

Документ для руководителя

БЕЗОПАСНОСТЬ И ЭЛЕКТРОННЫЕ ПЕРСОНЫ

www.novell.com

Novell Access Manager

Комплексное решение для управления доступом на предприятии

Novell

Простой и безопасный доступ к сетевым ресурсам

Бизнес-стимул 1: Экономия

Novell Access Manager помогает уменьшить расходы на эксплуатацию, повысить производительность труда и рационализировать цепочку поставок.

- Предоставляет единую, безопасную точку входа, одинаково удобную и для сотрудников, и для партнеров предприятия
- Снимает проблемы обеспечения безопасности для удаленных рабочих мест
- Устраняет зависимость от поставщика и снижает расходы на модернизацию

Бизнес-стимул 2:

Соблюдение нормативов

Приводит в соответствие бизнес-процессы, средства ИТ-контроля и отчетности для соблюдения отраслевых нормативов и стандартов.

- Обеспечивает и контролирует доступ к конфиденциальным данным в зависимости от роли пользователя в организации
- Поддерживает развитые средства аутентификации
- Автоматически предоставляет отчетность о доступе к данным с указанием всех пользователей и времени обращения

Корпоративные сети с каждым днем становятся все сложнее, по мере того как организации добавляют новые приложения, компоненты инфраструктуры и пользователей. В то же время современные сети выходят за традиционные границы предприятия, так как пользователям все чаще требуются возможности удаленной работы в защищенной среде. Для снижения расходов и сохранения конкурентоспособности организациям необходимо упростить свои сети. А именно, им требуется решение, которое защитит ИТ-инфраструктуру от исходящих из интернета угроз; обеспечит приватность пользователей в офисе, дома и в дороге; предоставит простой и безопасный доступ к сети сотрудникам и доверенным партнерам и гарантирует соблюдение бизнес-правил и государственных нормативов. Причем все это решение должно делать, поддерживая максимальную эффективность работы.

Способно ли одно решение справиться со всеми этими сложными, многоуровневыми проблемами? Только Novell® Access Manager в состоянии решить эту задачу. Он позволяет предприятиям интегрировать, автоматизировать и обеспечить безопасный доступ к сетевым ресурсам для заказчиков, партнеров и сотрудников. Благодаря Novell Access Manager системные администраторы могут контролировать доступ к веб- и традиционным бизнес-приложениям. Пользователи сети могут конфиденциально и безопасно вести дела через интернет. И в каждом случае пользователи не являются абсолютными незнакомцами. Доступ авторизован в зависимости от их роли в организации или отношения к ней. Более того, доступ может быть упрощен, и сеть при этом останется в безопасности — хотя организация сократит расходы, гарантирует соблюдение требований регулирующих органов и получит повышенный уровень контроля.

Проблемы доступа к сети

Современные ИТ-менеджеры сталкиваются со сложнейшими проблемами. Они испытывают постоянное давление к более эффективному использованию ресурсов, совершенствованию процесса доступа к сети для авторизованных пользователей, повышению безопасности, соблюдению правил и нормативов — и все это при снижении расходов. Но чтобы добиться всего этого, необходимо решить наиболее проблемные.

Управление доступом

Novell Access Manager обеспечивает управление доступом к сетевому контенту, приложениям и службам посредством широкого спектра платформ и служб каталога. Он делает это при помощи компонентов, основанных на ведущих отраслевых стандартах, включая Liberty Alliance, Web Services Security (WS-Security) и Security Assertions Markup Language (SAML). Беспрепятственная интеграция компонентов Novell Access Manager через HTTP- и не-HTTP среды обеспечивает безопасный доступ для сотрудников, партнеров и заказчиков в любое время и в любом месте. А благодаря единой точке входа через веб даже удаленные и мобильные пользователи могут обращаться ко всем службам в соответствии с правами доступа, которыми они наделены, исходя из роли этих людей в организации.

С точки зрения конечного пользователя Novell Access Manager — это удобство. Он предоставляет единую точку входа через веб, которая обеспечивает беспрепятственный доступ ко всем авторизованным внутренним и внешним службам. Чтобы обеспечить точное соблюдение правил, каждый из федеративных источников информации о профилях пользователей опирается на Access Manager. Он предоставляет такие им же права, как если бы они напрямую обращались в соответствующие системы. И для всех пользователей Novell Access Manager обеспечивает полную защиту от любых попыток нарушить работу или ИТ-инфраструктуру из интернета.

Управление паролями

Забытые пароли снабжают работой персонал служб технической поддержки во всем мире. Как и следовало ожидать, существует прямая связь между количеством паролей, которыми пользователям приходится манипулировать, и числом обращений в службу технической помощи. Но еще важнее связь между количеством паролей и вероятностью того, что один из них будет украден.

Внедрив инструмент единой точки входа, организация может усовершенствовать всю неэффективную систему и повысить продуктивность работы своего персонала технической помощи. Такой инструмент помог бы идентифицировать пользователей, автоматически прослеживая пароли и делая соблюдение нормативов менее трудоемким и дорогостоящим. Единая точка входа служит фундаментом для эффективного управления паролями; она использует электронные персоны для предоставления авторизованным внутренним и внешним пользователям безопасного доступа к ресурсам.

Благодаря Novell Access Manager ваша организация может внедрить стандартизованную единую точку входа через веб, а это означает, что ваши сотрудники, партнеры и заказчики должны будут помнить всего один пароль или способ регистрации для положенного им доступа ко всем корпоративным и веб-приложениям. Это означает гораздо меньшее число обращений в службу технической помощи — и меньшую вероятность того, что пользователи будут прибегать к опасной записи паролей на бумажках.

Упрощая работу с паролями и управление ими, Novell Access Manager помогает вашей организации облегчить жизнь пользователям, повысить безопасность, рационализировать бизнес-процессы и снизить расходы на администрирование и поддержку системы.

Соблюдение нормативных требований

Законы всегда будут прибавлять работы, но оперативная, автоматизированная инфраструктура может существенно уменьшить расходы и трудозатраты, связанные с их соблюдением. Внедряя инструменты сетевого доступа на базе электронных персон, ваше предприятие

сможет защитить приватность пользователей и конфиденциальную информацию. В то же время вы сможете уменьшить количество бумажной работы, необходимой для гарантированного применения надлежащих мер управления доступом. Гарантия соблюдения нормативных требований — это неотъемлемое преимущество Novell Access Manager.

В частности, Novell Access Manager поможет вам не нарушать законы Sarbanes-Oxley, HIPAA, законы о неприкосновенности частной жизни Европейской Комиссии и другие нормативные акты — и вы увидите, как легко будет их соблюдать. Novell Access Manager в любой момент составит необходимые отчеты для внутренней оценки или для внешней проверки. Благодаря своей мощной функциональности и простому в применении интерфейсу Novell Access Manager сможет превратить требования соблюдения нормативов в возможности по развитию и реализации процессов, улучшающих работу.

Соблюдение бизнес-правил

Суть управления электронными персонами: предоставить пользователям безопасный доступ к нужным ИТ-ресурсам в соответствии с их отношением к организации и ролью в ней. Ведь вы не хотите, чтобы сотрудники, не имеющие отношения к бухгалтерии, получили доступ к сведениям о заработной плате, а некоторую интеллектуальную собственность нельзя доверить даже партнеру. Систематически организуемые электронные персоны позволяют компании гарантировать соблюдение правил, защищая как ценную информацию, так и ИТ-инфраструктуру. Благодаря Novell Access Manager ваш ИТ-персонал получает инструменты, необходимые для простого предоставления безопасного доступа к приложениям, установленным на серверах. Вы устанавливаете правила, по которым пользователи получают доступ, а Novell Access Manager гарантирует соблюдение этих правил. А для веб-приложений вы можете задать требования по аутентификации вплоть до конкретного URL.

Бизнес-стимул 3: Безопасность

Защищает пользователей и данные, предоставляя им надежный доступ в зависимости от их роли в компании — как внутренним, так и удаленным работникам и доверенным партнерам, где бы они ни находились.

- Гарантирует безопасность удаленных рабочих мест
- Организует доступ к сети за считанные минуты, а не дни
- Предоставляет отчеты о событиях безопасности в режиме реального времени без крупных затрат

Бизнес-стимул 4: Оперативность

Решения быстро внедряются в ИТ-инфраструктуру с минимальными помехами для работы.

- Использует преимущества открытых стандартов, таких как SAML и Liberty Alliance
- Обеспечивает полное управление доступом — с единой точкой входа — для ваших подрядчиков и бизнес-партнеров
- Позволяет бизнес-решениям управлять ИТ — а не наоборот

Упрощая применение паролей и управление ими, Novell Access Manager помогает вашей организации улучшить работу пользователей, повысить безопасность, рационализировать бизнес-процессы и уменьшить стоимость администрирования и поддержки.

Novell Access Manager обеспечивает:

- Полное управление доступом с единой точкой входа и доступом на основе ролей к веб-, корпоративным и J2EE-приложениям
- Упрощает согласование профилей пользователей благодаря автоматическому созданию учетных записей и простому отображению федеративных верительных данных на определения политик
- Инфраструктура безопасности plug-and-play уменьшает расходы на внедрение и эксплуатацию

Федеративные электронные персоны

Многие современные предприятия тесно сотрудничают в онлайн, чтобы достичь новых уровней рентабельности и успеха. Они больше, чем когда-либо, сотрудничают над созданием совместимых технологий и продвижением на рынок новых, комплементарных предложений. Но чтобы происходило такое перекрестное опыление, доверенные бизнес-партнеры должны иметь безопасный доступ к ресурсам другого партнера. Во здесь-то и проявляется польза от федеративных электронных персон.

Novell Access Manager построен на прочном фундаменте, использующем стандарты федеративных электронных персон, включая Liberty Alliance, WS-Security и SAML. Этот фундамент минимизирует — или даже исключает — проблемы взаимодействия между внешними партнерами или внутренними отделами. На самом деле Novell Access Manager обеспечивает процесс идентичного конфигурирования всей федерации партнеров, будь то разные подразделения одной и той же организации или внешние бизнес-партнеры. В любом случае информация поступает туда, куда нужно — безопасно и беспрепятственно.

Защита приватности

Это составная часть соблюдения нормативных требований и доверительных деловых отношений: способность устанавливать для каждого из пользователей правила по обмену электронными персонами — в том числе правила типа «всегда разрешено», «требуется разрешение» или «не разрешено никогда». Novell Access Manager обеспечивает такой уровень встроенной защиты приватности как для ваших сотрудников, так и для партнеров, где бы они ни работали. Благодаря Novell

Access Manager ваша организация сможет гарантировать и документировать конфиденциальность пользователей. А для федеративного создания профилей пользователей Access Manager придерживается одних и тех же политик и протекций. Он требует, чтобы любая служба, прежде чем создавать их учетные записи, получала явное разрешение на это от ваших пользователей.

Компоненты Novell Access Manager

Novell Access Manager достаточно гибок, чтобы работать в самых сложных средах с оборудованием от многих поставщиков, обеспечивая гладкую интеграцию для управления доступом на всех уровнях. Novell Access Manager содержит поддержку лидирующего каталога Novell eDirectory, а также для Active Directory* и Sun* One* Directory Identity Stores. Он создает безопасные политики идентификации и доступа при помощи следующих компонентов:

- Identity Server
- Access Gateway
- Java * Application Agents
- SSL VPN
- Policy Engine
- Centralized Management Console

Identity Server

Identity Server — это компонент Novell Access Manager, который аутентифицирует пользователей и предоставляет информацию об их роли для принятия решений по авторизации. Он предлагает как прямую, так и федеративную аутентификацию с использованием разных методов: идентификаторы пользователей и пароли, сертификаты X.509 (взаимная аутентификация), жетоны (одноразовые пароли, получаемые через систему RADIUS) и Novell Modular Authentication Service (NMAS). Ваш администратор может указать любой из этих методов или комбинацию методов аутентификации, которые пользователи должны успешно пройти, чтобы получить доступ к вашим системам. Identity Server обеспечивает полную поддержку SAML и Liberty Alliance Web Service Framework. Благодаря этой поддержке ваша организация может легко сконфигурировать процесс аутентификации пользователей и распространения информации

электронных персон между разными доменами безопасности — будь то разные отделы внутри организации или внешние доверенные партнеры. Ваша организация может использовать стандартные профили Liberty Alliance Employee and Person, присутствующие в Identity Server, или задать специальные атрибуты и использовать их для принудительного соблюдения правил.

Identity Server обеспечивает также беспрепятственное согласованное создание пользователей, автоматически создавая учетные записи пользователей по запросам федерации. Без этой возможности пользователям приходилось бы регистрироваться (создавать учетные записи) у поставщика услуг, прежде чем он сможет включить их профили в федерацию.

Access Gateway

Access Gateway — это компонент Novell Access Manager, замещающий HTTP. Он служит точкой входа для веб-приложений и обеспечивает безопасность путем аутентификации, авторизации, единой точки входа через веб, введения учетной записи и шифрования данных — и все это без необходимости внесения изменений в реальные веб-приложения. Указатели URL защищенных ресурсов, определенные вашим администратором, можно связать с определенными веб-серверами, что позволит одному шлюзу защищать несколько веб-серверов. Администратор просто заменяет все записи DNS специальными службами, связывающими IP-адреса соответствующих веб-серверов с IP-адресами Access Gateway.

Ваш администратор может сконфигурировать разные политики единой точки входа для каждого ресурса и потребовать разных Authentication Contracts. Когда пользователь пытается получить доступ к ресурсу, который требует аутентификации, Access Gateway переадресует его к Identity Server с запросом соответствующего контракта аутентификации. После того как Identity Server выдаст необходимое

Access Gateway — это компонент Novell Access Manager, замещающий HTTP. Он служит точкой входа для веб-приложений и обеспечивает безопасность путем аутентификации, авторизации, единой точки входа через веб, введения учетной записи и шифрования данных — и все это без необходимости внесения изменений в реальные веб-приложения.

подтверждение, пользователь автоматически возвращается к Access Gateway с успешными результатами аутентификации и информацией о его роли. Информация о роли, которая может быть дополнена расширенными запросами к учетной записи пользователя, определяет право пользователя обращаться к запрашиваемым ресурсам.

Access Gateway также передает информацию учетных записей на веб-сервер, и вы можете использовать ее для персонализации контента или для исполнения дополнительных правил. Например, управляемая политиками функция введения учетных записей (identity injection) Access Gateway может использовать структуру Liberty Alliance Web Services Framework для извлечения информации из учетных записей и введения ее в веб-заголовки или строки запросов.

Благодаря Access Gateway имеющиеся у вас веб-приложения могут поддерживать новые службы идентификации без внесения в них каких-либо изменений, и вы можете сфокусировать требования авторизации вплоть до конкретного URL. Access Gateway может шифровать контент веб-сервера, что избавляет вас от необходимости устанавливать сертификаты SSL на каждый сервер. Access Gateway предоставляется как специальная служба NetWare или Linux, при этом она может содержать дополнительные службы, такие как Secure Sockets Layer Virtual Private Network (SSL VPN). Так как решение единой точки входа основано на браузере, администратору не потребуется устанавливать на машины конечных пользователей дополнительное клиентское ПО.

Компоненты Novell Access Manager:

- Identity Server
- Access Gateway
- Java Application Agents
- SSL VPN
- Policy Engine
- Централизованная консоль управления

«Теперь мы не только лучше контролируем права доступа пользователей к разным системам, но и можем предоставить нашим сотрудникам немедленный доступ к необходимым им ресурсам сразу после их зачисления в штат или смены подразделения».

Роберт Хенке (Robert Henke)

*Менеджер, Infrastructure Group
Intel
GEHE Pharma Handel GmbH*

Агенты Java-приложений

Novell предоставляет агенты Java-приложений (агенты J2EE) для IBM WebSphere, BEA WebLogic и JBoss. Новейшие версии этих агентов доступны для загрузки в любое время и не связаны с планом выпуска версий Novell Access Manager.

Точно так же, как Access Gateway защищает стандартные веб-приложения, агенты серверов Java-приложений обеспечивают аутентификацию и управление доступом, переадресовывая процесс аутентификации к Identity Server. Затем они используют информацию о роли пользователя, полученную от Identity Server, для выполнения политик. Для аутентификации и авторизации агенты используют стандарты Java Authentication and Authorization Service (JAAS) и Java Authorization Contract for Containers (JACC). Эти стандарты обеспечивают детальное управление аутентификацией для Enterprise JavaBeans* (EJBs) и сервлетов.

SSL VPN

Secure Sockets Layer Virtual Private Network (SSL VPN) — это безопасная технология удаленного доступа. Она использует веб-браузер для обеспечения бесклиентского, управляемого правилами дистанционного доступа к корпоративным приложениям, не основанным на HTTP. Данная служба базируется на Linux, и ее работу ускоряет Access Gateway, с которым она обменивается информацией.

При использовании SSL VPN администратор определяет ресурсы, к которым может обращаться пользователь, обычно указывая IP-адрес и интервал портов. Он также устанавливает определенные правила авторизации для ролей, которые созданы в Identity Server. Применяя эти правила, Novell Access Manager определяет, какие пользователи имеют право обращаться к центральным приложениям через SSL VPN.

Чтобы разрешить единую точку входа для удаленных пользователей, ваш администратор может сконфигурировать SSL VPN в качестве защищенной службы в рамках Access Gateway. Access Gateway переадресовывает запросы пользователей к Identity Server, как он это делает для защиты веб-приложений. Когда пользователь

аутентифицирован и роли определены, Access Gateway применяет единую точку входа для доступа к службе клиентской доставки SSL VPN. Затем модуль ActiveX или Java-апплет проверяет существование необходимого ПО, такого как межсетевой экран или антивирус. Тот же модуль или апплет устанавливает зашифрованное соединение и разрешает доступ к авторизованным корпоративным приложениям.

Policy Engine

Одно из главных преимуществ Novell Access Manager — это его способность управлять правилами и обеспечивать их соблюдение. Фактически, управление доступом на базе ролей является существенной частью всех компонентов Access Manager, которые опираются на соблюдение правил и регистрацию для составления регулярных отчетов о соответствии.

Novell Access Manager Policy Engine отличается высокой наращиваемостью и обеспечивает полный контроль над решениями в области правил и политик. Он позволяет независимым поставщикам интегрировать специальные процессы принятия решений. К тому же он обеспечивает разрешение определений политик и поддерживает определения правил на базе ролей или специальные способы принятия решений. Наконец, он обеспечивает соблюдение правил Java-приложениями, вплоть до уровня EJB и сервлетов EJB.

Централизованная консоль управления

Консоль управления на базе браузера предоставляет администраторы возможность централизованно просматривать, конфигурировать и управлять всеми установленными компонентами и правилами. С ее помощью ИТ-менеджер может контролировать состояние сети в режиме реального времени и автоматизировать распространение сертификатов. В масштабных системах консоль позволяет сгруппировать несколько шлюзов Access Gateway, а затем одновременно вносить изменения в их конфигурацию. Novell Access Manager реплицирует все конфигурации компонентов и правил в безопасном, отказоустойчивом хранилище.

Консоль управления отличается чрезвычайной гибкостью, что позволяет удовлетворить любые требования по администрированию. Она предлагает возможность делегировать функции администрирования:

- Серверов Identity Server
- Шлюзов Access Gateway (как для Linux, так и для NetWare)
- SSL VPN
- Агентов Java
- Устройств
- Политик

Платформа безопасного управления доступом

Снижение затрат. Повышение производительности труда. Защита интеллектуальной собственности. Ускорение инноваций и коллективная работа. Своевременный выпуск продуктов. Нарастивание продаж. Сегодня успех или провал всех этих усилий зависит от получения нужными людьми удобного и безопасного доступа к сетевым ресурсам. Доверенные сотрудники, партнеры и

заказчики — где бы они ни работали — нуждаются в беспрепятственном доступе. Хакеры и другие злоумышленники должны быть изолированы. ИТ-менеджерам требуется упрощенный, автоматизированный контроль над доступом, независимо от сетевой среды или ситуации.

Novell Access Manager представляет собой гибкое и мощное решение для управления доступом, которое обеспечивает контроль доступа к корпоративным сетям и приложениям всех видов. Для доверенных лиц, независимо от их местонахождения, это решение устраняет препятствия для доступа, в то же время повышая уровень безопасности.

Novell Access Manager — это ключевой компонент решения Novell для обеспечения безопасности и управления электронными персонками. Он служит фундаментом для управления доступом, который необходим для того, чтобы уверенно справляться с беспрецедентным ростом сетей и ужесточающимися требованиями регулирующих органов.

«Решения Novell для управления электронными персонками помогли нам объединить несколько компаний с различными базами данных и разными средствами управления, предоставив нашим пользователям единый идентификатор и пароль для доступа ко всем системам».

Д-р Вольфганг Зейлер (Dr. Wolfgang Seiler)

*Главный менеджер по технологиям
Allianz Suisse*

Novell Access Manager представляет собой гибкое и мощное решение для управления доступом, которое обеспечивает контроль доступа к корпоративным сетям и приложениям всех видов. Он устраняет препятствия для доступа со стороны доверенных лиц, где бы они ни находились, в то же время повышая уровень безопасности.

Для получения дополнительной информации обратитесь, пожалуйста, к местному авторизованному партнеру или в Московское представительство Novell:

121099, Москва,
Бизнес-Центр
«Новинский»,
Новинский бульвар, д. 3,
стр. 1
Тел.: +7(495)514-0910
Факс: +7 (495) 514-0911
Web: www.novell.ru

Телефоны в других странах:

США и Канада: 1 888 321
4272
Другие страны: 1 801 861
4272
Факс: 1 801 861 8473

Novell, Inc.
404 Wyman Street Waltham,
MA 02451 USA

