторы решили проблему повторной проверки прав доступа путем ввода дополнительных сущностей – диспетчера СКЦ и диспетчера ВС. В предложенной схеме диспетчер СКЦ служит точкой доступа к ГСУР, а коллектив равноправных диспетчеров ВС предназначен для распределения заданий из глобальной очереди в локальные. Недостаток такого подхода в том, что диспетчеры являются узлами отдельной защищенной распределенной сети. Масштабируемость подобного решения ограничена, так как при росте числа СКЦ и ВС в сети увеличиваются технические и организационные сложности поддержки функционирования защищенной сети.

Другим важным направлением исследований в области построения распределенной сети СКЦ является упрощение доступа пользователей к вычислительным ресурсам сети. С этой целью была предложена федеративная схема аутентификации и авторизации, позволяющая пользователям использовать одну учетную запись для доступа ко всем суперкомпьютерным ресурсам сети [3]. Распространенным решением для реализации механизмов аутентификации и использования идентификационной информации в нескольких организациях является федеративное управление идентификацией (*Federated Identity Management* – FIM). В федерации формируются трехсторонние отношения между поставщиком услуг (*Service Provider* – SP), поставщиком идентификационных данных (*Identification Provider* – IdP) и пользователем, которые позволяют пользователям получать доступ к SP с помощью одного набора учетных данных, таких как подписанные доверенным IdP токены и утверждения. Например, пользователь после аутентификации у поставщика идентификационных данных получает утверждение (билет) SAML (*Security Assertion Markup Language* – стандарт управления федеративными идентификационными данными), и этот IdP-билет позволяет ему авторизоваться на стороне поставщика услуг.

В [3] рассмотрен подход к организации авторизации пользователей в распределенной сети СКЦ, который дает возможность сочетать механизм федеративной аутентификации с традиционными методами доступа к суперкомпьютерам, основанными на протоколе ssh. В работе [4] авторы уточнили процедуру информационного обмена и состава информации (метаданных), предоставляемых организацией-клиентом (IdP) СКЦ при постановке заданий в очередь и передаваемых при перераспределении задания внутри сети СКЦ. Однако в исследованиях [3, 4] не учитывается двухуровневая организация управления заданиями пользователей. Рассмотрен только процесс взаимодействия пользователя с организацией, которая в рамках федерации сети СКЦ не является домашней.

В настоящей работе предложен метод управления заданиям пользователей на основе федеративного подхода организации сети СКЦ. Авторы рассматривают ГСУР как SP в федеративной сети СКЦ.

Актуальные исследования в области федеративной организации сети СКЦ

Для реализации федеративного управления идентификацией используются стандартные протоколы аутентификации и авторизации, такие как OAuth 2.0 (https://datatracker.ietf.org/doc/html/rfc6749), OIDC (https://openid.net/specs/openid-connect-core-1_0.html) или SAML (https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf). Существует достаточно много исследований, посвященных изучению и сравнению этих протоколов, например, работа [5], в которой определен ряд критериев сравнения и дана оценка каждому протоколу по каждому из критериев.

Рассмотрим основные направления исследований в области безопасности федеративного управления идентификацией.

1. *Поиск уязвимостей в различных реализациях протоколов.* В работах [6, 7] проводится сравнение различных реализаций протоколов федеративного управления идентификацией, таких как OAuth/OIDC и SAML. Анализиру-

ются их сильные и слабые стороны, уязвимости и общая безопасность. Например, в [7] исследуется практическая реализация OAuth/OIDC в платформозависимых приложениях из Google Play Store, выявлены типовые нарушения общепринятых рекомендаций.

2. *Моделирование работы протоколов для обнаружения уязвимостей.* В таких исследованиях моделируются различные сценарии использования протоколов для выявления потенциальных уязвимостей. В [8] моделируются потоки авторизации OAuth 2.0 и представляются решения для ослабления известных уязвимостей. В работе [9] авторы предлагают улучшение протокола OAuth 2.0 путем добавления криптографических схем для сохранения конфиденциальности данных пользователя.

3. *Улучшение подотчетности и прозрачности в системах федеративного управления идентификацией*. В работе [10] представлена система TicketT, в [11] – система T-FIM. Оба подхода используют общедоступные журналы для хранения информации о выданных билетах, что позволяет внешним участникам проверять их подлинность, обеспечивая при этом анонимность пользователей.

4. *Внедрение решений по управлению идентификацией на основе блокчейна, позволяющие пользователю взять на себя контроль над своей собственной идентификацией* (самосуверенной идентификацией, *Self-Sovereign Identity* – SSI). Самосуверенная идентификация – возможность пользователя контролировать свою цифровую идентичность. В работе [12] представлен наиболее полный обзор публикаций и предложений на рынке, касающихся применимости решений SSI на базе технологии блокчейн, а также обсуждаются основные компоненты архитектуры, анализируется безопасность, приводится сравнение систем идентификации на основе SSI с FIM и традиционными централизованными системами управления идентификацией.

В [13] авторы предлагают подход к оценке потенциальных атак на систему SSI и рисков безопасности, используя комбинацию модели дерева атак и матрицы рисков для оценки потенциальных атак и рисков безопасности. В работе [14] сравниваются SSI и FIM с точки зрения внешних угроз. Дана классификация 23 общих угроз для систем FIM по семи основным целям. Кроме этого, 20 общих угроз SSI классифицированы аналогично угрозам FIM для облегчения сравнения. Авторы делают вывод, что в целом система SSI менее подвержена атакам, несет меньше рисков и по сравнению с системой FIM не так полно раскрывает пользовательские данные. Исследование проводилось на теоретических моделях FIM и SSI, а не на конкретных реализациях этих подходов.

5. *Аутентификация пользователей СКЦ*. В работе [15] представлен набор программных компонентов, интегрированных для создания масштабируемого, готового к внедрению решения многофакторной аутентификации для систем высокопроизводительных вычислений с большим числом пользователей. Предлагаемое решение протестировано на системе, поддерживающей более 10 000 учетных записей пользователей.

Используемые инструменты и процесс интеграции портала MIT SuperCloud Portal для федеративной аутентификации с федерацией InCommon и инфраструктурой открытых ключей (PKI) правительства США обсуждаются в работе [16]. Авторы рассматривают ПО и методы, необходимые для настройки их системы на прием учетных данных, полученных от этих двух поставщиков идентификационных данных. В работе рассмотрены улучшения в области безопасности и удобства использования, наиболее заметным из которых является возможность использовать надежные системы многофакторной аутентификации, развернутые домашними организациями пользователей. В статье уделено внимание различным методам веб-доступа к суперкомпьютерным мощностям и процессу самостоятельной регистрации и проверки ключей протокола SSH.

Работы по интеграции с системами федеративной аутентификации научных организаций проводились в рамках инфраструктуры XSEDE (США) [17]. В ходе проекта AARC [18] разрабатывались проекты федеративной аутентификации для европейской инфраструктуры суперкомпьютерных приложений PRACE [19].

Актуальные публикации демонстрируют активность исследовательских работ в области создания федераций и протоколов федеративной аутентификации. Однако авторы данной статьи не обнаружили решений, связывающих иерархическое управление заданиями и вычислительными ресурсами в распределенной сети СКЦ с ее федеративной организацией.

Метод управления пользовательскими заданиями и вычислительными ресурсами на основе федеративной организации распределенной сети СКЦ коллективного пользования

Для управления заданиями в иерархически организованной распределенной сети СКЦ пред-

лагается метод, основанный на федеративной аутентификации. Рассмотрим базовые положения метода.

1. В основе метода лежит двухуровневая организация управления в сети СКЦ [1, 2], при которой выделяются глобальный (на уровне сети СКЦ) и локальный (на уровне отдельной ВС из состава сети СКЦ) уровни управления. Для каждой ВС из состава сети выделяется локальная система управления ресурсами, в которой ведется локальная очередь заданий. На уровне распределенной сети глобальной системой управления ресурсами ведется глобальная очередь заданий.

2. Сеть СКЦ объединяет вычислительные системы нескольких СКЦ, связанных коммуникационными каналами. Она характеризуется списком ВС, входящих в ее состав, и общей глобальной очередью заданий. Важно отметить, что сеть имеет децентрализованный характер, поскольку все СКЦ коллективного пользования являются независимыми. Ими владеют и управляют различные научные организации в разных ведомствах. Каждый СКЦ обрабатывает персональные данные тех пользователей, для которых он является домашней организацией, и, таким образом, выступает как провайдер вычислительных ресурсов и одновременно является поставщиком идентификационных данных.

3. Планирование заданий глобальной очереди заключается в их распределении по локальным очередям. Алгоритм распределения может быть произвольным: например, очередное задание может направляться в наименее загруженную локальную очередь. Алгоритм распределения в предлагаемом методе рассматривается в качестве специализированного сервиса, определяющего для каждого задания глобальной очереди ВС, в которой это задание будет выполнено.

4. Представим каждую ЛСУР и соответствующую ей локальную очередь в виде поставщика услуг (SP), глобальную очередь и ГСУР – в качестве отдельного SP. При наличии в составе сети СКЦ N ВС можно ввести следующие обозначения: SP_0 – глобальная очередь заданий, SP_1, SP_2, …, SP_N – локальные очереди. Пользователь имеет возможность обратиться к любому поставщику услуг из множества { SP_0, SP_1, …, SP_N}. Задание, поступившее в локальную очередь SP_i, может быть выполнено только на ресурсах *i*-й ВС. Задание, поступившее в глобальную очередь SP_0, может быть выполнено на любой ВС из состава сети СКЦ или на их заданном подмножестве.

5. Введем понятие глобального прокси-IdP, который выступает в качестве брокера федерации, функционируя и как IdP, и как SP. Прокси-IdP позволяет упростить дальнейшую интеграцию новых ВС в сеть СКЦ и предоставляет общий интерфейс для аутентификации на глобальной очереди (рис. 1).

6. Примем следующий общий порядок распределения заданий глобальной очереди.

6.1. Пользователь проходит идентификацию, аутентификацию и авторизацию в одном из СКЦ распределенной сети.

6.2. Авторизованный пользователь направляет задание в глобальную очередь SP_0 как информационный объект.

6.3. Задание, прошедшее глобальную очередь и распределенное в некую локальную очередь SP_i, преобразуется из объекта в субъект и авторизуется в *i*-й ВС.

Рассмотрим положения предлагаемого метода более подробно. Отметим, что в контексте организации сети СКЦ каждая ВС имеет уникальное имя в рамках СКЦ и собственную локальную очередь пользовательских заданий. Каждый СКЦ включает одну или несколько ВС с различными именами и характеризуется

– уникальным именем;

– организационной принадлежностью и территориальным расположением;

– списком ВС, входящих в его состав;

– отдельной системой хранения данных, содержащей проектные каталоги, исходные данные и результаты расчетов всех пользователей;

– отдельной системой авторизации пользователей, хранящей учетные записи всех пользователей СКЦ.

Попытаемся сохранить иерархическую архитектуру сети, однако глобальную очередь рассматриваем как поставщика услуг в рамках федерации. СКЦ будут рассмотрены как поставщики вычислительных ресурсов (поставщики услуг) и поставщики идентификационных данных пользователей, для которых они являются домашними организациями. Другими словами, каждый СКЦ должен предоставлять идентификационные данные пользователей через собственный IdP, поддерживающий стандартный протокол идентификации SAML,

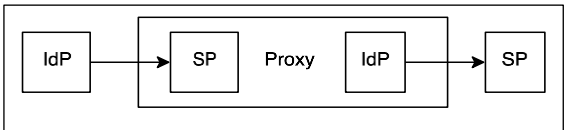

Рис. 1. Прокси-IdP

Fig. 1. IdP proxy

соответствующий определенному набору атрибутов (рис. 2).

Следует отметить, что можно обойтись и без прокси-IdP, однако тогда осложняется интеграция СКЦ в федерацию. Каждый СКЦ будет обязан синхронизировать свои метаданные с другим СКЦ и договариваться о формате передачи данных (рис. 3). Поскольку в данном случае федерация статическая, то есть создана на уровне администратора и связана юридическим договором с использованием определенного набора административных процедур, процесс интеграции нового СКЦ в федерацию будет занимать продолжительное время.

Использование прокси-IdP позволяет СКЦ синхронизировать метаданные только с глобальным прокси-IdP. Введение прокси-IdP дает возможность определить набор необходимых атрибутов, который должны передавать провайдеры каждого СКЦ. Прокси-IdP может сам приводить атрибуты к общему формату или дополнять их (например, для авторизации) и передавать поставщику вычислительных ресурсов. Подобная организация федерации значительно упрощает процесс интеграции в нее новых СКЦ (рис. 4). Однако у такого решения есть очевидный минус – появляется точка централизации.

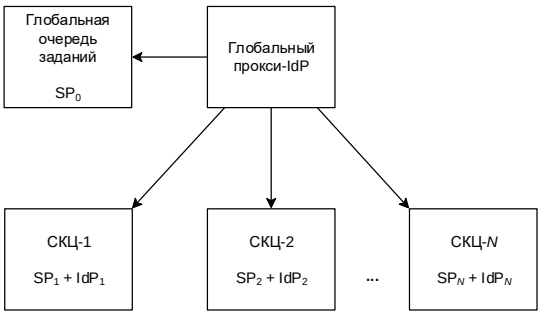

Рис. 2. Общая схема федерации СКЦ

Fig. 2. General scheme of SCC federation

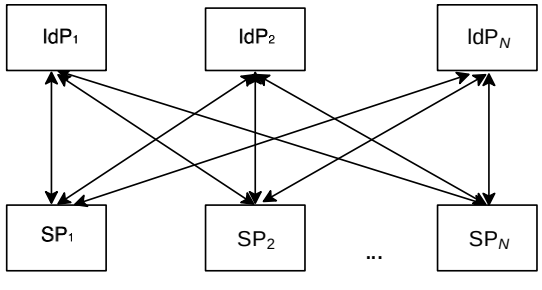

Рис. 3. Организация федерации без прокси-IdP

Fig. 3. Federation without IdP proxy

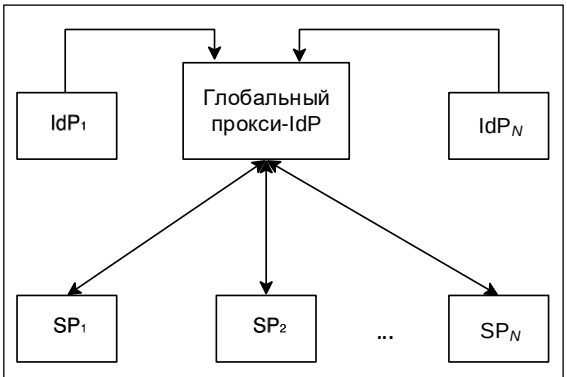

Рис. 4. Организация федерации с прокси-IdP

Fig. 4. Federation with IdP proxy

Порядок функционирования глобальной системы управления заданиями и вычислительными ресурсами распределенной сети СКЦ

Управление заданиями и вычислительными ресурсами основано на обращении пользователя для постановки задания в глобальную очередь и последующей авторизации задания в ЛСУР (рис. 5). Сама организация глобальной очереди инвариантна и рассматривается авторами как специализированный сервис в виде некоторого черного ящика. Пример одной из возможных схем организации глобальной очереди приведен в работе [2].

Глобальная очередь должна также предоставлять пользователю удобный интерфейс для управления и мониторинга заданий в очереди, то есть позволять

– добавлять новые глобальные задания;

– отслеживать состояния глобальных заданий;

– получать результаты выполнения глобальных заданий;

– просматривать конфигурацию сети СКЦ;

– проверять конфигурацию пользовательских настроек.

Добавление СКЦ (ВС) в состав сети СКЦ и удаление СКЦ (ВС) из состава сети осуществляются администраторами СКЦ и администраторами глобальной очереди путем синхронизации метаданных.

Задание может иметь один из статусов:

– «в глобальной очереди» – задание находится в глобальной очереди, ожидает распределения в ВС какого-либо СКЦ сети;

– «в локальной очереди СКЦ *X*» – задание ожидает в локальной очереди освобождения ресурсов ВС;

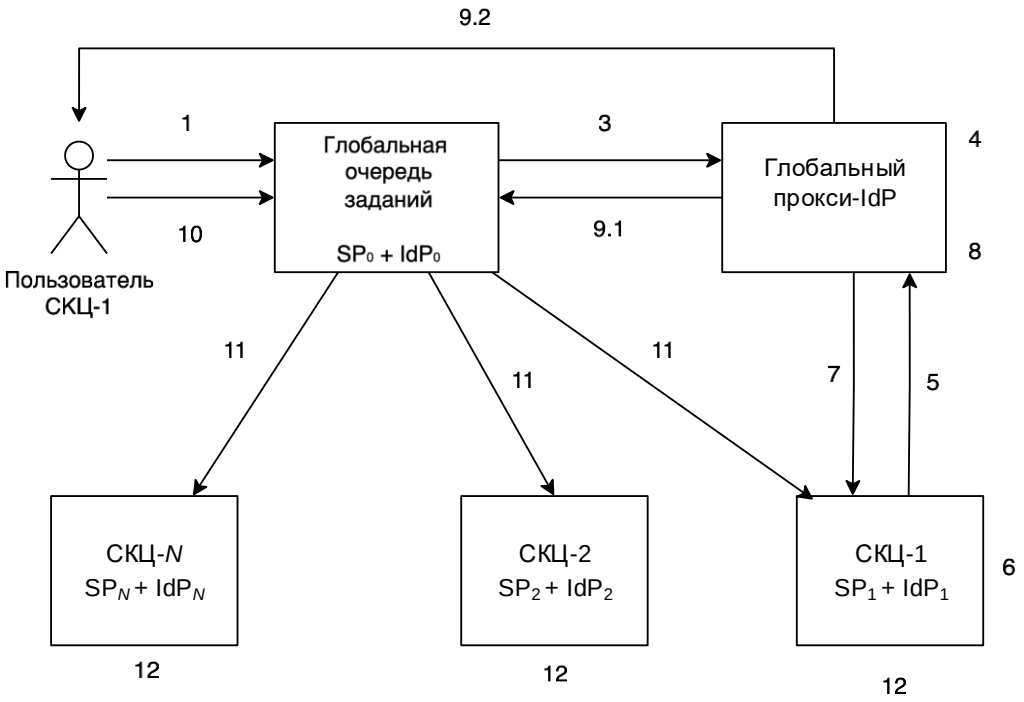

Рис. 5. Порядок обращения пользователя в глобальную очередь

Fig. 5. User access to the global queue

– «выполняется» – задание выполняется на вычислительных ресурсах;

– «завершено» – задание выполнилось и освободило ресурсы;

– «ошибка выполнения» – произошла ошибка на любом из этапов обработки задания.

Рассмотрим порядок обращения пользователя к глобальной очереди (рис. 5).

1. Пользователь СКЦ-1 пытается получить доступ к глобальной очереди заданий.

2. Пользователь выбирает глобальный прокси-IdP в качестве поставщика идентификационных данных.

3. Перенаправление на глобальный прокси-IdP.

4. Пользователь выбирает СКЦ-1 как IdP_1.

5. Перенаправление на IdP_1.

6. Аутентификация.

7. Передача атрибутов глобальному прокси-IdP.

8. Пользователь дает разрешение на передачу атрибутов глобальному прокси-IdP.

9.1. Передача утверждения от прокси-IdP SP_0 глобальной очереди.

9.2. Передача ссылки на утверждение пользователю.

10. Получение доступа к глобальной очереди, постановка задания в глобальную очередь.

11. Передача задания в ЛСУР одного из СКЦ и утверждения от IdP_0 глобальной очереди.

12. Проверка уровня доверия к процессу аутентификации утверждения SP_x СКЦ *X*.

12.1. Если уровень доверия к процессу аутентификации соответствует политике СКЦ *X*, то авторизация задания и предоставление доступа к ЛСУР, уведомление пользователя о постановке задания в локальной очереди СКЦ *X*.

12.2. Если уровень доверия к процессу аутентификации не соответствует политике СКЦ *X*, то отказ в доступе к ЛСУР, уведомление пользователя с требованием повторного прохождения процедуры аутентификации с соответствующим уровнем доверия, например, с помощью двухфакторной аутентификации.

Присоединение СКЦ к сети не должно сказываться на его локальных пользователях. Соответственно, при распределении нового задания из глобальной очереди должны соблюдаться ограничения, установленные администратором СКЦ, например, по числу глобальных заданий в локальной очереди или требуемых ресурсов для глобального задания. Администратор СКЦ также может выделить отдельный раздел ВС для обработки заданий из ГСУР.

Присоединение СКЦ к сети СКЦ не сказывается на процессе получения доступа пользо-

вателей к вычислительным ресурсам домашней организации. Пользователи могут подключаться к ЛСУР напрямую, например, по SSH. При этом появится возможность подключения к ЛСУР с помощью глобального IdP через SSH-соединение, например, как рассмотрено в [4]. Отметим, что существуют и другие решения, в частности, предложенные в [20].

Процесс получения пользователем доступа к ЛСУР посредством глобального прокси-IdP аналогичен процессу доступа к глобальной очереди (рис. 6).

1. Пользователь СКЦ-2 пытается получить доступ к ресурсам СКЦ-1.
2. Пользователь выбирает глобальный прокси-IdP как поставщика идентификационных данных.
3. Перенаправление на глобальный прокси-IdP.
4. Пользователь выбирает СКЦ-2 как IdP.
5. Перенаправление на IdP_2.
6. Аутентификация.
7. Передача атрибутов глобальному прокси-IdP.
8. Пользователь дает разрешение на передачу атрибутов глобальному прокси-IdP.
9. Предоставление доступа, пользователь может ставить задания в локальную очередь СКЦ-1.

Безопасность данных пользователей при федеративной организации распределенной сети

Современный характер научных исследований, основанный на кооперации ученых, обусловил создание интегрированных исследовательских инфраструктур, например, сети СКЦ. Подобные инфраструктуры имеют распределенный характер и охватывают несколько административных доменов. Инфраструктуры выступают в качестве поставщиков услуг, предоставляемых независимыми организациями. Эти организации должны работать согласованно, обмениваться данными между собой, чтобы предоставлять услуги общим пользователям. Для этого необходимо хранить, обрабатывать и передавать внутри инфраструктуры персональные данные пользователей. Чтобы обеспечить конфиденциальность персональных данных, а также соблюдение регуляторных требований, передаваемые и обрабатываемые данные должны быть соответствующим образом защищены. Соответственно, необходимо разработать политику не только предоставления атрибутов поставщиками идентификационных данных поставщикам услуг, но и обработки предоставленных персональных данных. Эти вопросы довольно сложны и выходят за рамки статьи, в работе рассматриваются лишь общие риски безопасности информации в объединенной распределенной инфраструктуре.

Здесь и далее под данными будут подразумеваться только те, которые необходимы для учета, мониторинга и взаимодействия, но не исследовательские наборы данных, порой содержащие конфиденциальную информацию. Кроме этого, не планируется подробно исследовать вопрос раскрытия атрибутов пользователя (данных, передаваемых от поставщика идентификационных данных поставщику услуг), а рассмотрены лишь ситуации, когда атрибуты

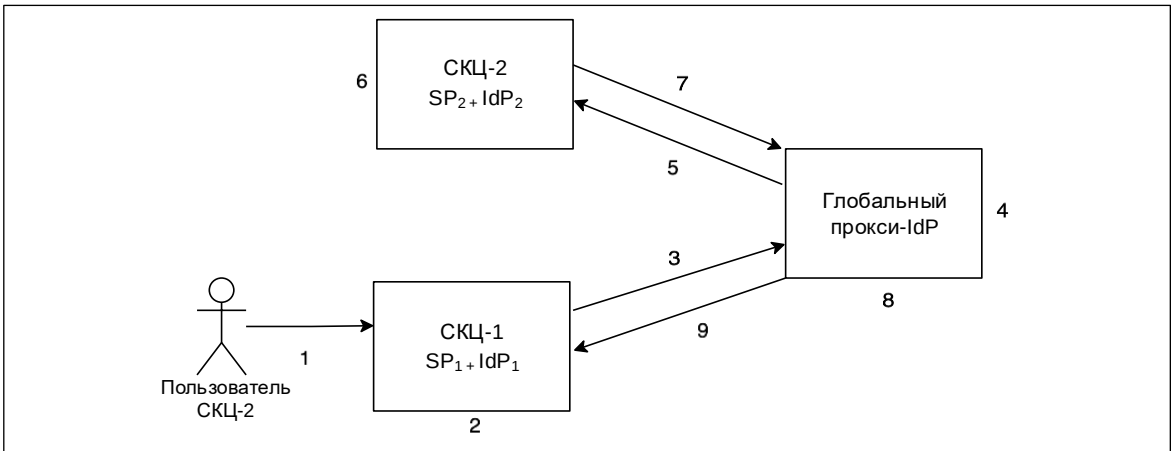

Рис. 6. Порядок обращения пользователя непосредственно в СКЦ с использованием глобального IdP

Fig. 6. The procedure for a direct user access to SCC using a global IdP

передаются с целью учета, мониторинга и организации взаимодействия.

В стандарте X.1250 федерация определяется как ассоциация, объединяющая любое количество поставщиков услуг и поставщиков идентификационных данных. Тот факт, что различные поставщики сформировали ассоциацию, означает, что они должны иметь определенный уровень доверия, достаточный для обмена сообщениями друг с другом. Когда эти сообщения содержат данные аутентификации и авторизации пользователей, позволяющие пользователям иметь доступ к ресурсам объединенной инфраструктуры, получается федеративное управление идентификацией. Федерация позволяет IdP предоставлять атрибуты аутентификации и (необязательно) атрибуты авторизации нескольким отдельно управляемым поставщикам услуг с помощью протоколов и утверждений федерации. Аналогично поставщики услуг могут использовать более одного поставщика идентификационных данных в качестве источников идентификационных данных. В FIM пользователь может использовать свои учетные данные от одного или нескольких поставщиков идентификационных данных для получения доступа к другим поставщикам услуг в рамках федерации. Другими словами, некоторый SP принимает утверждение, предоставленное некоторым IdP, и использует его для принятия решения об аутентификации и авторизации исходя из доверия к федерации, процессу регистрации и текущему событию аутентификации.

Федеративное управление позволяет минимизировать объем передаваемых атрибутов пользователя, что обеспечивает лучшую защищенность данных по сравнению с традиционными методами. Это достигается техническими методами (могут запрашиваться конкретные атрибуты пользователя) или политикой, которая будет определять категории передаваемых атрибутов, например, только электронная почта организации и логин пользователя. У федерации есть еще одно существенное преимущество: учетные данные пользователей (пароли, ключи доступа) хранятся в одном месте (в домашней организации пользователя), что способствует ограничению распространения информации между организациями.

При оценке рисков подразумеваются риски для пользователей (или субъектов данных), получающих доступ к ресурсам и использующих их. Хотя эти риски отличаются от рисков поставщиков услуг, их можно рассматривать вместе в ситуациях, когда риски одного из них влияют на другого. Например, при проникновении в сервисы может произойти утечка данных, содержащих личную информацию пользователей.

Информация о пользователях раскрывается только при доступе к некоторому сервису, причем лишь та информация, которая требуется этому сервису. В работе [4] рассмотрены соответствующие необходимые атрибуты. Такой сценарий выгоден всем участникам федерации, в том числе организациям, предоставляющим услуги, поскольку он обеспечивает гарантии в отношении информации о пользователях и позволяет поставщикам услуг идентифицировать пользователя и взаимодействовать с ним. В схеме также участвуют доверенные третьи стороны для посредничества между домашней организацией пользователя и поставщиком услуг либо для передачи дополнительных атрибутов. Все это способствует ограничению распространения информации о пользователях.

Дополнительные данные, которые обычно могут быть собраны, – это данные о подключении, такие как IP-адреса, журналы событий и др. Они, хотя и остаются персональными, не являются конфиденциальными. Нет оснований утверждать, что из-за распределенного характера инфраструктуры возрастет уровень угрозы по сравнению с традиционным подходом, например, при сценарии, где один СКЦ столкнется с утечкой пользовательских данных. Во-первых, не все пользователи получают доступ к распределенной инфраструктуре, а во-вторых, последствия все равно будут менее значительными, чем при сценарии, когда глобальный поставщик услуг сталкивается с утечкой данных. Следует учитывать склонность пользователей к повторному применению учетных данных на разных сервисах, что делает федеративный подход более предпочтительным, а последствия утечки данных одного поставщика услуг менее серьезными.

Таким образом, с точки зрения рисков безопасности рассматриваемый метод управления заданиями в распределенной сети СКЦ является более безопасным и предпочтительным для защиты информации, в том числе персональных данных пользователей.

Заключение

В статье предложен метод управления пользовательскими заданиями в распределенной сети СКЦ коллективного пользования. Метод

основан на применении двухуровневой схемы управления в сочетании с федеративной организацией распределенной сети СКЦ. Двухуровневая иерархия подразумевает наличие уровня глобальной очереди заданий, из которой задания распределяются в локальные очереди ВС из состава сети СКЦ. Предлагаемый метод учитывает то, что за время нахождения в глобальной очереди задание с точки зрения безопасности превращается из объекта в субъект, который заново должен быть авторизован в локальной очереди суперкомпьютера. Сущность метода заключается в том, что глобальная очередь заданий рассматривается как еще один член федерации. Глобальная очередь выступает в качестве поставщика услуг для пользователей федерации и одновременно является поставщиком идентификационных данных для авторизации заданий, распределяемых в локальные очереди СКЦ. Рассмотренные в статье сценарии применения метода показывают, что он позволяет повысить надежность и безопасность обрабатываемых данных, в том числе персональных данных пользователей.

Список литературы

1. Шабанов Б.М., Овсянников А.П., Баранов А.В., Лещев С.А., Долгов Б.В., Дербышев Д.Ю. Проект распределенной сети суперкомпьютерных центров коллективного пользования // Программные системы: теория и приложения. 2017. № 4. С. 245–262. doi: 10.25209/2079-3316-2017-8-4-245-262.

2. Шабанов Б.М., Телегин П.Н., Овсянников А.П., Баранов А.В., Тихомиров А.И., Ляховец Д.С. Система управления заданиями распределенной сети суперкомпьютерных центров коллективного пользования // Тр. НИИСИ РАН. 2018. Т. 8. № 6. С. 65–73.

3. Баранов А.В., Овсянников А.П., Шабанов Б.М. Федеративная аутентификация в распределенной инфраструктуре суперкомпьютерных центров // Тр. НИИСИ РАН. 2018. Т. 8. № 6. С. 79–83.

4. Гончар А.А., Морин Ю.Н., Овсянников А.П. Некоторые вопросы федеративной аутентификации в распределенной сети суперкомпьютерных центров // Тр. НИИСИ РАН. 2020. Т. 10. № 5-6. С. 13–20.

5. Naik N., Jenkins P. Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID Connect. Proc. Int. Conf. RCIS, 2017, pp. 163–174. doi: 10.1109/RCIS.2017.7956534.

6. Aldosary M., Norah A. A survey on federated identity management systems limitation and solutions. IJNSA, 2021, vol. 13, no. 3, pp. 43–59.

7. Sharif A., Carbone R., Sciarretta G., Ranise S. Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients. JISA, 2022, vol. 65, art. 103097. doi: 10.1016/j.jisa.2021.103097.

8. Singh J., Chaudhary N. OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities. JISA, 2022, vol. 65, 103091. doi: 10.1016/j.jisa.2021.103091.

9. Sucasas V., Mantas G., Althunibat S., Oliveira L., Antonopoulos A., Otung I., Rodriguez J. A privacy-enhanced OAuth 2.0 based protocol for Smart City mobile applications. Computers & Security, 2018, vol. 74, no. C, pp. 258–274. doi: 10.1016/j.cose.2018.01.014.

10. Chu D., Lin J., Li F., Zhang X., Wang Q., Liu G. Ticket transparency: Accountable single sign-on with privacy-preserving public logs. In: LNICST. Proc. SecureComm, 2019, vol. 304, pp. 511–531. doi: 10.1007/978-3-030-37228-6_25.

11. Xu B., Zhang Z., Sun A. et al. T-FIM: Transparency in federated identity management for decentralized trust and forensics investigation. Electronics, 2023, vol. 12, no. 17, art. 3591. doi: 10.3390/electronics12173591.

12. Ahmed M.R., Islam A.M., Shatabda S., Islam S. Blockchain-based identity management system and self-sovereign identity ecosystem: a comprehensive survey. IEEE Access, 2022, vol. 10, pp. 113436–113481. doi: 10.1109/ACCESS.2022.3216643.

13. Naik N., Grace P., Jenkins P., Naik K., Song J. An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity. Computers & Security, 2022, vol. 120, art. 102808. doi: 10.1016/j.cose.2022.102808.

14. Le A., Epiphaniou G., Maple C. A comparative cyber risk analysis between federated and self-sovereign identity management systems. Data & Policy, 2023, vol. 5, art. e38. doi: 10.1017/dap.2023.41.

15. Cyrus W.C., Storm P., Hanlon M.R., Mendoza N. Securing HPC: Development of a low cost, open source multi-factor authentication infrastructure. Proc. Int. Conf. SC, 2017, art. 37. doi: 10.1145/3126908.3126957.

16. Prout A., Klein A., Michaleas P. et al. Securing HPC using Federated Authentication. Proc. IEEE HPEC, 2019, pp. 1–7. doi: 10.1109/HPEC.2019.8916255.

17. Towns J., Cockerill T., Dahan M. et al. XSEDE: Accelerating scientific discovery. Computing in Science & Engineering, 2014, vol. 16, no. 5, pp. 62–74. doi: 10.1109/MCSE.2014.80.

18. Liampotis N. AARC Blueprint Architecture. AARC, 2019, no. AARC-G045, pp. 1–12. URL: https://core.ac.uk/download/pdf/289271206.pdf (дата обращения: 10.08.2024).

19. Oorsprong M., O'Neill H. PRACE Annual Report 2022. PRACE, 2022, pp. 1–42. URL: https://insightm.co.uk/wp-content/uploads/2023/06/PRACE_AP_22_Single_Hi_res.pdf (дата обращения: 24.07.2024).

20. Simmel D., Filus S. Flexible enforcement of multi factor authentication with SSH via Linux-PAM for federated identity users. Proc. PEARC, 2017, no. 10, pp. 1–9. doi: 10.1145/3093338.3093392.

Software & Systems doi: 10.15827/0236-235X.148.461-471 2024, 37(4), pp. 461–471

The user job managing in a HPC network using federated authentication

Anton V. Baranov [1, 2]✉, Egor E. Kuznetsov [2]

[1] Joint Supercomputer Center of RAS, Moscow, 119334, Russian Federation
[2] National Research Centre "Kurchatov Institute",
Moscow, 123182, Russian Federation

For citation
Baranov, A.V., Kuznetsov, E.E. (2024) 'The user job managing in a HPC network using federated authentication', *Software & Systems*, 37(4), pp. 461–471 (in Russ.). doi: 10.15827/0236-235X.148.461-471
Article info
Received: 20.07.2024 After revision: 22.08.2024 Accepted: 30.08.2024

Abstract. The paper presents a research on user task management in a distributed network of scientific HPC centers. The HPC network unites supercomputers of different architecture belonging to different centers. Each center independently determines its own security policy and maintains its own user accounting database. This complicates the management of user jobs; in particular, it complicates the operational job redistribution between supercomputers of different centers. The authors base their research methodology on combining two-level hierarchical job management and federated identity management, in particular federated authentication. The paper proposes a new method for managing user jobs in a distributed HPC network based on federated authentication. The upper level of the management hierarchy is a global job queue; the global queue jobs are distributed to the supercomputers of the distributed HPC network. The local queues of these supercomputers form the lower level of the job management hierarchy. Each job should be authenticated and authorized twice: when it is placed in the global queue and when it is allocated to a local queue. The proposed method takes into account that a job, when being in the global queue, from the point of view of information security, turns from an object into a subject, which must be authorized again in a local queue. The paper shows that the application of federated authentication in authorization of users and their jobs allows building a simple and secure scheme of job management in the HPC network. The practical significance of the research is the operation of the job management system in the distributed HPC network and the security analysis of such solution.

Keywords: SCC, task management, federated authentication, job queue, service provider, identification provider
Acknowledgements. The paper was carried out under the government assignment, project no. FNEF-2024-0014

References

1. Shabanov, B.M., Ovsiannikov, A.P., Baranov, A.V., Leshchev, S.A., Dolgov, B.V., Derbyshev, D.Yu. (2017) 'The distributed network of the supercomputer centers for collaborative research', *Program Systems: Theory and Applications*, (4), pp. 245–262 (in Russ.). doi: 10.25209/2079-3316-2017-8-4-245-262.
2. Shabanov, B.M, Telegin, P.N., Ovsiannikov, A.P., Baranov, A.V., Tikhomirov, A.I., Lyakhovets, D.S. (2018) 'Task management system for a distributed network of supercomputer centres for collective use', *Proc. of NIISI RAS*, 8(6), pp. 65–73 (in Russ.).
3. Baranov, A.V., Ovsiannikov, A.P., Shabanov, B.M. (2018) 'Federated authentication in distributed infrastructure of supercomputer centres', *Proc. of NIISI RAS*, 8(6), pp. 79–83 (in Russ.).
4. Gonchar, A.A., Morin, Yu.N., Ovsiannikov, A.P. (2020) 'Some issues of federated authentication in a distributed network of supercomputer centres', *Proc. of NIISI RAS*, 10(5-6), pp. 13–20 (in Russ.).
5. Naik, N., Jenkins, P. (2017) 'Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID Connect', *Proc. Int. Conf. RCIS*, pp. 163–174. doi: 10.1109/RCIS.2017.7956534.
6. Aldosary, M., Norah, A. (2021) 'A survey on federated identity management systems limitation and solutions', *IJNSA*, 13(3), pp. 43–59.
7. Sharif, A., Carbone, R., Sciarretta, G., Ranise, S. (2022) 'Best current practices for OAuth/OIDC Native Apps: A study of their adoption in popular providers and top-ranked Android clients', *JISA*, 65, art. 103097. doi: 10.1016/j.jisa.2021.103097.
8. Singh, J., Chaudhary, N. (2022) 'OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities', *JISA*, 65, art. 103091. doi: 10.1016/j.jisa.2021.103091.
9. Sucasas, V., Mantas, G., Althunibat, S., Oliveira, L., Antonopoulos, A., Otung, I., Rodriguez, J. (2018) 'A privacy-enhanced OAuth 2.0 based protocol for Smart City mobile applications', *Computers & Security*, 74(C), pp. 258–274. doi: 10.1016/j.cose.2018.01.014.
10. Chu, D., Lin, J., Li, F., Zhang, X., Wang, Q., Liu, G. (2019) 'Ticket transparency: Accountable single sign-on with privacy-preserving public logs', in *LNICST. Proc. SecureComm*, pp. 511–531. doi: 10.1007/978-3-030-37228-6_25.
11. Xu, B., Zhang, Z., Sun, A. et al. (2023) 'T-FIM: transparency in federated identity management for decentralized trust and forensics investigation', *Electronics*, 12(17), art. 3591. doi: 10.3390/electronics12173591.
12. Ahmed, M.R., Islam, A.M., Shatabda, S., Islam, S. (2022) 'Blockchain-based identity management system and self-sovereign identity ecosystem: a comprehensive survey', *IEEE Access*, 10, pp. 113436–113481. doi: 10.1109/ACCESS.2022.3216643.
13. Naik, N., Grace, P., Jenkins, P., Naik, K., Song, J. (2022) 'An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity', *Computers & Security*, 120, art. 102808. doi: 10.1016/j.cose.2022.102808.

14. Le, A., Epiphaniou, G., Maple, C. (2023) 'A comparative cyber risk analysis between federated and self-sovereign identity management systems', *Data & Policy*, 5, art. e38. doi: 10.1017/dap.2023.41.

15. Cyrus, W.C., Storm, P., Hanlon, M.R., Mendoza, N. (2017) 'Securing HPC: Development of a low cost, open source multifactor authentication infrastructure', *Proc. Int. Conf. SC*, art. 37. doi: 10.1145/3126908.3126957.

16. Prout, A., Klein, A., Michaleas, P. et al. (2019) 'Securing HPC using Federated Authentication', *Proc. IEEE HPEC*, pp. 1–7. doi: 10.1109/HPEC.2019.8916255.

17. Towns, J., Cockerill, T., Dahan, M. et al. (2014) 'XSEDE: Accelerating scientific discovery', *Computing in Science & Engineering*, 16(5), pp. 62–74. doi: 10.1109/MCSE.2014.80.

18. Liampotis, N. (2019) 'AARC Blueprint Architecture', *AARC*, (AARC-G045), pp. 1–12, available at: https://core.ac.uk/download/pdf/289271206.pdf (accessed August 10, 2024).

19. Oorsprong, M., O'Neill, H. (2022) 'PRACE Annual Report 2022', *PRACE*, pp. 1–42, available at: https://insightm.co.uk/wp-content/uploads/2023/06/PRACE_AP_22_Single_Hi_res.pdf (accessed July 24, 2024).

20. Simmel, D., Filus, S. (2017) 'Flexible enforcement of multi factor authentication with SSH via Linux-PAM for federated identity users', *Proc. PEARC*, (10), pp. 1–9. doi: 10.1145/3093338.3093392.

Авторы

Баранов Антон Викторович [1, 2], к.т.н., доцент, ведущий научный сотрудник, abaranov@jscc.ru

Кузнецов Егор Евгеньевич [2], инженер-исследователь, egor57k@jscc.ru

[1] Межведомственный суперкомпьютерный центр РАН, г. Москва, 119334, Россия

[2] Национальный исследовательский центр «Курчатовский институт», г. Москва, 123182, Россия

Authors

Anton V. Baranov [1, 2], Cand. of Sci. (Engineering), Associate Professor, Leading Researcher, abaranov@jscc.ru

Egor E. Kuznetsov [2], Engineer-Researcher, egor57k@jscc.ru

[1] Joint Supercomputer Center of RAS, Moscow, 119334, Russian Federation

[2] National Research Centre "Kurchatov Institute", Moscow, 123182, Russian Federation