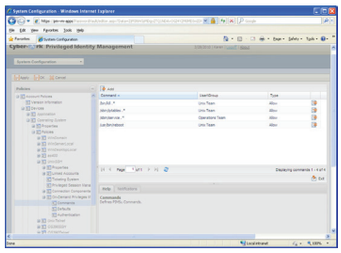
On-Demand Privileges Manager™ for Unix/Linux

On-Demand Privileges Manager — единое решение для управления доступом в Unix/Linux, позволяющее контролировать и отслеживать выполняемые суперпользователями команды на основании их ролей и задач.



Единая точка доступа для суперпользователя и привилегированных учетных записей других типов, реализованная при помощи простого в использовании веб-интерфейса для общего управления и определения политик привилегированных учетных записей. Решение позволяет эффективно управлять правами суперпользователей, необходимыми для выполнения конкретных команд.

Задача

Согласно данным СМИ, число инцидентов, в ходе которых злоумышленник получает доступ к критически важным данным компании, продолжает расти. Несанкционированный доступ (случайный или преднамеренный) к критически важным корпоративным системам и данным способен не только привести к продолжительным перебоям в работе и значительным расходам, но и существенно испортить репутацию Вашего бизнеса.

Возможность управления учетными записями с самыми широкими правами доступа. Во многих организациях ИТ-администраторы, разработчики приложений, администраторы баз данных и некоторые другие пользователи используют анонимные привилегии суперпользователя. Как следствие, слишком многие сотрудники обладают доступом к критически важным бизнес-системам и данным; при этом часто такой доступ не требуется им для выполнения повседневных служебных задач. Основная задача организаций, связанная с суперпользователями систем Unix и Linux, — обеспечение подотчетности и управляемости доступа к критически важным бизнес-системам и данным, а также регистрация времени этого доступа, причин и выполненных действий. Если эта информация недоступна, организация подвергается значительной угрозе. В числе факторов риска:

- Несоответствие нормативным требованиям и стандартам. Нормативные положения и стандарты (PCI DSS, SOX и т. д.) предъявляют все более строгие требования к управляемости и подотчетности действий суперпользователей
- Осложнения при выполнении рабочих процессов. Наличие в инфраструктуре нескольких суперпользователей без разделения доступа к командам может привести к увеличению количества человеческих ошибок, снижающих надежность, доступность и производительность критически важных систем.

Компромисс между уровнем безопасности, требованиями бизнеса и удобством эксплуатации. В настоящее время наиболее распространенным решением является SUDO. Однако его применение на уровне предприятия затруднено в связи с недостаточными возможностями масштабирования, а также необходимостью управления множеством серверов UNIX и выполнения задач по их обслуживанию. Кроме того, в SUDO отсутствует механизм создания отчетов для менеджеров и аудиторов. В целом это решение не обеспечивает требуемой безопасности, поскольку файлы и журналы аудита хранятся в локальных системах и доступны привилегированным пользователям.

Решение и его основные преимущества

CyberArk On-Demand Privileges Manager (OPM) — это первый унифицированный продукт под управлением политик, расширяющий возможности управления ИТ-инфраструктурой и обеспечивающий полную управляемость и прозрачность действий суперпользователей Unix/Linux и других привилегированных учетных записей в организации.

Устранение внутренних угроз: эффективное управление доступом. Решение позволяет защитить наиболее ценные ИТ-ресурсы благодаря предоставлению суперпользователям Unix/Linux разрешений на выполнение только определенных команд. Это позволяет снизить риск злоупотреблений и ошибок.

Обеспечение соответствия требованиям: персонализированный аудит и регистрация действий. Возможность связать привилегированную учетную запись и действия от ее имени с учетной записью конкретного пользователя является ключевым требованием в области аудита. Решение On-Demand Privileges Manager позволяет регистрировать действия каждого пользователя. Кроме того, функция записи текстовых данных обеспечивает сохранение всех введенных команд и их результатов, а также надежное размещение этих данных в хранилище CyberArk Digital Vault

Оптимизация бизнеса: единое решение для управления привилегированными учетными записями и привилегированными пользователями. Предварительно интегрированное решение позволяет оптимизировать работу ИТ-специалистов и аудиторов, предоставляя возможность централизованного управления и создания отчетов о пользователях, обладающих доступом к привилегированным учетным записям, а также о связанных с командами действиях, которые эти пользователи могут выполнять. Сочетание этих двух продуктов представляет собой мощное решение, которое позволяет управлять паролями привилегированных пользователей, а также осуществлять аудит и регистрировать действия пользователей на уровне команд.

Решение CyberArk On-Demand Privileges Manager обладает уникальными возможностями:

- Минимизация риска несанкционированного доступа к данным и сбоев ИТ-систем, связанных с неограниченными правами доступа суперпользователя.

- Обеспечение соответствия стандартам; демонстрация аудиторам способности обеспечивать безопасность, управляемость и подотчетность привилегий суперпользователя.

- Усовершенствованные инструменты мониторинга и отчетности позволяют с легкостью обнаруживать критические ошибки в бизнес-системах.

- Повышение защищенности серверов с аппаратной защитой под управлением Unix/Linux.

- Замена изолированных решений на базе SUDO масштабируемым продуктом корпоративного класса, обеспечивающим непревзойденный уровень безопасности, удобное централизованное управление и расширенные возможности аудита.

- Снижение совокупной стоимости владения благодаря внедрению интегрированного решения, устраняющего необходимость использования двух отдельных продуктов для управления привилегированными учетными записями и привилегированными пользователями.

Функции

Решение On-Demand Privileges Manager (OPM) для Unix/Linux является уникальным сочетанием передовых технологий защиты данных, гибких возможностей мониторинга и средств создания отчетов для управления учетными записями суперпользователей. Особенности решения:

- Единая точка доступа для ИТ-администраторов и аудиторов. Веб-портал позволяет пользователям определять политику для общих учетных записей, управлять ей и осуществлять поиск сохраненных сеансов.
- Эффективное управление доступом при использовании учетных записей суперпользователей. Делегирование прав привилегированных пользователей и других суперпользователей по требованию для выполнения конкретных команд.
- Встроенная функциональная возможность интеграции с решением Privileged Account Security. Возможность легко расширять требования к управлению привилегированными учетными записями на другие задачи бизнеса: управление привилегированными учетными записями, исключение встроенных паролей из сценариев приложений, безопасный единый вход для привилегированных и общих учетных записей, управление привилегированными сессиями.
- Удобный веб-интерфейс. Удобная навигация и поиск между всеми доменами привилегированных учетных записей, а также интуитивно понятные, пошаговые мастера создания рабочих процессов.
- Регистрация нажатий клавиш и текстового вывода команд. Расширенные средства аудита и отчетности.
- Централизованный механизм создания аудиторских и операционных отчетов. Унифицированная функция записи в журнал всех действий суперпользователя, интегрированная с другими функциями управления привилегированными учетными записями.
- Легкость интеграции с продуктами SIEM. Позволяет дополнить средства системного аудита и управления событиями средствами анализа действий привилегированных учетных записей.
- Высокая доступность. Встроенные решения для обеспечения высокой доступности и аварийного восстановления позволяют поддерживать сотни тысяч серверов.
- Возможность внедрения на уровне предприятия. Простота интеграции с существующей инфраструктурой предприятия, а также возможность расширения по мере развития организации.
- Безопасное, защищенное от несанкционированного доступа хранилище. Запатентованная и удостоенная отраслевых наград технология CyberArk Digital Vault™ позволяет защитить средства управления доступом и информацию о политиках, а также хранить данные сеансов доступа и информацию, необходимую для аудиторских проверок. Защищенная инфраструктура позволяет предотвратить незаконное изменение привилегий учетных записей и сохраненных данных сеансов как при передаче, так и при хранении.

Возможности решения On-Demand Privileges Manager для Windows

Привилегии администратора на серверах и настольных компьютерах Windows действительны в рамках всей организации. Однако стандартным пользователям для выполнения обычных рабочих задач привилегии администратора на постоянной основе не требуются. Решение On-Demand Privileges Manager для Windows дает возможность организациям реализовывать политику предоставления минимальных привилегий в средах Windows. При таком подходе сотрудники, имеющие права обычного пользователя, получают расширенные привилегии для отдельных приложений в соответствии с заранее определенными правилами. Это позволяет снизить затраты и повысить уровень безопасности.

Характеристики

Защищенная платформа:

- Многоуровневая система защиты
- Отсутствие прямого доступа к данным
- Интеграция с HSM

Управление доступом и рабочими процессами:

- Поддержка каталогов LDAP
- Идентификация и управление доступом

Многоязычный портал:

- Интеграция с решением SIEM
- SNMP
- Уведомления по электронной почте