ПРОВЕРКИ БЕЗОПАСНОСТИ БАЗ ДАННЫХ С ПОНЯТНЫМ РЕЗУЛЬТАТОМ

GuardVea

База данных работает.
А безопасно ли она настроена?

Проверьте настройки. Разберитесь в результатах.
Определите, что нужно исправить.



От рекомендаций по безопасности
к конкретным действиям вашей команды.

SoftVea, s.r.o.

www.guardvea.com · info@softvea.com · +421 940 404 737

ЧТО GuardVea МОЖЕТ ДЛЯ ВАС СДЕЛАТЬ

Четко определите настройки вашей базы данных.

Приложение запущено и пользователи работают. Это все еще не отвечает на вопрос о том, как защищена база данных.



Компания хранит в базе данных заказы, контакты и оперативные данные. Администратор знает техническую сторону дела, но руководству нужно решить, на что потратить время и деньги. GuardVea помогает проверить выбранные настройки безопасности и показать, какие рекомендации выполняются, а какие требуют внимания.

У контроля есть особые правила

Вы выбираете набор рекомендаций для своей среды базы данных. Для каждой проверки вы узнаете, что проверяется, почему это важно и какой ожидается результат. Вы можете основывать разговор о безопасности на определенных настройках.

Результат поможет определиться с дальнейшей работой

В отчете вас переведут с сервера базы данных на конкретную проверку и ее результат. Администратор может просмотреть подробную информацию и рекомендуемые действия по исправлению ситуации. Руководство получит более четкую основу для соглашения о дальнейших шагах.

> ### Когда руководство спрашивает о безопасности
> Вместо общего успокоения вы можете просмотреть отдельные проверки, их результаты и выводы, которые еще необходимо учесть.

ЧТО ВЫ БУДЕТЕ ПОДГОТОВИТЬ В СИСТЕМЕ

Ваши серверы. Объем вашего аудита.

Начните с того, что вам нужно проверить и в какой среде базы данных.

Вы указываете серверы баз данных

Вы добавляете в заказ адреса серверов и называете их по мере необходимости. Таким образом, вы будете иметь четкое представление о том, к каким средам применяется элемент управления. При подготовке также стоит назначить администратора, который обеспечит подключение и сможет объяснить контекст работы.

Ваши серверы

Базы данных, которые вы хотите сканировать.

Ваши чеки

Рекомендации и выбранный профиль.

Ваши результаты

Выводы и основания для исправления.

Вы выбираете подходящие рекомендации

Бенчмарк CIS — это набор рекомендаций по безопасной настройке конкретной технологии. Вы выбираете доступный файл, его версию и соответствующий профиль. В этом случае проверка основывается на указанном диапазоне, к которому вы можете обратиться при чтении результатов.

Вы учитываете метод работы

База данных на собственном сервере и управляемый облачный сервис предлагают администратору различные возможности. Поэтому выбор профиля также зависит от того, к каким настройкам у вас есть доступ. Объем проверки должен соответствовать тому, как вы используете базу данных.

Работайте в своем веб-браузере

Откройте библиотеку рекомендаций, подготовьте заказ и просмотрите результаты проверки в общей рабочей области. Инструменты открываются в отдельных окнах над рабочей областью с панелью значков, обеспечивающей доступ к каждому разделу.

> **Уточните объем перед проверкой**
> Какой сервер проверяете, по какой версии рекомендаций и с каким профилем? Эти данные придают результату необходимый контекст.

КАК РАБОТАЕТ ПРОВЕРКА

От выбора сервера до результата.

Отдельные шаги следуют друг за другом. Вы знаете, что готовить и где искать находки.



01 Определите объем аудита

Вы указываете серверы баз данных, доступный тест производительности и профиль сканирования. В заказе вы выбираете позиции из прайс-листа и проверяете данные.

02 Вы готовите соединение

Администратор создает назначенную учетную запись базы данных и предоставляет необходимый доступ. Проверка соединения поможет определить, можно ли связаться с сервером.

03 Пройдёт проверка

После оплаты заказа начнется проверка безопасности. Автоматические проверки подтверждают настройки; вы завершаете ответы и выражения в ручных проверках.

04 Вы проверите результаты

Вы увидите статус, оценку и подробную информацию о каждой проверке. По результатам проверки вы ознакомитесь с рекомендуемыми действиями по устранению проблемы и согласуете дальнейшие действия с администратором.

> Результат должен привести к следующему шагу
> Важно понимать открытие, его значение для вашего окружения и то, кто будет заниматься возможным исправлением.

БИБЛИОТЕКА РЕКОМЕНДАЦИЙ ПО БЕЗОПАСНОСТИ

Знайте, какие требования проверяются.

По каждой рекомендации вы можете посмотреть ее содержание и причину обратить на нее внимание.



Тест и версия

Вы выбираете определенный набор рекомендаций в библиотеке. Разрешение версии помогает назвать, на каких документах основана проверка. Таким образом, вы сможете говорить о том же объеме и для следующей работы.

Проверить описание

С выбранной рекомендацией вы прочтете, что подлежит проверке. Техническое название будет объяснено, и администратору будет проще понять, к какой настройке относится запрос.

Обоснование и влияние

Знать, что настройка рекомендована, недостаточно. Вам также необходимо понять, почему и как изменение может повлиять на ваши системы. Эта информация поможет вам оценить рекомендации для вашей среды.

Процедура проверки и исправления

Подробности могут включать этапы аудита, ожидаемый результат и процедуру исправления. У администратора под рукой есть документы, которые помогут ему проверить выводы и подготовить решение.

> Когда коллега спрашивает, зачем это менять
> Откройте конкретную рекомендацию. Вместе вы рассмотрите ее цель, результат проверки и влияние предлагаемого изменения.

ВЫБОР ПРОФИЛЯ

Проверьте в соответствии с вашей средой.

Выберите доступный профиль, соответствующий вашему способу работы и требуемой строгости.



Базовый профиль сервера

Профиль L1_server предназначен для сервера базы данных с доступом к операционной системе. Он обеспечивает отправную точку для проверки основных рекомендаций в среде, которой вы управляете.

Облачный профиль

Профиль L1_cloud находится в порядке для SQL Server на AWS RDS. Он учитывает среду управляемой службы. Поэтому при выборе основывайте свое решение на конкретной технологии базы данных и методе ее работы.

Более строгий профиль сервера

Профиль L2_server расширяет требования к более жесткой настройке. Некоторые рекомендации могут повлиять на работу или производительность. Прежде чем использовать их, необходимо оценить, как они повлияют на ваши приложения.

> Например, с базой данных бизнес-приложения.
> Администратор вместе с владельцем приложения выбирает профиль и проверяет эффективность рекомендаций. Затем вы оцениваете результат в пределах согласованного диапазона.

Вы можете проверить конкретный эталон и доступные профили при подготовке заказа. Выбор должен основываться на вашем окружении.

АВТОМАТИЧЕСКИЕ ПРОВЕРКИ

Проверьте определенные настройки.

Для поддерживаемых проверок вы получите результат проверки базы данных, к которому можно вернуться.



Подключение к серверу

Перед фактической проверкой требуется функциональное соединение. В обзоре можно увидеть, удалось ли подключение. Если нет, у администратора есть повод проверить доступность сервера, учетной записи или необходимых разрешений.

Ход проверки

Выполняя проверки, вы отслеживаете их статус и ход выполнения. Различают ожидание, выполняющуюся обработку, завершение и сбой. Так вы узнаете, есть ли у вас уже результат или вам еще нужно посвятить себя самому бегу.

Результат рекомендации

Оценивайте каждую проверку в сравнении с тем, что она должна была проверить. Его оценка и подробные результаты помогают администратору просмотреть результаты наряду с ожидаемыми настройками.

Основа для информативной дискуссии

Руководству и администратору не нужно начинать с общего вопроса, все ли в порядке. Они выбирают конкретную проверку, смотрят результат и определяют, что еще нужно проверить.

> ### Когда проверка не завершена
> Сначала вы проверяете причину обработки. Недоступный сервер или ошибка сканирования требуют другого следующего шага, чем обнаруженный несоответствующий параметр.

РУЧНАЯ ПРОВЕРКА

Человек должен что-то подтвердить.

Если необходимо знать процедуры или оперативный контекст, вы должны заполнить ответы в анкете.



Вопросы по рекомендации

Ручная проверка откроет анкету по выбранной рекомендации. Ответственное лицо ответит на вопросы и может добавить короткое заявление. Таким образом, проверка также фиксирует информацию, которую невозможно прочитать только из технических настроек.

Заявление о результате

К ответам вы добавите итоговое заявление об общем выполнении рекомендации. Коллега, который вернется к результату позже, также сможет получить устное объяснение.

Автоматические и ручные шаги дополняют друг друга

Автоматическая проверка помогает при определенных настройках. В анкете, составленной вручную, будут использоваться знания людей, которые управляют окружающей средой. В обзоре эти виды проверок разделены, чтобы вы знали, как был получен результат.

> Например, в корпоративной процедуре
> Технический результат не может объяснить, как команда выступает на практике. Ответ и примечание ответственного лица добавят необходимый контекст.

РЕЗУЛЬТАТЫ И ОБЗОР

От обзора к конкретному выводу.

Сначала вы смотрите состояние сервера и проверяете. Затем вы открываете то, на чем вам нужно сосредоточиться.



Заказы и серверы

В обзоре вы выбираете заказ и его цели в базе данных. У вас при себе объем проверки и информация о ее ходе. Имея несколько серверов, вы можете определить, к какой среде относится результат.

Счет и подробности результатов

Выбрав проверку, вы можете увидеть оценку, статус и отчет. Счет служит для быстрого ориентирования. Принимая решение о дальнейших действиях, вы дополните их, ознакомившись с выводами и содержанием рекомендации.

Прочитайте результат в контексте

Это зависит от профиля, объема контроля и того, как вы используете базу данных. Администратор может объяснить технические детали, а владелец приложения может добавить смысл операции. Вместе они определят соответствующий следующий шаг.

> ### На рабочей встрече
> Вы выбираете сервер и открываете конкретный чек. От результата вы сразу переходите к вопросу, что нужно проверить, кто этим будет заниматься и когда вы к этому вернетесь.

РЕКОМЕНДАЦИИ ПО КОРРЕКЦИИ

Это открытие является началом дальнейшей работы.

Если в обзоре обнаружена проблема, вам необходимо понять рекомендуемое изменение и его влияние.



Найдите шаги по исправлению для каждой рекомендации.

Подробно вы найдете раздел, посвященный средству. Администратор может обратиться к описанным шагам и сравнить их с текущим состоянием базы данных. Не обязательно начинать с краткого указания на неудовлетворительный результат.

Принимайте решения с учетом вашей операционной среды

Рассмотрите рекомендуемое изменение, а также то, какие приложения используют базу данных и что им от нее нужно. При планировании это поможет узнать возможное воздействие, ответственного лица и подходящую дату вмешательства.

После изменения вы можете проверить результат

После исправления повторите соответствующую проверку и просмотрите новый результат. Это показывает, соответствует ли настройка ожидаемому состоянию или все еще требует внимания.

> ### Когда необходимо изменить важную настройку
> Администратор рассматривает рекомендацию с владельцем приложения и согласовывает дальнейшие действия. Результат проверки обеспечивает основу для этой работы.

ПОДГОТОВКА ДОСТУПА

Ваш администратор подготовит соединение.

Перед проверкой вы уточняете необходимый аккаунт, наличие сервера и ответственность за подготовку.



Указанная учетная запись базы данных

Заказ работает с пользователем базы данных Guardvea. Администратор создаст его на указанных серверах в соответствии с требованиями проверки. Вы подтвердите в системе, что аккаунт готов.

Учетные данные для подключения

При подготовке заказа вы сгенерируете пароль для указанной учетной записи. Администратор обеспечит его настройку на серверах, входящих в область действия. Данные должны соответствовать подготовленному соединению.

Проверить наличие

Перед началом необходимо убедиться, что сервер доступен и можно войти в систему. Состояние соединения помогает отделить проблему подготовки доступа от самого результата проверки безопасности.

Прекращение доступа

Приказ также включает подтверждение того, что пользователь Guardvea будет удален после завершения проверки. Поэтому согласуйте этот последний шаг с администратором.

> Подготовка имеет своего человека
> Назначьте администратора для настройки учетной записи, проверки соединения и обеспечения отзыва доступа после завершения аудита.

ДЛЯ КОГО ПРЕДНАЗНАЧЕН GuardVea

Каждому нужна другая точка зрения.

Совместный результат помогает связать технические выводы с принятием бизнес-решений.



Руководство компании

Он получит более конкретную основу для разговора о безопасности баз данных. Он может поинтересоваться результатами, необходимой работой и следующей процедурой.

Менеджер базы данных

Просматривает рекомендации, результаты и процедуры исправления для конкретной среды. Ему есть на что опираться при подготовке изменений.

Команда безопасности

Он работает с определенным объемом контроля и его результатами. В случае технических заключений он может отслеживать работу администратора.

Владелец приложения

Он добавляет из базы данных то, что нужно приложению. Это помогает оценить, как рекомендуемое изменение повлияет на повседневную работу.

Внешний ИТ-партнер

Может пройти проверку и подготовку среды вместе с компанией. Обсуждение основано на конкретных проверках результатов.

> ### Общий язык для следующего шага
> Администратор объясняет обнаружение, владелец заявки заполняет операционный контекст, а руководство определяет время и ресурсы для решения.

ПРЕДПОСЫЛКИ И ПОЯСНЕНИЯ

Вы также понимаете причину проверки.

У рекомендации есть цель. При оценке результата это также поможет узнать его более широкий контекст.



Почему это проверяется?

Обоснование рекомендации объясняет, почему эта настройка важна. Администратор может лучше объяснить, почему делается открытие и что необходимо учитывать при принятии решения.

На что может повлиять изменение

Раздел «Воздействие» помогает с планированием корректирующих мер. Таким образом, вы можете прочитать технические рекомендации вместе с описанием приложений и требований к эксплуатации.

Ссылки и справочная информация

Ссылки и ссылки на CIS Controls также доступны в деталях, если они содержатся в документах. Если вам нужна более детальная оценка, вам есть куда продолжить.

> ### Когда нужно объяснить рекомендацию руководству
> Начните с его цели, покажите результат и распишите возможное воздействие средства. Основа для решения будет создана на основе технических деталей.

ОБЫЧНАЯ СИТУАЦИЯ ИЗ ПРАКТИКИ

Новое приложение. Новые вопросы.

Компания готовится к развертыванию приложения и хочет проверить настройки среды своей базы данных.



До проверки

Администратор определяет сервер базы данных и доступный тест. Вместе с владельцем приложения он выбирает профиль, подготавливает необходимую учетную запись и проверяет соединение.

Во время проверки

Команда отслеживает ход автоматических проверок. В случае ручных рекомендаций ответственное лицо добавляет ответы и объясняет, как компания справляется с этим требованием.

При чтении результатов

Администратор откроет результаты и просмотрит их вместе с владельцем приложения. В случае неудовлетворительных настроек они оценят рекомендуемое средство и его влияние.

При планировании дальнейшей работы

Компания определит ответственность и сроки внесения любых изменений. После изменения он может повторить соответствующие проверки и проверить новое состояние базы данных.

> ### От вопроса к решению
> Вместо общей дискуссии команда делает конкретные выводы. Он знает, что ему нужно проверить и согласовать, прежде чем сделать следующий шаг.

ЧТО ВЫ ПОЛУЧАЕТЕ ОТ ЧЕКА

Более четкая основа для следующих шагов вашей команды.

Ценность обзора в том, что он помогает понять состояние и подготовиться к дальнейшей работе.



Обзор проверенной области

Вы можете определить, какие серверы и рекомендации были проверены и какой профиль был выбран. Этот контекст остается с результатами, что делает объем проверки понятным.

Конкретные выводы

Вы можете увидеть результат и подробную информацию по каждой рекомендации. У администратора есть основание для проверки настроек, а руководство может запросить дальнейшие действия для получения конкретных результатов.

Информация для планирования следующих шагов

Описание, обоснование, влияние и меры по исправлению ситуации помогают подготовить решение. Результат относится к выбранным элементам управления; принимая решение, вы оцениваете его наряду с другой информацией о безопасности компании.

> ### Когда проверка окончена
> Договоритесь о том, какие выводы вы будете проверять, кто будет их решать и как вы будете проверять результаты изменений. Таким образом, проверка также может помочь в дальнейшей работе.

КАК НАЧАТЬ

Начните с одной среды баз данных.

Давайте выберем конкретный сервер и вопросы, на которые вам нужно ответить. Мы подготовим ассортимент в соответствии с вашей средой.

1. Расскажите нам, чем вы занимаетесь

Подготовьте тип и версию базы данных, порядок ее работы и краткое описание приложений, которые ее используют. Вместе мы выясним, что вам нужно проверить и кто позаботится о техническом обучении у вас дома.

2. Согласуйте соответствующий объем аудита.

Мы рассмотрим доступные тесты, профили и необходимые элементы управления. Администратор готовит доступ и подключение. Прежде чем создать заказ, вы просматриваете его позиции и цену.

3. Вы оцениваете результаты и дальнейшую работу

После завершения проверки вы увидите как выводы, так и рекомендации. Вы и ваша команда определите, какие настройки необходимо просмотреть и какие изменения подготовить. В зависимости от результата вы можете продолжить работу с другими базами данных.

Ваше окружение

Тип и версия базы данных · Режим работы

Объем контроля

Серверы баз данных · Тест · Профиль

Следующая процедура

Результаты · Оценка результатов · Средства правовой защиты

У вас есть особые требования?

Опишите среду вашей базы данных и цель проверки. Мы обсудим с вами наличие соответствующих средств контроля и необходимую подготовку. С самого начала будет яснее, каким должен быть результат.

> Для первого разговора достаточно конкретного примера
> Например, база данных вашего основного приложения, его версия и принцип работы. Мы покажем вам подходящую следующую процедуру.

СВЯЗАТЬСЯ

Давайте посмотрим на ваши базы данных.

Мы будем рады рассказать вам, что вам нужно проверить и как GuardVea может помочь.



Каждая среда имеет свои требования. Кто-то готовит новое приложение, кто-то хочет проверить существующий сервер или получить основу для доработок безопасности. Начнем с того, что важно для вашего бизнеса.

Согласуйте объем вашей первой проверки

Напишите нам или позвоните нам. Мы рассмотрим тип базы данных, принцип ее работы и цель проверки. Вместе мы уточним доступные варианты и что нужно будет подготовить перед осмотром.

SoftVea, s.r.o.

info@softvea.com

+421 940 404 737

www.guardvea.com · www.softvea.com

Проверьте настройки. Понять выводы.