ivanti

# Новый подход к управлению идентификацией и доступом

# Содержание

# Новый подход в организации доступа

***Подход, основанный на политиках повысит эффективность управления и идентификации***

Переход от традиционной ролевой системы управления идентификацией и доступом (IAM) к более технологичному решению на основе политик может быть трудной задачей. Выбор системы на основе политик, которая выглядит более целостно с точки зрения идентификации, будет более эффективным решением, которое даст больше гибкости и возможностей для ИТ.

Чтобы понять важность комплексной стратегии управления идентификацией и доступом, рассмотрим часто встречающуюся задачу по организации безопасного доступа к ресурсам.
Идентификация и соответствующие права доступа часто организуются на ролевой основе: роль каждого сотрудника ассоциируется с набором определенных ресурсов, затем настраивается система предоставления исключений. После того, как сотрудник был идентифицирован, ему предоставляется доступ – часто либо через громоздкое решение управления идентификацией и доступом, либо с помощью собственных сценариев и автоматизированных процессов. А затем настраиваются запросы на исключения. Они часто обрабатываются службами технической поддержки, что обычно влечет за собой значительные затраты ресурсов на каждый запрос.

## Простое решение вместо скриптов

Во-первых, традиционные решения для управления идентификацией и доступом - это сложные системы, требующие комплексной интеграции и обслуживания. Они дорогие в приобретении и обслуживании, и - пока они выполняют свою работу - приносят новые проблемы в обслуживании для ИТ-персонала.

Во-вторых, подход «напишем для этого скрипт» имеет серьёзные недостатки. Эти решения могут быть неустойчивыми и дорогостоящими. Если внедряется индивидуальный процесс или происходит изменение технологии, сценарии и обработки могут оказаться громоздкими - это означает, что вы можете с высокой долей вероятности получить «доступ отсутствует» и кучу непродуктивных сотрудников вместе с этим.

Решения для идентификации и предоставления доступа независимо от их типа являются критически важными. Без них вы повышается риск утечки конфиденциальной информации, несоответствия стандартам безопасности, что грозит вашей организации финансовыми и репутационными потерями.

Что если современные решения для управления идентификацией и доступом могут быть заменены мощным, автоматизированным, простым в управлении решением, которое легко реализуется и управляется даже в сложных распределенных гибридных инфраструктурах?

Давайте посмотрим, что необходимо для создания безопасного решения по организации доступа, которое справится  с самыми трудными задачами, сделает работников более продуктивными и легко управляется и развертывается.

## Динамичная рабочая среда

Итак, вопрос: сколько рабочих ролей существует в среднем на современном предприятии? А сколько их было 100 лет назад? Найти статистику по этому вопросу может оказаться сложнее, чем вы думаете. Можем ли мы считать, что разнообразие рабочих ролей увеличивается? И это не просто роли, это приложения, ИТ-сервисы и доступ к ПО для офисных и мобильных сотрудников, и это лишь некоторые из растущего списка задач ИТ.

С диверсификацией рабочих ролей потребности в доступе также становятся все более разносторонними. Для сопоставления сервисов и прав доступа для каждого отдельного сотрудника необходимо:

- Политики, которые регулируют, кто и когда должен получить доступ ресурсу
- Вовремя переданная информация, необходимая для обеспечения доступа в соответствии с политикой

Но постойте! Это еще не все. Быстрые темпы развития бизнеса сопровождаются частыми изменениями в рабочей среде и в организации соответствующего доступа. Добавьте к этому некоторые общие бизнес сценарии – слияния, приобретения, подрядчики, сезонная работа и сотрудники - и …. в общем, кажется, что управление доступом это просто, но на самом деле это серьезная и довольно сложная задача для ИТ. К счастью она может быть решена. Итак, давайте начнем рассматривать решения.

## Две различных системы

Давайте рассмотрим два подхода:

- Традиционная ролевая система
- Технологичная система на основе политик

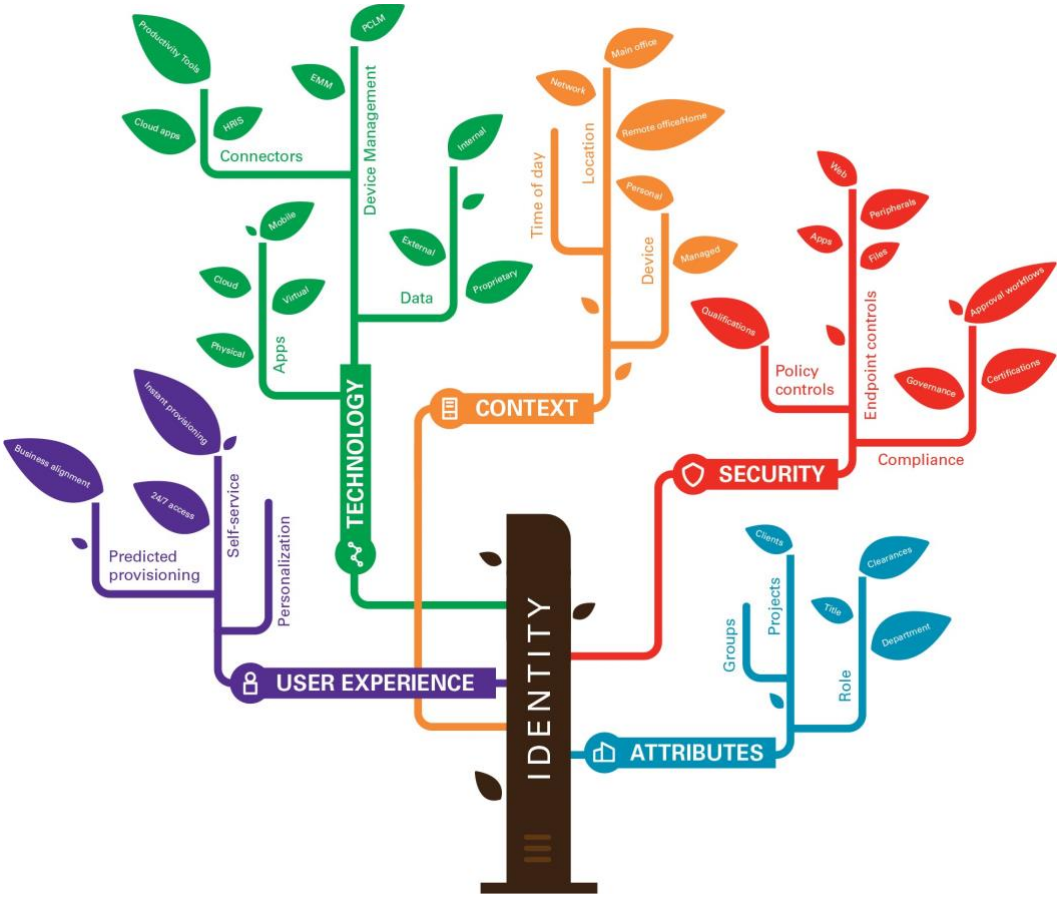
Давайте начнем с традиционной ролевой системы. В ней роль сотрудника определяет его базовые потребности в ресурсах, и основные изменения этой роли запускают соответствующие изменения в доступе. Когда сотрудника принимают на работу, ему обеспечивают доступ к необходимым ресурсам, соответствующим его позиции.

Например, менеджеры по продажам получают лицензии на доступ к CRM, а руководители получают привилегированный доступ к HRIS для просмотра информации о продажах. Спустя какое-то время, сотрудники переходят на новые должности, и в результате их новые рабочие роли требуют доступа к другим ресурсам. А когда их рабочая роль удаляется – например, при увольнении - доступ ко всем ресурсам прекращается.

Эта ролевая система интуитивно понятна, проста и, кажется, довольно надежной и устойчивой. Но действительно ли она отвечает всем требованиям современного мира? Что делать, если сотруднику нужно получить доступ к важной базе данных, когда он работает удалённо – скажем, в холле отеля через публичную сеть Wi-Fi? Или что если сотруднику крайне неудобно использовать корпоративную систему общего доступа к файлам - он заходит в свое личное облачное хранилище для обмена файлами и загружает туда конфиденциальные данные компании? Должно ли это действие быть разрешено или запрещено? В обоих примерах необходимы различные права доступа, но ни в каком из случаев рабочая роль сотрудника не была затронута. Поэтому система организации доступа на основе ролей не привела бы к изменению его прав доступа, хотя это могло быть необходимо в рамках политики безопасности компании.

Альтернативный вариант заключается в гибком решении на основе политик. Вместо того чтобы сосредоточиться на ролях, управление доступом на основе политик фокусируется на определении политик доступа,  который необходим каждому сотруднику в его рабочем контексте. Например, политики могут быть определены требованиями безопасности: никому не предоставлять доступ к конфиденциальной базе данных клиентов, которая содержит номера кредитных карт и другие личные данные, при подключении через общедоступную сеть Wi-Fi. Вместо этого настраивается предупреждение о безопасности при каждой попытке доступа, советующее перейти в защищенную сеть.

Это гораздо более гибкий подход, который предоставляет гораздо больше возможностей для ИТ-специалистов. Но такая система управления доступом также требует огромного объема данных. Чтобы понять, как это работает, давайте рассмотрим модель «древа идентификации»




Наше древо идентификации описывает, какая информация необходима для определения того, какой доступ должен предоставляться каждому человеку в зависимости от его рабочего контекста и множества других факторов. Как видно, это гораздо более комплексный подход, чем доступ на основе ролей. Дерево разбивает информацию о доступе на пять основных категорий:

- **Атрибуты** определяют, кем является сотрудник, и сообщают информацию о его обязанностях, чтобы мы могли понять его потребности в доступе и приложениях. Это похоже на систему ролевого доступа, но здесь намного больше возможностей.
- **Пользовательский опыт** определяет, как обеспечить сотрудника необходимыми сервисами в нужное время. Сотрудники более продуктивны, когда необходимые им ресурсы персонализированы и легко настраиваются.
- **Безопасность** проверяет, какие политики и средства контроля должны быть созданы для защиты сотрудника (или организации от неосторожных или злонамеренных действий сотрудника), а также для сбора информации необходимой для аудита.
- **Контекст** сообщает, находится ли наш сотрудник в безопасной среде, или же он нуждается в дополнительной защите для обеспечения безопасности данных. Мы понимаем, что, когда работник подключен к корпоративной сети в известном месте и использует защищенное устройство, выданное компанией, это безопасная среда. В иных же случаях, автоматически добавляются ограничения.

## Суть подхода

Если у вас есть большой набор данных, как в древе идентификации, это позволит вам наделить каждого сотрудника в нужное время именно теми ресурсами, которые ему необходимы, а также ограничить доступ к ресурсам, которые им не нужны, из соображений стоимости и безопасности.

Из HRIS можно извлечь довольно много идентификационных данных, таких как имя, роль, должность. Но есть и еще. Где сотрудники находятся в момент подключения? В офисе, в безопасной среде? Работают из дома, холла отеля или уличного кафе? Вы не можете за ними постоянно следить, но ваша сеть знает, где они находятся благодаря обнаружению IP. Какое устройство они используют? Личное или корпоративное? Возможно, вы захотите настроить тщательный контроль над действиями при использовании личных USB устройств в корпоративных ноутбуках?

Все эти и другие данные можно легко получить из существующих систем, развернутых в вашей инфраструктуре. Они могут использоваться для определения требований к доступу сотрудника – не только на основе статического списка приложений, данных, но и на основе его рабочего контекста и перемещений.

Представьте, что сотрудник получает доступ к приложению, в котором хранятся конфиденциальные данные. Он безопасно работает в офисе компании, защищенный брандмауэром. Теперь представьте, что он уходит на обед и продолжает пользоваться тем же приложением со своего смартфона через общественную Wi-Fi сеть столовой? Да, это все тот же человек – по крайней мере большинство систем идентификации будут так считать. Но его рабочий контекст теперь сильно отличается, и этой разницы должно быть достаточно для изменений доступа к приложениям и данным на время его обеда.

Разве не должна система идентификации быть достаточно умной, чтобы понять это и отреагировать соответствующим образом? А затем продолжить также динамично управлять доступом на основе реального изменяющегося контекста?

## Новый взгляд на управление идентификацией и доступом

Нет, мы еще не закончили разработку нашего решения для управления идентификацией и доступом. Давайте рассмотрим еще несколько вопросов:

- Сколько ручного труда требует ваш текущий подход к управлению организации доступа?
- Как быстро вы можете адаптироваться к изменениям в рабочем контексте и ролях сотрудников?
- Кто инициирует запросы на предоставление ресурсов и доступа?
- Какие технологии вы используете для идентификации сотрудников? Эффективны ли они?
- Легко ли работать с этими решениями или требуется постоянное обслуживание и корректировка?

Традиционные решения для управления идентификацией и доступом, как известно, громоздки. В результате многие компании решают задачи IAM статическим способом, требуя от кого-то из ИТ-отдела каждый раз точечно вносить изменения в настройки доступа либо вручную, либо путем выполнения сценариев.

В результате этот длительный подверженный ошибкам процесс может подвергнуть вашу компанию серьезному риску. В результате человеческой ошибки могут быть допущены серьезные нарушения безопасности. Например случаи, когда сотрудники, уже покинувшие компанию, все еще имеют доступ к корпоративным ресурсам на протяжении нескольких недель или месяцев.

С этими проблемами можно легко справиться, применив подход на основе политик. Автоматизировав ручной труд, вы сможете точно и последовательно вносить изменения при низких эксплуатационных расходах. Но для этого необходимо правильно организовать рабочие процессы.

Определите рабочие процессы и этапы согласования для каждой задачи – заказа нового устройства или предоставления доступа к новой базе данных – затем автоматизируйте эти процессы таким образом, чтобы их можно было легко отрегулировать по мере изменений потребностей бизнеса.

Цель подхода к IAM основанного на политиках состоит в том, чтобы распознавать и оперативно реагировать на изменения рабочего контекста каждого сотрудника и учитывать эти изменения при управлении доступом. Это позволит вашей инфраструктуре автоматически и незамедлительно предоставлять или аннулировать правила доступа на основе воспринимаемых рисков безопасности, определяемых IP адресом, типом устройства, временем суток и т.д. в момент запроса доступа. И это определенно здорово.

## Продвинутые технологии

Кто инициирует запросы на доступ к новым приложениям, данным, сервисам? Чаще всего, сами сотрудники запускают процесс, отправляя запрос (обычно в службу поддержки). Но что, если этот запрос может быть размещен на портале самообслуживания, а затем автоматически выполнен? В конце концов, сотрудники лучше всех понимают свои собственные потребности. Получив возможность запрашивать ИТ-услуги самостоятельно, сотрудники, как правило, получают ответ на свой запрос гораздо быстрее.

Это также безопасно, если портал самообслуживания работает в связке с решением по организации доступа на основе политик. Политика автоматически определяет, доступ к каким сервисам может иметь каждый сотрудник. Нет никакого риска перерасхода в связи с избыточным обеспечением или предоставления доступа к системам и данным, которые должны быть тщательно защищены. Разрешения на доступ к выбранным сервисам могут быть выданы, как только отправлен запрос. Это происходит автоматически через уведомления, направленные ответственным лицам.

.

Обычные запросы могут быть утверждены и выполнены автоматически с уведомлением, тогда как порядок утверждения других может быть настроен в соответствии с потребностями бизнеса. Помимо быстрого времени отклика, компания получает выгоду от более высокой продуктивности как сотрудников, так и руководителей или ИТ-специалистов, которые смогут сосредоточиться на проектах с более высоким приоритетом вместо выполнения рутинных задач.

## Измените подход к управлению доступом с Ivanti

В то время как многие организации используют традиционную ролевую систему управления идентификацией и доступом (IAM), они могут получить больше, пересмотрев свои подходы. Работая с Ivanti, организации получат следующее:

- Управление доступом станет достаточно «умным», чтобы идентифицировать сотрудника и его рабочий контекст, обеспеченный автоматизированными рабочими процессами и порталом самообслуживания, что увеличит продуктивность ваших сотрудников.
- Организации смогут автоматизировать предоставление ресурсов, основываясь на политиках, а управление доступом будет определяться динамическим взаимодействием между ИТ и остальными отделами.

С Ivanti организации смогут воплотить в жизнь этот уникальный подход к управлению доступом, который комплексно обрабатывает идентификацию сотрудника и применяет соответствующую политику.

**www.ivanti.com**

**1.800.982.2130**

**sales@ivanti.com**