Руководство Администратора

по системе RS-Discovery (R-Sight)

RS TEAM

rs.team

СОДЕРЖАНИЕ

1 НАЧАЛО РАБОТЫ С RS-DISCOVERY (R-SIGHT)

Добро пожаловать в RS-Discovery (R-Sight)! Данное руководство поможет вам настроить и запустить нашу платформу интеллектуального анализа ИТ-инфраструктуры на базе ИИ всего за несколько минут.

1.1 Обзор быстрого старта

RS-Discovery (R-Sight) трансформирует ваши ИТ-операции путем автоматического обнаружения инфраструктуры, сопоставления зависимостей и предоставления аналитики на базе ИИ. Вот чего вы добьетесь с помощью этого руководства:

- Создадите учетную запись RS-Discovery (R-Sight)
- Настроите свою первую организацию
- Развернете агентов обнаружения в вашей сети
- Запустите первое сканирование инфраструктуры
- Включите функции ИИ для интеллектуальной аналитики

1.2 Получение учетной записи

1. Регистрация в RS-Discovery (R-Sight)

Посетите сайт RS-Discovery (R-Sight) и нажмите «Зарегистрироваться», чтобы создать учетную запись:

- Введите ваш рабочий адрес электронной почты
- Выберите надежный пароль
- Подтвердите адрес электронной почты
- Заполните профиль организации

2. Настройка организации

Настройте параметры вашей организации:

- **Название организации:** Название вашей компании
- **Часовой пояс:** Для точности планирования и отчетности
- **Основной контакт:** Техническое контактное лицо для уведомлений
- **Предпочтения по уведомлениям:** Email, SMS

1.3 Первое сканирование Discovery

Скачивание агента Discovery

В вашей панели управления перейдите в раздел Discovery → Агенты и скачайте подходящего агента для вашей среды:

- **Windows-агент:** Для обнаружения серверов и рабочих станций Windows
- **Linux-агент:** Для обнаружения систем Linux/Unix
- **Сетевой агент:** Для обнаружения сетевых устройств на базе SNMP
- **Облачный агент**

Программа установки агента проведет вас через процесс настройки с помощью простого интерфейса мастера установки.

Создание токена Discovery

В панели управления RS-Discovery (R-Sight):

1. Перейдите в Настройки → Токены обнаружения
2. Нажмите «Создать новый токен»
3. Настройте параметры токена:

- **Имя:** Описательное имя (например, «Производственная сеть»)
- **Разрешения:** Выберите область Discovery
- **Срок действия:** Установите время жизни токена

4. Надежно скопируйте сгенерированный токен

Настройка области Discovery

Определите конкретику для Discovery:

1. Перейдите в Discovery → Конфигурация
2. Установите параметры Discovery:

- **IP-диапазоны:** Определите сегменты сети для сканирования
- **Учетные данные:** Добавьте сервисные учетные записи для доступа через WMI/SSH
- **Расписание:** Установите частоту сканирования (рекомендуется: каждые 4 часа)
- **Глубина Discovery:** Выберите между быстрым, стандартным или глубоким сканированием

Мониторинг прогресса Discovery

Наблюдайте за прогрессом:

- **Активные сканирования:** Статус Discovery в реальном времени
- **Активы:** Серверы, рабочие станции, приложения
- **Связи:** Автоматически сопоставленные зависимости
- **ИИ-аналитика:** Немедленный анализ объектов

Основные компоненты панели мониторинга

После вашего первого сканирования панель мониторинга покажет:

Обзор инфраструктуры

- Общее количество обнаруженных устройств по типам
- Распределение операционных систем
- Визуализация топологии сети
- Статус критически важных услуг

Панель ИИ-аналитики

- Оценка рисков
- Возможности оптимизации
- Пробелы в соответствии Compliance
- Прогнозируемые проблемы

Поток событий

- Обновления discovery в реальном времени
- Результаты корреляции
- Предупреждающие уведомления
- Состояние здоровья системы

1.4 Активация функций ИИ

1. Включение ИИ-анализа

Функции ИИ RS-Discovery (R-Sight) готовы к использованию немедленно:

1. Перейдите в Настройки → Конфигурация ИИ
2. Включите желаемые функции:

- **Авто-аналитика:** Автоматический анализ инфраструктуры
- **Прогнозная аналитика:** Прогнозирование сбоев
- **Умная корреляция:** Интеллектуальная группировка событий
- **Поиск на естественном языке:** Запросы на обычном языке

2. Попробуйте запросы на естественном языке
Используйте строку поиска, чтобы задавать вопросы на обычном языке:
- «Покажи мне все Windows-серверы в промышленной среде»
- «На каких серверах отсутствуют критические исправления?»
- «Найди базы данных с высоким использованием процессора»
- «Выведи список всех просроченных SSL-сертификатов»

3. Настройка предпочтений ИИ
Настройте поведение ИИ:
- **Частота анализа:** Как часто генерировать аналитику
- **Чувствительность предупреждений:** Установите пороги для прогнозов
- **Фокусные области:** Приоритет безопасности, производительности или соответствия нормативным требованиям
- **Контроль затрат:** Установите лимиты на обработку данных ИИ

1.5 Создание ваших первых отчетов

Быстрая генерация отчетов
Перейдите в Отчеты → Создать новый. Выберите шаблон отчета:
- **Резюме для руководства:** Высокоуровневый обзор инфраструктуры
- **Отчет об инвентаризации:** Полный список активов
- **Оценка рисков:** Безопасность и операционные риски

Отчеты, созданные ИИ
Позвольте ИИ создавать отчеты за вас:
- Нажмите «Сгенерировать с помощью ИИ»
- Опишите, что вам нужно: «Создай ежемесячный отчет о состоянии здоровья инфраструктуры для руководства»
- Просмотрите и настройте сгенерированный отчет
- Запланируйте автоматическую доставку

1.6 Настройка уведомлений

Настройка каналов предупреждений
Перейдите в Настройки → Уведомления. Добавьте каналы уведомлений:
- **Электронная почта:** Индивидуальные адреса или списки рассылки
- **Microsoft Teams:** Нативная интеграция с Teams
- **SMS:** Для критических предупреждений
- **Webhook:** Пользовательские интеграции

Правила предупреждений
Создайте умные правила уведомлений:
- **На основе серьезности:** Маршрутизация по степени критичности
- **На основе услуг:** Предупреждения для конкретных приложений
- **На основе времени:** Рабочее время в сравнении с нерабочим
- **Эскалация:** Многоуровневые цепочки уведомлений

2 АНАЛИТИКА НА БАЗЕ ИИ

Использование искусственного интеллекта для интеллектуального управления ИТ-операциями.

2.1 Обзор

Аналитика RS-Discovery (R-Sight) на базе ИИ превращает необработанные данные об инфраструктуре в практически значимую информацию, обеспечивая проактивное управление ИТ и принятие обоснованных решений.

2.2 Возможности ИИ

Обнаружение зависимостей

- Автоматическое сопоставление услуг
- Обнаружение зависимостей приложений
- Анализ паттернов взаимодействия
- Идентификация бизнес-услуг

Анализ связей

- Классификация соединений
- Определение ролей услуг
- Оценка важности зависимостей
- Оценка влияния

Прогнозная аналитика

- Прогнозирование сбоев
- Прогнозирование мощностей
- Анализ трендов производительности
- Обнаружение аномалий

2.3 Ключевые функции

1. Интеллектуальное сопоставление услуг

Автоматическое обнаружение и классификация услуг

- Идентифицирует услуги на основе сетевого трафика
- Сопоставляет зависимости приложений
- Обнаруживает потоки аутентификации
- Выявляет процессы обмена данными

2. Оценка рисков

Анализ безопасности

- Корреляция уязвимостей
- Оценка подверженности угрозам
- Анализ путей атак

- Пробелы в соответствии нормативным требованиям (Compliance)

Операционный риск

- Единые точки отказа
- Цепочки зависимостей
- Критичность услуг
- Влияние на бизнес

3. Обработка естественного языка

Семантический поиск

- Запрос: «Найти все серверы баз данных в промышленной среде»
- Результаты: Серверы с SQL Server, MySQL, PostgreSQL, помеченные тегом среды Production

Интеллектуальные запросы

- Понимание естественного языка
- Поиск с учетом контекста
- Нечеткое соответствие
- Распознавание синонимов

4. Автоматизированная аналитика

Рекомендации по инфраструктуре

- Улучшение конфигураций
- Укрепление безопасности
- Оптимизация производительности
- Снижение затрат

Анализ влияния изменений

- Затронутые услуги
- Оценка рисков
- Планирование отката
- Рекомендации по тестированию

2.4 Модели ИИ

- Сложные логические рассуждения
- Технический анализ
- Генерация текстов на естественном языке
- Понимание контекста

Машинное обучение

- Распознавание образов
- Обнаружение аномалий
- Прогнозное моделирование

- Алгоритмы классификации

Векторные представления (Embeddings) и RAG

- Векторный поиск
- Поиск по сходству
- Извлечение знаний
- Расширение контекста

2.5 Лучшие практики

1. Качество данных

- Обеспечьте точность данных о КЕ (конфигурационных единицах)
- Регулярно обновляйте данные Discovery
- Проверяйте корректность связей
- Очищайте метаданные

2. Оптимизация ИИ

- Контролируйте использование токенов
- Кэшируйте ответы ИИ
- Группируйте похожие запросы
- Используйте подходящие модели

3. Валидация результатов

- Проверяйте предложения ИИ
- Тестируйте рекомендации
- Подтверждайте зависимости
- Верифицируйте оценки рисков

2.6 Мониторинг и метрики

Производительность ИИ

- Время ответа
- Показатели точности
- Потребление токенов
- Частота ошибок

Бизнес-ценность

- Предотвращенные инциденты
- Сэкономленное время
- Улучшение точности
- Снижение затрат

3 УПРАВЛЕНИЕ НОРМАТИВНЫМИ ТРЕБОВАНИЯМИ (COMPLIANCE)

Автоматизированная проверка соответствия и отчетность по нормативным стандартам.

3.1 Обзор

Функции управления соответствием RS-Discovery (R-Sight) помогают организациям соблюдать нормативные стандарты посредством автоматизированного сканирования, непрерывного мониторинга и формирования всеобъемлющей отчетности.

Оценка уязвимостей

- Сопоставление CVE (общих уязвимостей и подверженностей)
- Статус исправлений (патчей)
- Обновления безопасности
- Отклонение конфигурации (дрифт)

Непрерывный мониторинг

Проверки в реальном времени

- Изменения конфигурации
- Модификации доступа
- Нарушения политик
- События безопасности

3.2 Управление политиками

Назначение политик

- По типу КЕ (конфигурационной единицы)
- По департаменту
- По среде
- По критичности

Панель управления Compliance

Представление для руководителей

- Оценка Compliance
- Анализ трендов
- Тепловая карта рисков
- Пункты плана действий

Отчетность

Отчеты Compliance

Стандартные отчеты

- Резюме для руководства
- Детальные результаты
- Планы устранения нарушений
- Аудиторские доказательства

Пользовательские отчеты

- Специфические контроли
- Фокус на департаментах
- Анализ по временным периодам
- Отчеты о трендах

Форматы отчетов

- PDF (готов к аудиту)
- Excel (детальные данные)
- HTML (интерактивный)
- API (интеграция)

Интеллектуальное соответствие на базе ИИ

Интеллектуальный анализ

- Распознавание образов
- Сокращение количества ложных срабатываний
- Приоритизация рисков
- Предложения по устранению нарушений

Первоначальная настройка

- Выбор нормативных требований (Compliance)
- Определение области действия (KE/департаменты)
- Настройка политик
- Установка расписания сканирования
- Назначение ответственных

Лучшие практики

1. Непрерывное совершенствование

- Регулярные обновления политик
- Пересмотр базовых показателей
- Управление исключениями
- Оптимизация процессов

2. Документирование

- Ведение базы доказательств
- Документирование исключений
- Отслеживание устранения нарушений

- Архивация отчетов

3. Автоматизация

- Автоматизированное сканирование
- Автоматическое устранение нарушений
- Автоматизация рабочих процессов
- Генерация отчетов

Поддержка аудита

Сбор доказательств

- Автоматические скриншоты
- Резервные копии конфигураций
- Журналы изменений
- Записи о доступе

Доступ аудитора

- Учетные записи только для чтения
- Фильтрованные представления
- Возможности экспорта
- Безопасный доступ

4 ИНТЕГРАЦИЯ ВИДЖЕТОВ ОТЧЕТОВ ДЛЯ ПАНЕЛИ МОНИТОРИНГА

4.1 Обзор

Платформа RS-Discovery (R-Sight) поддерживает бесшовную интеграцию между шаблонами отчетов и виджетами панели мониторинга. Эта функция позволяет пользователям:

- Использовать шаблоны отчетов в качестве предварительно настроенных виджетов панели мониторинга
- Создавать многоразовые визуализации с согласованными конфигурациями
- Быстро собирать панели мониторинга, выбирая из доступных шаблонов отчетов
- Поддерживать единообразие на различных панелях мониторинга

4.2 Ключевые функции

1. Тип виджета «Отчет» Тип виджета «отчет» (report) напрямую использует шаблоны отчетов.

2. Конфигурация виджета в шаблоне отчета Шаблоны отчетов теперь включают специфические настройки виджета в поле widgetConfig:

3. Сопоставление типов визуализации Шаблоны отчетов поддерживают различные типы визуализации, которые соответствуют отрисовке виджета:

Визуализация отчета	Отображение виджетов
stat, card, gauge	Статичный виджет
bar, line, pie, donut, area, scatter	Виджет диаграммы
table, grid	Виджет таблицы
list	Виджет списка
heatmap	Виджет диаграммы (планируемое улучшение)

4.3 Использование шаблонов отчетов в панелях мониторинга

Интерфейс конструктора панелей мониторинга

Конструктор панелей мониторинга теперь отображает доступные шаблоны отчетов на боковой панели:

- Перейдите в Конструктор панелей мониторинга
- Нажмите на вкладку «Виджеты»
- Прокрутите вниз до раздела «Шаблоны отчетов»
- Нажмите на любой шаблон отчета, чтобы добавить его как виджет
- Откроется диалоговое окно конфигурации виджета с предварительно заполненными настройками

Диалоговое окно конфигурации виджета

При настройке виджета отчета:

- **Вкладка «Основные»:** Показывает заголовок виджета (наследуется из названия отчета)
- **Вкладка «Источник данных»:** Отображает детали выбранного шаблона отчета, включая: Описание, Категорию, Тип визуализации, Теги

- **Вкладка «Визуализация»:** Показывает, что настройки управляются шаблоном отчета
- **Вкладка «Дополнительно»:** Настройка интервала обновления и других параметров

4.4 Примеры шаблонов отчетов

Система включает предопределенные шаблоны отчетов:

- **Обзор статуса КЕ** — Круговая диаграмма, показывающая распределение КЕ по статусу
- **Открытые запросы по приоритету** — Столбчатая диаграмма открытых запросов
- **Количество активных КЕ** — Виджет статистики, показывающий общее число активных КЕ
- **Последние действия** — Список последних системных событий
- **Распределение типов КЕ** — Диаграмма-пончик по типам КЕ
- **Сводка статусов задач** — Таблица, показывающая количество задач по статусам

4.5 Лучшие практики

- **Согласованное именование:** Используйте описательные названия для шаблонов отчетов, которые будут отображаться на панелях мониторинга
- **Подходящий размер:** Устанавливайте разумные размеры по умолчанию в зависимости от типа визуализации
- **Производительность:** Учитывайте сложность запроса при установке интервалов обновления
- **Повторное использование:** Создавайте универсальные шаблоны отчетов, которые могут работать в различных контекстах
- **Документирование:** Добавляйте четкие описания, чтобы помочь пользователям понять, что показывает каждый шаблон

4.6 Конечные точки API (API Endpoints)

Шаблоны отчетов

- GET /api/reports/templates — Список всех доступных шаблонов
- POST /api/reports/templates — Создание нового шаблона
- POST /api/reports/execute/:id — Выполнение отчета и получение данных

Виджеты панели мониторинга

- POST /api/dashboards/:id/widgets — Добавление виджета на панель
- GET /api/dashboards/:id/widgets/:widgetId/data — Получение данных виджета
- PUT /api/dashboards/:id/widgets/:widgetId — Обновление конфигурации виджета

5 ФУНКЦИИ DISCOVERY

Всеобъемлющие возможности Discovery для сетей и инфраструктуры.

5.1 Обзор

Движок Discovery RS-Discovery (R-Sight) автоматически идентифицирует и каталогизирует ИТ-активы во всей вашей инфраструктуре, создавая инвентарную опись аппаратного обеспечения, программного обеспечения и услуг в реальном времени.

5.2 Методы Discovery

Агентный Discovery
Агент RS-Discovery (R-Sight)
- Легковесные агенты на Python/PowerShell
- Глубокая инспекция системы
- Мониторинг в реальном времени
- Безопасная связь

Возможности
- Инвентаризация оборудования
- Обнаружение ПО
- Мониторинг услуг
- Сопоставление сети
- Метрики производительности

Безагентный Discovery
Поддержка протоколов
- WMI: Системы Windows
- SSH: Системы Linux/Unix
- SNMP: Сетевые устройства
- API: Облачные платформы

Преимущества
- Без установки ПО
- Минимальное воздействие
- Широкая совместимость
- Быстрое развертывание

5.3 Область Discovery

Discovery для инфраструктуры
Серверы
- Физические серверы
- Виртуальные машины
- Контейнеры
- Облачные экземпляры (компоненты)

Рабочие станции
- Настольные ПК
- Ноутбуки

- Тонкие клиенты
- Мобильные устройства

Сетевые устройства
- Маршрутизаторы
- Коммутаторы
- Межсетевые экраны
- Балансировщики нагрузки

Discovery для программного обеспечения
Операционные системы
- Windows (Серверные/Клиентские)
- Дистрибутивы Linux
- Варианты Unix
- ОС для контейнеров

Приложения
- Установленное ПО
- Запущенные сервисы
- Веб-приложения
- Системы баз данных

Лицензии
- Лицензионные ключи
- Даты истечения срока действия
- Метрики использования
- Статус соответствия

Discovery для услуг
Сетевые услуги
- Активные услуги
- Прослушиваемые порты
- Определение протоколов
- Зависимости услуг

Услуги приложений
- Веб-серверы
- Серверы баз данных
- Серверы приложений
- Очереди сообщений

5.4 Процесс Discovery

1. Первоначальное сканирование
Настройте параметры Discovery:
- **Диапазон:** Определите диапазон IP-адресов для сканирования (например, 192.168.0.0/16)
- **Методы:** Выберите протоколы Discovery (WMI, SSH, SNMP)
- **Учетные данные:** Используйте учетные данные, хранящиеся в защищенном хранилище
- **Расписание:** Установите время автоматического сканирования (например, ежедневно в 02:00)

2. Сбор данных

Процесс Discovery автоматически собирает исчерпывающую информацию о каждом найденном активе:

- **Информация об узле:** Имя узла, детали операционной системы и конфигурация системы
- **Детали оборудования:** Спецификации процессора, объем памяти и установленное оборудование
- **Информация о хранилище:** Дисковые накопители, емкость и проценты использования
- **Сетевые детали:** Сетевые интерфейсы и активные соединения

3. Конвейер обработки

- Валидация данных
- Дедупликация
- Создание/обновление КЕ
- Сопоставление связей
- Обогащение данными ИИ

4. Обновление инвентарной описи

- Создание новых КЕ
- Обновление существующих КЕ
- Пометка неактивных КЕ
- Отслеживание изменений

5.5 Продвинутые функции

Интеллектуальная классификация

Определение типа устройства

- Сервер против рабочей станции
- Среда Prod против среды Dev
- Физическое против виртуального
- Идентификация роли

Категоризация ПО

- Семейства приложений
- Отслеживание версий
- Обнаружение окончания срока службы (EOL)
- Обновления безопасности

Сетевое сопоставление

Discovery соединений

- Соединения TCP/UDP
- Взаимодействия услуг
- Паттерны трафика
- Использование пропускной способности

Сопоставление топологии

- Сегменты сети
- Обнаружение VLAN
- Пути маршрутизации
- Правила межсетевого экрана

Discovery для изменений

Мониторинг в реальном времени

- Изменения конфигурации
- Обновления ПО
- Модификации услуг
- Сетевые изменения

Отслеживание истории

- Временная шкала изменений
- Режимы сравнения
- Путь аудита
- Точки отката

5.6 Автоматизация Discovery

Плановый Discovery

Настройте графики автоматического Discovery в соответствии с вашими потребностями:

- **Полный Discovery**
  - Тип: Полное сканирование инфраструктуры
  - Частота: Еженедельно (рекомендуется)
  - Расписание: Часы минимальной нагрузки (например, воскресенье 02:00)
- **Инкрементальный Discovery**
  - Тип: Только изменения
  - Частота: Ежечасные обновления
  - Цель: Быстрая фиксация изменений конфигурации
- **Критически важные системы**
  - Тип: Целевое сканирование
  - Частота: Каждые 15 минут
  - Фокус: Промышленные серверы и бизнес-критичные системы

Событийный Discovery

- Обнаружение новых устройств
- События DHCP
- Обновления DNS
- Облачное масштабирование

Интеграция через API

RS-Discovery (R-Sight) предоставляет программный доступ к функциям Discovery для автоматизации и интеграции с существующими рабочими процессами. Вы можете запускать сканирования, мониторить прогресс и получать результаты через интерфейс API платформы.

5.7 Производительность и масштабирование

Оптимизация

- Параллельное сканирование
- Интеллектуальное планирование
- Ограничение потребления ресурсов (Throttling)
- Механизмы кэширования

Крупные среды

- Распределенные агенты
- Discovery по зонам
- Инкрементальные обновления
- Балансировка нагрузки

5.8 Безопасность

Управление учетными данными

- Шифрованное хранение
- Интеграция с хранилищем (Vault)
- Политики ротации
- Принцип наименьших привилегий

Сетевая безопасность

- Безопасные протоколы
- Валидация сертификатов
- Проходимость через межсетевые экраны
- Аудиторское логирование

5.9 Поиск и устранение неисправностей

Общие проблемы

- **Ошибки аутентификации:** Проверьте учетные данные, проверьте разрешения, просмотрите правила межсетевого экрана
- **Неполный Discovery:** Увеличьте время ожидания (timeout), проверьте сетевой доступ, просмотрите исключения
- **Влияние на производительность:** Настройте интенсивность сканирования, планируйте на нерабочее время, используйте инкрементальные сканирования

Инструменты отладки Агент Discovery RS-Discovery (R-Sight) включает встроенные диагностические инструменты:

- **Тестирование связности:** Проверка соединения с конкретными узлами перед запуском полного сканирования; подтверждение сетевого доступа и валидности учетных данных.
- **Подробное логирование (Verbose):** Включение детальных журналов; пошаговое отслеживание прогресса Discovery.
- **Режим пробного запуска (Dry Run):** Предварительный просмотр того, что было бы обнаружено, без внесения изменений; валидация конфигураций сканирования перед исполнением.

6 ШАБЛОНЫ ОТЧЕТОВ

RS-Discovery (R-Sight) включает в себя обширную библиотеку готовых шаблонов отчетов, которые помогут вам быстро приступить к работе. Эти шаблоны охватывают распространенные сценарии управления ИТ и могут использоваться как есть или настраиваться под ваши конкретные нужды.

Доступные шаблоны

Отчеты по CMDB и инфраструктуре

Обзор статуса КЕ

- **Описание:** Визуальный обзор всех конфигурационных единиц по их текущему статусу.
- **Визуализация:** Круговая диаграмма, показывающая активные, неактивные и другие статусы.
- **Варианты использования:** Быстрая проверка состояния вашей инфраструктуры.
- **Размер виджета:** 4x3 единицы сетки.
- **Обновление:** Каждые 5 минут.

Распределение типов КЕ

- **Описание:** Разбивка вашей инфраструктуры по типам конфигурационных единиц.
- **Визуализация:** Диаграмма-пончик, показывающая серверы, рабочие станции, ПО и т.д.
- **Варианты использования:** Понимание состава вашей инфраструктуры.
- **Размер виджета:** 4x3 единицы сетки.
- **Обновление:** Каждые 10 минут.

Количество активных КЕ

- **Описание:** Общее количество активных конфигурационных единиц.
- **Визуализация:** Крупный статистический показатель с индикатором тренда.
- **Варианты использования:** Виджет KPI на панели мониторинга, резюме для руководства.
- **Размер виджета:** 3x2 единицы сетки.
- **Обновление:** Каждые 10 минут.

Общее количество КЕ

- **Описание:** Общее количество всех конфигурационных единиц в вашей CMDB.
- **Визуализация:** Карточка статистики с индикатором тренда.
- **Варианты использования:** Панели мониторинга для руководства, обзор инфраструктуры.
- **Размер виджета:** 3x2 единицы сетки.
- **Обновление:** Каждые 10 минут.

Общее количество серверов

- **Описание:** Общее количество серверов в CMDB.
- **Визуализация:** Карточка статистики с числом.
- **Варианты использования:** Метрики инфраструктуры, планирование мощностей.
- **Размер виджета:** 3x2 единицы сетки.
- **Обновление:** Каждые 10 минут.

Общее количество рабочих станций

- **Описание:** Общее количество рабочих станций в CMDB.
- **Визуализация:** Карточка статистики с числом.
- **Варианты использования:** Управление рабочими местами, планирование лицензий.
- **Размер виджета:** 3x2 единицы сетки.
- **Обновление:** Каждые 10 минут.

Отчеты Device Discovery (обнаружение устройств)

Количество устройств по типу

- **Описание:** Общее количество серверов и рабочих станций в CMDB.
- **Визуализация:** Круговая диаграмма, показывающая распределение «Серверы vs Рабочие станции».
- **Варианты использования:** Анализ состава инфраструктуры.
- **Размер виджета:** 4x3 единицы сетки.
- **Обновление:** Каждые 10 минут.

Device Discovery по годам

- **Описание:** Показывает обнаружения устройств, сгруппированные по годам.
- **Визуализация:** Столбчатая диаграмма с годовыми трендами.
- **Варианты использования:** Анализ исторического роста.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Ежемесячная временная шкала Device Discovery

- **Описание:** Ежемесячная разбивка обнаружений устройств.
- **Визуализация:** Линейная диаграмма или диаграмма с областями, показывающая тренды Discovery.
- **Варианты использования:** Анализ паттернов Discovery.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 15 минут.

Device Discovery по дням недели

- **Описание:** Распределение обнаружений по дням недели.
- **Визуализация:** Столбчатая диаграмма, показывающая недельные паттерны.

- **Варианты использования:** Оптимизация расписания.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Недавно обнаруженные устройства

- **Описание:** Список самых последних обнаруженных устройств.
- **Визуализация:** Таблица с деталями устройств.
- **Варианты использования:** Отслеживание новых устройств, проверка постановки на учет.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 5 минут.

Распределение устройств по возрасту

- **Описание:** Показывает возраст устройств на основе даты Discovery.
- **Визуализация:** Столбчатая диаграмма с возрастными диапазонами.
- **Варианты использования:** Планирование обновления парка, управление жизненным циклом.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Отчеты по операционным системам

Распределение операционных систем

- **Описание:** Показывает устройства, сгруппированные по ОС.
- **Визуализация:** Столбчатая диаграмма (Windows 11, Windows 10, Linux и т.д.).
- **Варианты использования:** Стандартизация ОС, планирование обновлений.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 10 минут.

Матрица распределения ОС — Все устройства

- **Описание:** Всеобъемлющее распределение ОС по всем устройствам.
- **Визуализация:** Матрица/Таблица с подробными версиями.
- **Варианты использования:** Детальная инвентаризация ОС.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Матрица распределения ОС — Серверы

- **Описание:** Распределение ОС только для серверов.
- **Визуализация:** Матрица/Таблица с деталями серверных ОС.
- **Варианты использования:** Планирование стандартизации серверов.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Матрица распределения ОС — Рабочие станции

- **Описание:** Распределение ОС только для рабочих станций.
- **Визуализация:** Матрица/Таблица с деталями ОС рабочих станций.
- **Варианты использования:** Управление десктопными ОС.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Отчеты по оборудованию

Распределение памяти серверов

- **Описание:** Распределение объема памяти по серверам.
- **Визуализация:** Столбчатая диаграмма, сгруппированная по диапазонам памяти (4ГБ, 8ГБ, 16ГБ и т.д.).
- **Варианты использования:** Планирование мощностей, выявление необходимости апгрейда.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Распределение памяти рабочих станций

- **Описание:** Распределение объема памяти по рабочим станциям.
- **Визуализация:** Столбчатая диаграмма, сгруппированная по диапазонам памяти.
- **Варианты использования:** Планирование апгрейда десктопов.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Распределение типов дисков

- **Описание:** Распределение типов дисков (SSD, HDD, NVMe).
- **Визуализация:** Круговая/Столбчатая диаграмма, показывающая типы хранилищ.
- **Варианты использования:** Планирование модернизации хранилищ.
- **Размер виджета:** 4x3 единицы сетки.
- **Обновление:** Каждые 30 минут.

КЕ рабочих станций по названию модели

- **Описание:** Распределение рабочих станций по производителю и модели.
- **Визуализация:** Столбчатая диаграмма топовых моделей.
- **Варианты использования:** Стандартизация оборудования.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Отчеты по управлению программными активами (SAM)

Самое устанавливаемое ПО

- **Топ-20 самых устанавливаемых программ:**
  - **Описание:** Показывает 20 наиболее часто встречающихся программ на всех серверах и рабочих станциях.

- **Визуализация:** Столбчатая диаграмма с количеством установок.
- **Варианты использования:** Выявление популярного ПО, возможности для стандартизации.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Самое устанавливаемое ПО по семействам

- **Описание:** Установки ПО, сгруппированные по семействам (Базы данных, Безопасность, Разработка и т.д.).
- **Визуализация:** Диаграмма-пончик, показывающая распределение по семействам.
- **Варианты использования:** Анализ портфеля ПО, управление категориями.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Тренды установки ПО

- **Описание:** Ежемесячный тренд установок ПО за последние 6 месяцев.
- **Визуализация:** Линейная диаграмма, показывающая паттерны установки.
- **Варианты использования:** Анализ роста, отслеживание развертывания.
- **Размер виджета:** 8x3 единицы сетки.
- **Обновление:** Каждые 60 минут.

Лицензии и Compliance

- **Обзор лицензий и Compliance:**
  - **Описание:** Сравнение лицензионных и нелицензионных установок ПО.
  - **Визуализация:** Статистика в процентах с цветовой кодировкой порогов.
  - **Варианты использования:** Мониторинг соответствия, готовность к аудиту.
  - **Размер виджета:** 3x2 единицы сетки.
  - **Обновление:** Каждые 10 минут.

Временная шкала истечения лицензий

- **Описание:** Предстоящие истечения лицензий в ближайшие 90 дней.
- **Визуализация:** Таблица с указанием ПО, вендора, даты истечения и оставшихся дней.
- **Варианты использования:** Планирование продлений, прогнозирование бюджета.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Инвентаризация ПО

- **Общее количество экземпляров ПО:**

- **Описание:** Общее число отслеживаемых установок программного обеспечения.
- **Визуализация:** Карточка статистики с числом.
- **Варианты использования:** Обзор управления лицензиями.
- **Размер виджета:** 3x2 единицы сетки.
- **Обновление:** Каждые 10 минут.

Распределение версий ПО

- **Описание:** Распределение версий программного обеспечения в инфраструктуре.
- **Визуализация:** Стековая столбчатая диаграмма, сгруппированная по ПО и версии.
- **Варианты использования:** Стандартизация версий, планирование обновлений.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Несопоставленные экземпляры ПО

- **Описание:** Экземпляры ПО без привязки к каталогу.
- **Визуализация:** Таблица с именем, хостом, датой обнаружения и статусом.
- **Варианты использования:** Улучшение Discovery, ведение каталога.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 10 минут.

Распределение программного обеспечения баз данных

- **Описание:** Показывает все ПО баз данных, установленное в инфраструктуре.
- **Визуализация:** Столбчатая диаграмма (SQL Server, Oracle, MySQL, PostgreSQL и т.д.).
- **Варианты использования:** Лицензирование баз данных, стандартизация.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Программное обеспечение по вендорам

- **Описание:** Распределение ПО, сгруппированное по производителям.
- **Визуализация:** Столбчатая/Круговая диаграмма распределения вендоров.
- **Варианты использования:** Управление поставщиками, консолидация.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Безопасность и Compliance

Программное обеспечение с истекшим сроком эксплуатации

- **Описание:** ПО, которое достигло или приближается к завершению жизненного цикла.
- **Визуализация:** Таблица с ПО, версией, датой EOL, статусом и количеством установок.
- **Варианты использования:** Управление рисками безопасности, планирование обновлений.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Уязвимое ПО (на основе CPE)

- **Описание:** Программное обеспечение с известными уязвимостями на основе данных CPE.
- **Визуализация:** Горизонтальная столбчатая диаграмма, показывающая количество уязвимостей.
- **Варианты использования:** Устранение угроз безопасности, управление патчами.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Оценка стандартизации ПО

- **Описание:** Измеряет соблюдение утвержденных стандартов программного обеспечения.
- **Визуализация:** Процентный показатель с индикатором тренда.
- **Варианты использования:** Метрики управления, отслеживание соответствия.
- **Размер виджета:** 3x2 единицы сетки.
- **Обновление:** Каждые 10 минут.

Оптимизация затрат

Анализ дублирующегося ПО

- **Описание:** Выявление дубликатов установленного ПО, которые можно консолидировать.
- **Визуализация:** Таблица с ПО, сервером, количеством дублей и потенциальной экономией.
- **Варианты использования:** Снижение затрат, оптимизация лицензий.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Траты на ПО по вендорам

- **Описание:** Общие расходы на ПО, сгруппированные по поставщикам.
- **Визуализация:** Круговая диаграмма распределения трат.
- **Варианты использования:** Управление вендорами, анализ бюджета.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 60 минут.

Операционные KPI

Охват Discovery для программного обеспечения

- **Описание:** Процент экземпляров ПО, успешно сопоставленных с каталогом.
- **Визуализация:** Индикатор (Gauge) с цветовой кодировкой порогов (Хорошо: выше 80%, Предупреждение: 60-80%, Критично: ниже 60%).
- **Варианты использования:** Эффективность Discovery, качество данных.
- **Размер виджета:** 3x3 единицы сетки.
- **Обновление:** Каждые 10 минут.

Новые обнаружения ПО (за последние 30 дней)

- **Описание:** Недавно обнаруженные экземпляры программного обеспечения.
- **Визуализация:** Список с названием, вендором, версией и датой Discovery.
- **Варианты использования:** Отслеживание изменений, идентификация нового ПО.
- **Размер виджета:** 4x4 единицы сетки.
- **Обновление:** Каждые 10 минут.

Отчеты по управлению услугами

Открытые запросы по приоритетам

- **Описание:** Текущие открытые запросы на обслуживание, сгруппированные по уровню приоритета.
- **Визуализация:** Столбчатая диаграмма (Высокий, Средний, Низкий приоритет).
- **Варианты использования:** Управление Service Desk, планирование нагрузки.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 5 минут.

Сводка статусов задач

- **Описание:** Обзор показателей выполнения задач по всем проектам.
- **Визуализация:** Таблица, показывающая количество и процентное соотношение статусов.
- **Варианты использования:** Управление проектами, распределение ресурсов.
- **Размер виджета:** 4x3 единицы сетки.
- **Обновление:** Каждые 5 минут.

Сетевые отчеты

Количество оборудования по диапазонам IP

- **Описание:** Распределение устройств по IP-диапазонам.

- **Визуализация:** Столбчатая диаграмма и таблица, показывающая количество устройств на подсеть.
- **Варианты использования:** Планирование сети, анализ сегментации.
- **Размер виджета:** 8x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Распределение IP-подсетей

- **Описание:** Визуальное представление использования сетевых подсетей.
- **Визуализация:** Столбчатая диаграмма количества устройств на подсеть.
- **Варианты использования:** Планирование сетевых мощностей.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Операции и мониторинг

Последние действия

- **Описание:** Список последних системных действий и изменений.
- **Визуализация:** Прокручиваемый список с временными метками и описаниями.
- **Варианты использования:** Управление изменениями, путь аудита.
- **Размер виджета:** 4x4 единицы сетки.
- **Обновление:** Каждую 1 минуту.

Оценка актуальности данных CMDB

- **Описание:** Показывает, насколько недавно обновлялись данные о КЕ.
- **Визуализация:** Карточка оценки с метриками актуальности.
- **Варианты использования:** Мониторинг качества данных.
- **Размер виджета:** 4x3 единицы сетки.
- **Обновление:** Каждые 15 минут.

Обнаружение устаревших КЕ

- **Описание:** Выявляет КЕ, которые давно не обновлялись.
- **Визуализация:** Таблица со списком потенциально неактуальных КЕ.
- **Варианты использования:** Управление качеством данных.
- **Размер виджета:** 6x4 единицы сетки.
- **Обновление:** Каждые 30 минут.

Использование шаблонов

Запуск шаблона

1. Перейдите в **Отчеты → Шаблоны**.
2. Найдите нужный шаблон.
3. Нажмите **Предпросмотр**, чтобы увидеть пример данных.
4. Нажмите **Запустить отчет**, чтобы сгенерировать его на основе «живых» данных.

5. Экспортируйте или добавьте на панель мониторинга при необходимости.

Настройка шаблонов

1. Откройте шаблон, который хотите изменить.
2. Нажмите **Редактировать** или **Создать копию**.
3. Настройте фильтры, диапазоны дат или визуализации.
4. Сохраните как новый пользовательский шаблон.
5. Поделитесь с командой.

Добавление на панели мониторинга

1. В любом шаблоне нажмите **Добавить на панель мониторинга**.
2. Выберите существующую панель или создайте новую.
3. Разместите и измените размер виджета.
4. Настройте интервалы обновления.
5. Сохраните панель мониторинга.

Конфигурация шаблона

Источники данных

Шаблоны могут получать данные из:

- **CMDB:** Конфигурационные единицы и связи.
- **Запросы на обслуживание:** Данные назначений и рабочих процессов.
- **Системные события:** Логи действий и изменений.
- **Метрики производительности:** Данные об использовании ресурсов.

Примечание: Интеграция с внешними API запланирована в будущих релизах.

Опции визуализации

- **Диаграммы:** Столбчатые, линейные, круговые, пончики, с областями, точечные.
- **Таблицы:** Сортируемые и фильтруемые сетки данных.
- **Статистика:** Числа KPI с трендами.
- **Списки:** Последние действия и предупреждения (алерты).
- **Индикаторы (Gauges):** Индикаторы прогресса и пороговые значения.

Настройка фильтров

- **Диапазоны дат:** Последние 7 дней, 30 дней, произвольные периоды.
- **Департаменты:** Фильтрация по организационным единицам.
- **Типы устройств:** Серверы, рабочие станции, сетевые устройства.
- **Статус:** Активен, неактивен, обслуживание.
- **Категории:** Пользовательские группы и теги.

Продвинутые функции

Шаблоны с поддержкой ИИ

Многие шаблоны включают функции на базе искусственного интеллекта:

- **Smart Insights:** Автоматизированный анализ и рекомендации.
- **Обнаружение аномалий:** Выявление необычных паттернов.
- **Анализ трендов:** Прогнозирование будущих значений.
- **Естественный язык:** Резюме на обычном языке.

Возможности детализации (Drill-Down)

Нажмите на элементы диаграммы, чтобы:

- Увидеть детальные данные.
- Отфильтровать по конкретным категориям.
- Перейти к связанным отчетам.
- Экспортировать подмножество данных.

7 ОТЧЕТНОСТЬ И АНАЛИТИКА

RS-Discovery (R-Sight) предоставляет мощные возможности отчетности и аналитики, которые помогут вам понять вашу ИТ-инфраструктуру, отслеживать операции и принимать решения на основе данных. Независимо от того, нужны ли вам быстрые выводы или детальный анализ, наша гибкая система отчетности обеспечит вас всем необходимым.

Обзор

Система отчетности сочетает в себе готовые шаблоны с настраиваемой аналитикой для предоставления практически значимой информации. Все отчеты можно просматривать в приложении, экспортировать в различные форматы или добавлять на панели управления для мониторинга в реальном времени.

С чего начать

Доступ к отчетам

- Перейдите в раздел **Отчеты** в главном меню.
- Просмотрите **Шаблоны отчетов**, чтобы увидеть доступные варианты.
- Нажмите **Создать шаблон**, чтобы собрать собственный отчет.
- Используйте **Предпросмотр**, чтобы увидеть пример данных перед запуском.

Ваш первый отчет

1. Выберите предопределенный шаблон (например, «Обзор статуса КЕ»).
2. Нажмите **Предпросмотр**, чтобы увидеть пример данных.
3. Нажмите **Запустить отчет**, чтобы сгенерировать его на основе «живых» данных.
4. Экспортируйте в PDF или Excel при необходимости.

Шаблоны отчетов

Предопределенные шаблоны Готовые к использованию шаблоны для распространенных задач:

- **Отчеты CMDB**
  - Обзор статуса КЕ — круговая диаграмма активных и неактивных единиц.
  - Распределение типов КЕ — диаграмма-пончик вашей инфраструктуры по типам (серверы, рабочие станции и т. д.).
  - Количество активных КЕ — виджет KPI с общим числом активных объектов.
- **Управление услугами**
  - Открытые запросы по приоритетам — столбчатая диаграмма запросов в Service Desk.
  - Сводка статусов задач — таблица с показателями выполнения задач.
  - Последние действия — список последних изменений и действий в системе.
- **Операции и мониторинг**
  - Устройства по операционным системам — распределение Windows, Linux и других типов ОС.
  - Временная шкала Discovery — данные о том, когда устройства сканировались и обновлялись в последний раз.
  - Инвентаризация ПО — приложения и лицензии во всей вашей инфраструктуре.

Пользовательские шаблоны

Создавайте собственные отчеты с помощью нашего интуитивно понятного конструктора:

- **Выбор источника данных** — CMDB, события, метрики или внешние API.
- **Выбор визуализации** — диаграммы, таблицы, индикаторы или статистика.
- **Настройка фильтров** — диапазоны дат, департаменты, типы устройств.
- **Дизайн макета** — перетаскивание компонентов (drag-and-drop) для создания структуры.

Типы визуализации

Диаграммы и графики

- **Столбчатые диаграммы** — сравнение значений по категориям.
- **Линейные графики** — отображение трендов во времени.
- **Круговые/пончиковые диаграммы** — отображение пропорций и распределений.
- **Диаграммы с областями** — визуализация изменений объема.
- **Точечные диаграммы** — выявление корреляций.
- **Тепловые карты** — отображение плотности данных и паттернов.

Отображение данных

- **Таблицы** — детальные данные с сортировкой и фильтрацией.
- **Списки** — последние действия, алерты и уведомления.
- **Статистика** — ключевые показатели эффективности (KPI).
- **Индикаторы (Gauges)** — индикаторы прогресса и пороговые значения.
- **Карточки** — блоки с краткой сводной информацией.

Интерактивные функции

- **Детализация (Drill-down)** — клик по диаграмме для перехода к детальным данным.
- **Фильтрация** — сужение результатов по критериям.
- **Сортировка** — организация данных по любому столбцу.
- **Экспорт** — выгрузка в PDF, Excel или CSV.

Панели мониторинга (Dashboards)

Создание панелей мониторинга

1. Перейдите в **Панели мониторинга** и нажмите **Новая панель**.
2. Выберите шаблон или начните с чистого листа.
3. Добавьте виджеты: выбирая из шаблонов отчетов или создавая пользовательские виджеты.
4. Перетаскивайте и меняйте размер виджетов для настройки макета.
5. Сохраните и поделитесь с командой.

Типы панелей мониторинга

- **Личные** — ваша приватная панель.
- **Командные** — доступные конкретным командам.
- **Системные** — общие панели для всей компании.

Опции виджетов

- **Автообновление** — обновление данных каждые 1–15 минут.
- **Диапазоны дат** — последние 7 дней, 30 дней или произвольный период.
- **Адаптивный размер** — автоматическая подстройка под размер экрана.
- **Стилизация** — настройка цветов, шрифтов и тем.

Отчетность с поддержкой ИИ

Интеллектуальная аналитика

Наш ИИ анализирует ваши данные и предоставляет:

- **Анализ трендов** — «Использование CPU серверов выросло на 15% в этом месяце».
- **Обнаружение аномалий** — «Обнаружен необычный сетевой трафик на серверах БД».
- **Рекомендации** — «Рассмотрите возможность увеличения памяти на этих 5 серверах».
- **Оценка влияния** — «Критично: 3 сервера влияют на 12 бизнес-услуг».

Запросы на естественном языке

Задавайте вопросы на обычном языке:

- «Покажи все Windows-серверы с высокой загрузкой CPU».
- «Какие приложения установлены на наибольшем количестве устройств?».
- «Какие изменения были внесены в серверы баз данных на прошлой неделе?».

Планирование и рассылка

Планирование отчетов

Настройте автоматическую доставку отчетов:

1. Откройте любой шаблон отчета.
2. Нажмите **Запланировать**.
3. Выберите частоту (ежедневно, еженедельно, ежемесячно).
4. Выберите получателей.
5. Выберите формат (PDF, Excel, Email).

Варианты рассылки

- **Email** — отправка отдельным лицам или группам.
- **Общие папки** — сохранение в сетевые папки.
- **API** — интеграция с другими системами.

Форматы экспорта

- **PDF** — профессиональные отчеты с графиками и форматированием.
- **Excel** — необработанные данные для анализа и сводных таблиц.
- **CSV** — простой экспорт данных для интеграции.
- **HTML** — интерактивные веб-отчеты.

Разрешения и безопасность

Контроль доступа

- **Владелец** — полный контроль над отчетом.
- **Редактор** — может изменять и запускать отчеты.
- **Зритель** — может только просматривать и экспортировать отчеты.

Безопасность данных

- **Изоляция клиентов** — каждый департамент видит только свои данные.
- **Доступ на основе ролей** — разные представления для разных ролей.
- **Путь аудита** — отслеживание того, кто и когда обращался к отчетам.

8 АВТОМАТИЗАЦИЯ РАБОЧИХ ПРОЦЕССОВ

Оптимизируйте ИТ-операции с помощью интеллектуальной автоматизации рабочих процессов.

Обзор

Автоматизация рабочих процессов в RS-Discovery (R-Sight) позволяет организациям создавать, управлять и оптимизировать ИТ-процессы с помощью визуального проектирования, условной логики и бесшовных интеграций.

Типы рабочих процессов

Рабочие процессы запросов на обслуживание

- Прием на работу новых сотрудников (Onboarding)
- Предоставление доступа
- Запросы на программное обеспечение
- Распределение оборудования

Управление изменениями

- Согласование изменений
- Оценка рисков и влияния
- Отслеживание внедрения
- Процедуры отката

Реагирование на инциденты

- Маршрутизация предупреждений
- Пути эскалации
- Отслеживание разрешения инцидента
- Анализ после инцидента

Рабочие процессы обслуживания

- Циклы установки исправлений (патчей)
- Верификация резервного копирования
- Обновление сертификатов
- Проверки на соответствие нормативным требованиям (compliance)

Действия

Системные действия

- Выполнение скриптов
- Вызовы API
- Запросы к базам данных
- Операции с файлами

Интеграционные действия

- Создание назначений
- Отправка уведомлений
- Обновление CMDB
- Вызов webhook

ИИ-действия

- Анализ данных
- Генерация аналитики
- Принятие решений
- Прогнозирование результатов

Управление согласованиями

Типы согласований

- Один согласующий
- Несколько согласующих
- Иерархическое согласование
- На основе голосования

Интерфейс согласования

- Email-уведомления
- Мобильное приложение
- Веб-портал
- Интеграция через API

Мониторинг и аналитика

Метрики рабочих процессов

- Время выполнения
- Процент успеха
- «Узкие места»
- Соблюдение SLA

Анализ процессов

- Обнаружение паттернов
- Выявление неэффективности
- Оптимизация путей
- Прогнозирование задержек

9 МОДУЛИ CMDB

Обзор CMDB

База данных управления конфигурациями (CMDB) — это центральное хранилище всех компонентов вашей ИТ-инфраструктуры, их атрибутов и связей. CMDB в RS-Discovery (R-Sight) предлагает аналитику на базе ИИ и автоматизированный **Discovery** для поддержания точного и актуального представления о всем вашем ИТ-ландшафте в режиме реального времени.

Что такое CMDB?

База данных управления конфигурациями хранит информацию о конфигурационных единицах (КЕ) — любом компоненте, которым необходимо управлять для предоставления ИТ-услуги. Сюда входят:

- **Оборудование:** Серверы, рабочие станции, сетевые устройства, системы хранения данных.
- **Программное обеспечение:** Приложения, операционные системы, базы данных, промежуточное ПО.
- **Связи:** Зависимости и соединения между компонентами.
- **Документация:** Лицензии, контракты, процедуры, политики.

Ключевые функции

Автоматизированный Discovery

- Мультипротокольное сканирование (WMI, SSH, SNMP)
- Агентный и безагентный **Discovery**
- Синхронизация в реальном времени
- Обнаружение и отслеживание изменений

Интеллект на базе ИИ

- Автоматическая классификация КЕ
- Вывод связей (инференс)
- Обнаружение аномалий
- Прогнозная аналитика

Всеобъемлющее отслеживание

- Спецификации оборудования и жизненный цикл
- Инвентаризация ПО и лицензирование
- Сетевая топология и зависимости
- Картирование бизнес-услуг

Compliance и безопасность

- Интеграция оценки уязвимостей
- Контроль доступа и путь аудита
- Шифрование при хранении и передаче

Типы КЕ

RS-Discovery (R-Sight) поддерживает различные типы конфигурационных единиц:

Инфраструктурные КЕ

- **Серверы:** Физические и виртуальные серверы.
- **Рабочие станции:** Настольные ПК и ноутбуки.
- **Сетевые устройства:** Маршрутизаторы, коммутаторы, межсетевые экраны.

Программные КЕ

- **Операционные системы:** Windows, Linux, варианты Unix.
- **Приложения:** Бизнес-приложения, утилиты.
- **Базы данных:** РСУБД, NoSQL, хранилища данных.
- **Промежуточное ПО:** Веб-серверы, серверы приложений, очереди сообщений.

КЕ услуг

- **Бизнес-услуги:** Услуги, ориентированные на клиента.
- **Технические услуги:** Инфраструктурные услуги.
- **Компоненты услуг:** Строительные блоки услуг.

Преимущества

1. **Единый источник истины:** Централизованное хранилище всех ИТ-активов; согласованность данных между командами.
2. **Анализ влияния:** Понимание зависимостей перед внесением изменений; минимизация простоев услуг.
3. **Оптимизация затрат:** Отслеживание использования лицензий; выявление недогруженных ресурсов.
4. **Compliance и управление:** Автоматическая проверка нормативных требований; ведение пути аудита.

С чего начать

1. **Определите область действия:** Определите критические бизнес-услуги и типы КЕ для отслеживания.
2. **Настройте Discovery:** Разверните агентов, настройте учетные данные и расписание сканирования.
3. **Установите связи:** Сопоставьте зависимости услуг и определите правила влияния на бизнес.
4. **Включите функции ИИ:** Настройте автоматические инсайты и обнаружение аномалий.

10 УПРАВЛЕНИЕ ОБОРУДОВАНИЕМ

Управление оборудованием в CMDB RS-Discovery (R-Sight) обеспечивает комплексное отслеживание всех физических и виртуальных компонентов инфраструктуры. Благодаря аналитике на базе ИИ и интеллектуальной категоризации вы можете поддерживать точную видимость всего вашего парка оборудования в режиме реального времени.

Типы КЕ оборудования

Серверы Физические и виртуальные серверы, включая:

- **Физические серверы:** Стоечные, блейд-серверы, башенные серверы.
- **Виртуальные машины:** VMware, Hyper-V, KVM, облачные экземпляры.
- **Контейнеры:** Контейнеры Docker, поды Kubernetes.
- **Облачные экземпляры**

Рабочие станции Вычислительные устройства конечных пользователей:

- **Настольные ПК:** Традиционные компьютеры.
- **Ноутбуки:** Портативные компьютеры.
- **Тонкие клиенты:** Zero- и тонкие клиенты.
- **Мобильные устройства:** Планшеты, смартфоны.

Сетевые устройства Компоненты сетевой инфраструктуры:

- **Маршрутизаторы:** Магистральные, пограничные и маршрутизаторы филиалов.
- **Коммутаторы:** Ядра, распределения и доступа.
- **Межсетевые экраны:** Аппаратные экраны, устройства UTM.
- **Балансировщики нагрузки:** Контроллеры доставки приложений.
- **Беспроводная связь:** Точки доступа, контроллеры беспроводной сети.

Системы хранения данных Инфраструктура хранения данных:

- **SAN:** Массивы сетей хранения данных.
- **NAS:** Сетевые хранилища.
- **Резервное копирование:** Ленточные библиотеки, устройства бэкапа.
- **Облачное хранение:** Объектные и блочные хранилища.

Атрибуты оборудования

Основные атрибуты

Каждая КЕ оборудования включает:

- **Базовая информация:** Имя (уникальный ID), серийный номер, инвентарный номер, модель, производитель, местоположение, статус (Активен, Неактивен, Списан).
- **Технические характеристики:** Тип процессора (CPU), ядра, частота; объем памяти (RAM), тип; емкость дисков, тип, RAID; сетевые адаптеры, MAC-адреса, IP; конфигурация блоков питания; версия BIOS/UEFI.

Расширенные атрибуты

Дополнительные возможности отслеживания:

- **Жизненный цикл:** Дата покупки, гарантия (даты начала/окончания, покрытие), лизинг, даты окончания эксплуатации/поддержки (EOL/EOS), плановая дата обновления.
- **Финансовая информация:** Цена покупки, текущая стоимость (с учетом амортизации), стоимость обслуживания, расчет совокупной стоимости владения (TCO).

- **Параметры среды:** Энергопотребление (Ватт/BTU), требования к охлаждению, позиция в стойке (U), физический вес.

Методы Discovery

Агентный Discovery

- **Агент для Windows собирает:** Данные WMI, реестр, сетевую конфигурацию, установленное ПО, запущенные процессы, логи событий.
- **Агент для Linux собирает:** Данные DMI/SMBIOS, информацию о CPU и памяти, данные о PCI и USB устройствах, сетевые интерфейсы, конфигурацию дисков, системные логи.

Безагентный Discovery

- **Сканирование SNMP:** Описание системы, информация об интерфейсах, загрузка CPU/памяти, датчики среды, статус компонентов.
- **Интеграция с VMware vSphere:** Конфигурация VM, распределение ресурсов, сопоставление с хостами, использование хранилищ, сетевые назначения.

Автоматизированные рабочие процессы

- **Постановка нового оборудования на учет:** Автоматический **Discovery** при подключении к сети, классификация типа оборудования с помощью ИИ, автозаполнение характеристик, картирование связей с услугами.
- **Планирование обновления (Refresh):** ИИ-рекомендации на основе возраста оборудования, статуса гарантии и метрик производительности.

Анализ влияния

При управлении оборудованием RS-Discovery (R-Sight) автоматически:

- Сопоставляет зависимые услуги.
- Рассчитывает влияние на бизнес.
- Выявляет пробелы в резервировании.
- Предлагает стратегии по минимизации рисков.

Отчеты по оборудованию

- **Инвентаризация:** Полный список, сводка характеристик, карта размещения, анализ возраста.
- **Статус гарантии:** Истекающие гарантии, устройства без поддержки, рекомендации по продлению.
- **Планирование мощностей:** Тренды использования ресурсов, прогнозы роста, выявление «узких мест».
- **Инсайты ИИ:** Например, выявление серверов с низкой загрузкой (<20%) для последующей консолидации.

11 УПРАВЛЕНИЕ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

Управление программным обеспечением в RS-Discovery (R-Sight) обеспечивает полную видимость и контроль над вашими программными активами — от обнаружения до обеспечения compliance. Благодаря интеллектуальным функциям на базе ИИ и автоматизированным процессам вы можете оптимизировать затраты, гарантировать соблюдение лицензионных соглашений и поддерживать актуальную инвентаризацию ПО.

Обзор

Управление программным обеспечением в RS-Discovery (R-Sight) помогает вам:

- **Автоматически обнаруживать** все установки ПО во всей вашей инфраструктуре.
- **Нормализовать** названия и версии программ с помощью ИИ для единообразия.
- **Отслеживать лицензии** и обеспечивать соответствие соглашениям с вендорами.
- **Оптимизировать затраты**, выявляя неиспользуемые или недостаточно используемые лицензии.
- **Управлять жизненным циклом ПО** от развертывания до вывода из эксплуатации.

Инвентаризация программного обеспечения

Иерархия ПО

RS-Discovery (R-Sight) организует программное обеспечение на трех иерархических уровнях:

1. **Семейства ПО (Software Families)** Группы связанных продуктов от одного вендора или со схожими функциями (например, *Microsoft Office*, *Adobe Creative Suite*, *Системы БД*).
2. **Программные продукты (Software Products)** Конкретные рыночные наименования (например, *Microsoft Excel*, *Adobe Photoshop*). Включают определения продуктов, не зависящие от версии, и модели лицензирования.
3. **Экземпляры ПО (Software Instances)** Фактические установки, обнаруженные в вашей инфраструктуре. Включают конкретные версии, даты установки, пути и паттерны использования.

Процесс Discovery программного обеспечения

RS-Discovery (R-Sight) использует несколько методов для автоматического сбора данных:

- **Агентный Discovery:** Сканирование реестра Windows, опрос менеджеров пакетов Linux, идентификация запущенных процессов и услуг.
- **Нормализация на базе ИИ:** Стандартизация различных вариаций написания имен, автоматическое сопоставление с глобальным каталогом и определение семейств.

- **Автоматическая классификация:** Категоризация по типам (ОС, БД, утилиты), определение критичности и привязка к базам данных уязвимостей.

Глобальный каталог программного обеспечения

Глобальный каталог — это эталонный справочник вашей организации, содержащий:

- **Каталоги вендоров:** Официальные списки ПО от крупнейших производителей.
- **Внутренние стандарты:** Список разрешенного ПО в вашей компании.
- **Определения лицензий:** Стандартные типы и условия лицензирования.
- **Интеграция безопасности:** Уведомления об окончании срока поддержки и рекомендации по безопасности.

Управление лицензиями

RS-Discovery (R-Sight) поддерживает все распространенные модели лицензирования:

- **На устройство (Per Device):** Одна лицензия на одну машину (физическую или виртуальную).
- **На пользователя (Per User):** Лицензия закрепляется за конкретным пользователем (типично для SaaS).
- **На ядро/процессор (Per Core/Processor):** На основе характеристик серверного оборудования.
- **Конкурентные лицензии (Concurrent):** Ограничение по количеству одновременных пользователей.
- **Подписка (Subscription):** Право доступа на определенный период времени.

Политики ПО (Черные и белые списки)

Политики позволяют контролировать использование ПО в организации:

- **Черные списки (Blacklisting):** Идентификация опасного, нелицензионного или устаревшего ПО. При обнаружении система может отправить алерт, создать запрос или инициировать удаление.
- **Белые списки (Whitelisting):** Определение стандартов ПО для конкретных департаментов или всей компании.
- **Управление исключениями:** Возможность временного или постоянного разрешения ПО для специфических задач (например, инструментов разработки) с фиксацией бизнес-обоснования.

Оптимизация и отчетность

Система предоставляет глубокую аналитику для снижения затрат:

- **Сбор лицензий (License Harvesting):** Выявление установленного, но не используемого ПО для перераспределения лицензий.

- **Анализ дубликатов:** Поиск схожих по функционалу инструментов для консолидации парка ПО.
- **Готовые отчеты:** Инвентаризационные описи, отчеты о лицензионном соответствии нормативным требованиям (Compliance Report) и анализ расходов по вендорам.

12 ДОКУМЕНТАЦИЯ СИСТЕМЫ СВЯЗЕЙ КЕ

Обзор

Система связей КЕ в RS-Discovery (R-Sight) обеспечивает интеллектуальное картирование сетевых соединений между конфигурационными единицами (КЕ) для автоматического обнаружения и поддержания зависимостей услуг. Система использует архитектуру двунаправленных связей, которая гарантирует согласованность данных и точное определение направления трафика.

Основные концепции

Двунаправленные связи

В отличие от традиционных систем, создающих отдельные записи о связях для каждой КЕ, RS-Discovery (R-Sight) использует единый объект связи для каждой пары соединений. Этот подход:

- Предотвращает дублирование связей между одними и теми же КЕ.
- Обеспечивает согласованность данных при многократном сканировании.
- Снижает избыточность данных в CMDB.
- Предоставляет двойную перспективу через атрибуты sourceView (представление со стороны источника) и targetView (представление со стороны цели).

Определение направления

Система использует иерархический подход для определения корректного направления связи:

1. **Реестр ListeningService** (высший приоритет).
2. **Анализ состояния соединения** (состояние LISTEN).
3. **Обнаружение общеизвестных портов** (Well-Known Ports).
4. **Классификация диапазонов портов** (динамические порты против зарегистрированных).
5. **Детерминированный откат** (по меньшему номеру порта).
6. **Алфавитный порядок** (крайний случай).

Архитектура

Модель данных

Каждая связь КЕ отслеживает следующую информацию:

- **Идентификация соединения:** Исходная и целевая КЕ, тип связи (обычно «Connected To»), протокол (TCP/UDP).
- **Перспектива источника:** Имя процесса и ID, инициирующего соединение; локальные и удаленные порты; счетчик соединений.
- **Перспектива цели:** Процесс, принимающий соединение; PID; порты и метаданные.
- **Определение направления:** Уровень достоверности (высокий/средний/низкий/предположение), обоснование направления, признак двунаправленности.

Алгоритм определения направления

1. Проверка ListeningService

Система в первую очередь проверяет, зарегистрирован ли какой-либо из портов как «слушающий сервис» (listening service). Например, если кастомный экземпляр SQL Server настроен на прослушивание порта 1440 или 1488, эти порты

регистрируются в системе. **Результат:** КЕ со слушающим портом становится целевым объектом (получателем/target).

2. Анализ состояния соединения

Для соединений, содержащих информацию о состоянии:

- **State = 2 (LISTEN):** КЕ является целью (target).
- **State = 5 (ESTABLISHED):** Требуется дальнейший анализ.
- **State = 11 (TIME_WAIT):** КЕ, скорее всего, была источником (source).

3. Общеизвестные порты (Well-Known Ports)

Стандартные сервисные порты указывают на серверную сторону. К ним относятся:

- Порт 21 (FTP)
- Порт 22 (SSH)
- Порт 80 (HTTP)
- Порт 443 (HTTPS)
- Порт 1433 (SQL Server)
- Порт 1521 (Oracle)
- Порт 3306 (MySQL)
- Порт 5432 (PostgreSQL)
- И многие другие. **Результат:** КЕ с общеизвестным портом становится целевым объектом (target).

4. Классификация диапазонов портов

- **Зарегистрированные порты (1024–49151):** Вероятные сервисы.
- **Динамические порты (49152–65535):** Клиентские соединения.

Пример: КЕ1 использует порт 50123 (динамический) → КЕ2 использует порт 8080 (зарегистрированный). **Направление:** КЕ1 — источник (source), КЕ2 — цель (target).

5. Соединения без «слушателя» (Non-Listener Connections)

Для соединений типа peer-to-peer или RPC, где ни одна из сторон не находится в состоянии прослушивания, система применяет резервные правила. Например:

- Две КЕ соединяются через порты 48765 и 49123 (оба динамические).
- Listening service не обнаружен ни на одной из сторон.
- Система предполагает, что меньший номер порта (48765) представляет сервис.

Направление определяется так: КЕ с портом 49123 — источник (source), КЕ с портом 48765 — цель (target). Уровень достоверности (Confidence) помечается как «низкий» (low) или «предположение» (guess).

Детали реализации

Ключевые функции

Функция определения направления Система использует основную функцию, которая анализирует две КЕ и данные их соединений для применения иерархических правил определения направления.

Анализируемая информация:

- Объект первой КЕ и данные её соединений.
- Объект второй КЕ (если известна) и данные её соединений.
- ID тенанта для поиска сервисов в реестре.

Предоставляемый результат:

- Идентифицированная КЕ-источник (source).
- Идентифицированная КЕ-цель (target).
- Уровень достоверности (высокий, средний, низкий или предположение).
- Обоснование того, почему было выбрано именно это направление.
- Признак того, является ли соединение двунаправленным.

Ключевая логика:

- Поиск связи в обоих направлениях.
- Корректировка направления, если существующая связь была инвертирована.
- Обработка неизвестных устройств с использованием идентификаторов.

Обновление представления связей

Обновляет соответствующее представление (sourceView или targetView) в зависимости от роли сканируемой КЕ.

Возможности:

- Агрегирует несколько соединений с одной и той же конечной точкой.
- Сохраняет исторические данные (порты, процессы).
- Ведет счетчик количества соединений.
- Хранит детали последних соединений (до 100 записей).
- Обогащает данные информацией о приложении.
- Добавляет метаданные о семействе ПО.

История соединений

Система хранит историю до **100 последних соединений** для каждой связи. Каждая запись о соединении фиксирует:

- Локальные и удаленные адреса.
- Используемые локальные и удаленные порты.
- Протокол (TCP/UDP).
- Состояние соединения.
- Имя и ID процесса.
- Временную метку соединения.

Обработка неизвестных устройств

Если удаленная КЕ не найдена в CMDB, система создает запись **Неизвестного устройства** с IP-адресом и портом. Это позволяет отслеживать соединения с:

- Внешними сервисами и API.

- Непросканированными устройствами.
- Облачными ресурсами.

Конфигурация

Управление ListeningService

Добавляйте кастомные порты сервисов для точного определения направления соединений. Вы можете регистрировать «слушающие сервисы» (listening services), которые используются в вашей организации (например, проприетарные приложения, работающие на специфических портах). Это помогает системе безошибочно определять, какая КЕ является сервером, а какая — клиентом в каждом конкретном соединении.

Настройка типов связей

По умолчанию система использует тип связи **«Connected To»** (Подключен к) для представления сетевых соединений между КЕ. В системе этот тип классифицируется как тип связи **«Dependency»** (Зависимость).

Статистика и мониторинг

Система отслеживает метрики обработки связей, включая:

- Количество созданных и обновленных связей.
- Количество созданных UnknownDevice.
- Ошибки обработки и найденные дубликаты.

Используйте эти метрики для мониторинга эффективности обработки и измерения качества данных.

Просмотр связей

Вы можете просматривать связи КЕ через веб-интерфейс:

- **Запросы:** Фильтрация по направлению, уровню достоверности и конкретной КЕ.
- **Информация:** Каждая связь отображает источник, цель, протокол, порты, обоснование направления и детальную статистику по каждой из сторон (перспективы source/target).

13 ОБЗОР DISCOVERY

RS-Discovery (R-Sight) Discovery автоматически находит и сопоставляет всю вашу ИТ-инфраструктуру, создавая точное представление обо всем оборудовании, программном обеспечении и связях между ними в режиме реального времени. Используя несколько методов обнаружения и анализ на базе ИИ, решение устраняет процессы ручной инвентаризации и гарантирует актуальность вашей CMDB.

Что такое Discovery?

Discovery — это автоматизированный процесс, включающий:

- **Поиск** устройств и приложений в вашей сети.
- **Сбор** подробной информации о конфигурации и состоянии.
- **Сопоставление** связей и зависимостей.
- **Анализ** паттернов и аномалий с помощью ИИ.
- **Обновление** CMDB актуальными данными.

Методы Discovery

Агентный метод (Agent-Based Discovery)

Преимущества:

- Глубокая системная информация
- Обновления в режиме реального времени
- Доступ за сетевыми экранами (firewalls)
- Минимальное влияние на сеть

Безагентный метод (Agentless Discovery) – Сетевое сканирование, на основе API

Гибридный метод (Hybrid Discovery)

Сочетает агентный и безагентный методы для:

- Полного охвата инфраструктуры
- Минимального количества слепых зон
- Оптимизированной производительности
- Гибкости развертывания

Функции обнаружения на основе ИИ

Распознавание паттернов и Обнаружение аномалий

- Идентификация стандартных паттернов развертывания
- Обнаружение стеков приложений
- Распознавание конфигураций кластеров
- Сопоставление сервисов с балансировкой нагрузки

Планирование Discovery

Типы расписаний

Полное обнаружение (Full Discovery)

- Полное сканирование инфраструктуры

- Сбор всех атрибутов
- Пересборка связей
- Расписание: Еженедельно

Инкрементальное обнаружение (Incremental Discovery)

- Только изменения
- Новые или измененные устройства
- Быстрые обновления
- Расписание: Каждые 4 часа

Обнаружение в режиме реального времени (Real-time Discovery)

- Изменения на базе агентов
- Немедленные обновления
- Только для критически важных систем
- Расписание: Непрерывно

14 СЕТЕВОЕ СКАНИРОВАНИЕ (NETWORK SCANNING)

Сетевое сканирование является фундаментом обнаружения инфраструктуры в RS-Discovery (R-Sight). Используя несколько протоколов и методы интеллектуального сканирования, платформа автоматически находит устройства, сопоставляет топологию сети и идентифицирует сервисы, запущенные в вашей сети.

Протоколы сканирования

WMI (Windows Management Instrumentation)

WMI предоставляет глубокую системную информацию о среде Windows через стандартизированный интерфейс. Это основной протокол для обнаружения серверов и рабочих станций Windows.

Что собирает WMI:

Категория	Информация
Оборудование	ЦП, оперативная память, дисковые накопители, сетевые адаптеры, BIOS/UEFI
Программное обеспечение	Установленные приложения, компоненты Windows, запущенные службы, патчи
Система	Журналы событий, учетные записи пользователей, запланированные задачи, правила брандмауэра
Производительность	Загрузка ЦП, использование памяти, ввод-вывод диска (I/O)

Сетевые требования:

- **Порт TCP 135** (RPC Endpoint Mapper)
- **Динамические порты RPC** (49152-65535)
- На целевых системах должна быть включена **служба WMI**

SSH (Secure Shell)

SSH обеспечивает безопасное обнаружение устройств на базе Linux, Unix, а также сетевого оборудования. Поддерживается аутентификация как по паролю, так и по ключам.

Что собирает SSH:

Категория	Информация
Система	Версия ОС, ядро, сведения об оборудовании
ПО	Списки пакетов, запущенные процессы, системные службы
Сеть	Конфигурация интерфейсов, маршрутизация, активные соединения
Производительность	Использование ресурсов, ввод-вывод диска, системная нагрузка

Два режима сканирования:

- **Базовый режим (обычный пользователь):** системная информация, конфигурация сети, процессы, установленные пакеты.
- **Расширенный режим (root/sudo):** все базовые данные плюс сведения об оборудовании, информация BIOS, состояние дисков, виртуализация.

15 SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

SNMP — основной протокол для обнаружения сетевых устройств: коммутаторов, маршрутизаторов, брандмауэров и принтеров.

Поддерживаемые версии:

- **SNMPv2c:** на основе строк сообщества (community-based) с улучшениями по сравнению с v1.
- **SNMPv3:** безопасный протокол с аутентификацией и шифрованием (**рекомендуется**).

Что собирает SNMP:

Категория	Информация
Система	Описание устройства, имя хоста, местоположение, контакт, аптайм
Интерфейсы	Сетевые интерфейсы, скорость, статус, счетчики трафика
Топология	Обнаружение соседей (CDP/LLDP), распределение VLAN
Специфика	Информация от конкретных вендоров (Cisco, HP и др.)

Интеграция с vCenter

Обнаруживайте всю инфраструктуру VMware, включая центры обработки данных (ЦОД), кластеры, хосты ESXi и виртуальные машины.

Что собирает vCenter:

Категория	Информация
Инфраструктура	ЦОДы, кластеры, пулы ресурсов
Хосты	Хосты ESXi, спецификации оборудования, конфигурация
Виртуальные машины	Инвентаризация ВМ, распределение ресурсов, гостевые ОС
Хранилище	Хранилища данных (Datastores), емкость, использование
Сеть	Виртуальные коммутаторы, группы портов, VLAN

Настройка сканирования Discovery

Шаг 1: Создание расписания Discovery

1. Перейдите в раздел **Discovery > Schedules (Расписание)**.
2. Нажмите **Create Schedule (Создать расписание)**.
3. Настройте следующие параметры:
   - **Имя (Name):** Понятное описание сканирования.
   - **IP-диапазоны (IP Ranges):** Целевые сетевые диапазоны (в нотации CIDR, например, 192.168.1.0/24).
   - **Протоколы (Protocols):** Выберите WMI, SSH, SNMP или vCenter.
   - **Учетные данные (Credentials):** Назначьте сохраненные учетные данные для каждого протокола.

Шаг 2: Назначение учетных данных

Каждый протокол требует соответствующих прав доступа:

Протокол	Тип учетных данных
WMI	Учетная запись домена Windows с правами локального администратора
SSH	Имя пользователя/пароль или пара SSH-ключей
SNMP	Строка Community (v2c) или имя пользователя/аутентификация/приватность (v3)
vCenter	Учетная запись vCenter с доступом «Только чтение» (Read-only)

Шаг 3: Настройка расписания

Выберите время запуска сканирования:

- **Однократно (One-time):** запустить немедленно или в назначенное время.
- **Периодически (Recurring):** ежедневно, еженедельно или с настраиваемыми интервалами.
- **Непрерывно (Continuous):** постоянный мониторинг с настраиваемыми интервалами.

Шаг 4: Просмотр результатов

После завершения сканирования:

1. Перейдите в раздел **Discovery > История сканирования**.
2. Изучите обнаруженные устройства и их детали.
3. Проверьте наличие ошибок сканирования или неполных результатов.
4. Просмотрите созданные или обновленные КЕ в CMDB.

Обнаружение топологии (Topology Discovery)

RS-Discovery (R-Sight) может сопоставлять вашу физическую и логическую топологию сети:

Обнаружение на уровне Layer 2:

- Идентификация соседей через **CDP** (Cisco Discovery Protocol).
- Идентификация соседей через **LLDP** (Link Layer Discovery Protocol).
- Сопоставление назначений VLAN и портов коммутаторов.
- Маппинг физических соединений.

Обнаружение на уровне Layer 3:

- Анализ таблиц маршрутизации.
- Идентификация подсетей.
- Сопоставление шлюзов по умолчанию.
- Определение границ сети.

16 СПРАВОЧНОЕ РУКОВОДСТВО ПО СКАНЕРУ VMWARE VCENTER

Этот документ представляет собой подробное руководство по сканеру VMware vCenter, используемому для обнаружения сетевой инфраструктуры в RS-Discovery (R-Sight). Сканер vCenter выполняет глубокий анализ сред VMware для сбора полных данных о виртуализации.

Сетевые порты и протоколы

Взаимодействие с vCenter API

- **Порт 443 (TCP)** — vSphere API через HTTPS (обязательно).
- **Протокол** — SOAP/REST API через TLS.
- **Аутентификация** — vSphere SSO (Single Sign-On).

Триггер обнаружения

Сканер vCenter запускается автоматически, когда:

1. В ходе сетевого сканирования обнаруживается открытый порт 443.
2. Вручную настроена цель vCenter с соответствующими учетными данными.

Требования к аутентификации

Учетные данные vCenter

Для работы сканера требуются учетные данные vCenter с соответствующими правами:

Минимально необходимые разрешения:

- **Роль (Role):** Read-Only (Только чтение) — достаточно для операций обнаружения.
- **Глобальные разрешения (Global Permissions):** Требуются на уровне vCenter.
- **Распространение (Propagation):** Права должны наследоваться (распространяться) на все дочерние объекты.

Необходимые привилегии:

- System.Anonymous
- System.Read
- System.View
- Global.Licenses
- Host.Config.AdvancedConfig
- VirtualMachine.Config.AdvancedConfig

Процесс аутентификации (Flow):

1. **SSL-соединение** — устанавливается безопасное соединение с vCenter.
2. **SSO Login** — аутентификация с использованием предоставленных данных.
3. **Управление сессией** — поддержка активной сессии во время сбора данных.
4. **Корректный выход** — правильное закрытие сессии после завершения работы.

Информация о сервере vCenter

Собираемые данные

Идентификация

- Имя и версия vCenter
- Номер сборки (Build number)
- Версия API
- UUID экземпляра (Instance UUID)

Конфигурация

- IP-адрес
- Тип операционной системы
- Информация о лицензиях
- Название и версия продукта

Метрики состояния vCenter

- Общий статус работоспособности системы
- Статус сервисов
- Количество подключенных хостов
- Общее количество ВМ

Обнаружение дата-центров

Информация о дата-центре

Базовые свойства

- Имя дата-центра
- Уникальный идентификатор (MoRef)
- Общий статус (зеленый/желтый/красный/серый)

Структура папок

- Пути к папкам ВМ, хостов, сетей и хранилищ (Datastores)

Счетчики ресурсов

- Общее количество хостов ESXi
- Общее количество виртуальных машин
- Общее количество кластеров

- Общее количество хранилищ

Конфигурация кластера

Свойства кластера

Идентификация

- Имя кластера и уникальный идентификатор
- Ссылка на родительский дата-центр

Конфигурация ресурсов

- Общее количество ядер ЦП
- Общий объем оперативной памяти
- Текущее использование ЦП (МГц) и памяти (МБ)
- Общее количество размещенных ВМ

Настройки High Availability (HA)

- Статус HA (включено/выключено)
- Контроль допуска (Admission control)
- Уровень отказоустойчивости (Failover level)
- Статус мониторинга хостов

Distributed Resource Scheduler (DRS)

- Конфигурация DRS (включено/выключено)
- Уровень автоматизации (ручной/частичный/полный)
- Порог миграции
- Настройки управления питанием

Enhanced vMotion Compatibility (EVC)

- Статус режима EVC
- Текущий базовый уровень (baseline) EVC
- Требования к совместимости ЦП

Обнаружение хостов ESXi

Системная информация хоста

Сведения об оборудовании

- Имя хоста и домен
- Производитель и модель
- Серийный номер и UUID
- Версия BIOS

Спецификации ЦП

- Модель процессора
- Количество физических процессоров (CPU packages)

- Общее количество ядер
- Потоки ЦП (логические процессоры)
- Частота ЦП (МГц)

Конфигурация памяти

- Общий объем физической памяти
- Детальная информация о модулях памяти
- Текущее использование памяти

Состояние и статус хоста

Состояние подключения (Connection State)

- Connected (Подключен)
- Disconnected (Отключен)
- Not Responding (Не отвечает)
- Maintenance Mode (Режим обслуживания)

Состояние питания (Power State)

- Powered On (Включен)
- Powered Off (Выключен)
- Standby (Ожидание)
- Unknown (Неизвестно)

Операционные метрики

- Время загрузки
- Время непрерывной работы (Uptime в днях)
- Количество запущенных ВМ
- Общий статус работоспособности

Информация о гипервизоре

Детали VMware ESXi

- Полное название продукта
- Номер версии и номер сборки
- Версия API
- Уровень исправлений (Patch level)

Сетевая конфигурация

- **Сеть управления:** IP-адреса управления
- **vMotion:** IP-адреса для миграции
- **Сеть хранения:** IP-адреса для систем хранения данных
- **Виртуальные коммутаторы:** конфигурация vSwitch

Обнаружение виртуальных машин

Идентификация VM

Уникальные идентификаторы

- Имя ВМ
- UUID (vCenter UUID, Instance UUID, BIOS UUID)
- Идентификатор MoRef

Конфигурация VM

Спецификации оборудования

- Количество виртуальных процессоров (vCPU)
- Выделенная память (МБ)
- Версия виртуального оборудования
- Сконфигурированная гостевая ОС

Распределение ресурсов

- Резервирование и лимиты ЦП (МГц)
- Резервирование и лимиты памяти (МБ)

Информация о работе VM

- **Состояние питания:** Powered On, Powered Off, Suspended (Приостановлена)

Сведения о гостевой системе

- Обнаруженная гостевая ОС и её ID
- Статус и версия **VMware Tools**
- Имя хоста гостевой ОС
- IP-адреса (все сетевые интерфейсы)

Метаданные VM

Административная информация

- Аннотации и заметки
- Пользовательские атрибуты
- Теги и категории
- Дата создания
- Время последней загрузки

Расположение файлов

- Путь к конфигурационному файлу VM (.vmx)
- Расположение виртуальных дисков (.vmdk)
- Информация о снимках состояния (Snapshots)

Обнаружение шаблонов

Сканер автоматически идентифицирует и классифицирует шаблоны VM:

- Шаблоны помечаются флагом is_template: true.
- Шаблоны исключаются при создании KE, чтобы не загромождать CMDB неиспользуемыми объектами.

Обнаружение систем хранения

Информация о хранилищах

Идентификация

- Имя хранилища и уникальный идентификатор
- Тип (VMFS, NFS, vSAN, vVOL и др.)
- URL или системный путь

Метрики емкости

- Общая емкость (ГБ)
- Свободное место (ГБ)
- Используемое пространство (ГБ)
- Процент заполнения

Конфигурация

- Версия файловой системы
- Размер блока
- Максимальный размер файла
- Статус доступности

Свойства хранилищ

Информация о доступе

- Возможность многопользовательского доступа (несколько хостов)
- Текущий статус доступности
- Статус режима обслуживания

Связанные ресурсы

- Количество VM, использующих данное хранилище
- Информация о точках монтирования на хостах
- Пути монтирования для каждого хоста
- Права доступа (чтение/запись)

Сетевое обнаружение

Типы виртуальных сетей

Стандартные сети

- Сети стандартных виртуальных коммутаторов (**vSwitch**).

- Конфигурация групп портов (**Port groups**).
- Назначенные идентификаторы **VLAN**.

Распределенные сети

- Распределенные виртуальные коммутаторы (**DVS**).
- Распределенные группы портов.
- Конфигурации VLAN и настройки управления сетевым вводом-выводом (**Network I/O Control**).

Свойства сети

Конфигурация

- Имя сети и **VLAN ID**.
- Настройки **MTU**.
- Политика объединения адаптеров (**Teaming policy**).

Связанные ресурсы

- Количество подключенных виртуальных машин и хостов.
- Активные порты и конфигурация восходящих каналов (**Uplinks**).

Информация о пулах ресурсов

Иерархия пулов ресурсов

- Имя пула и путь в иерархии.
- Родительский кластер или хост.
- Дочерние пулы.
- Список виртуальных машин, входящих в пул.

Распределение ресурсов

Ресурсы ЦП

- **Reservation:** зарезервированная мощность ЦП (МГц).
- **Limit:** ограничение потребления ЦП.
- **Shares:** доли приоритета (shares).
- **Expandable reservation:** возможность расширяемого резервирования.

Ресурсы памяти

- **Reservation:** зарезервированный объем памяти (МБ).
- **Limit:** ограничение потребления памяти.
- **Shares:** доли приоритета памяти.
- **Expandable reservation:** статус расширяемого резервирования памяти.

Сопоставление связей

Инфраструктурные связи

Сканер автоматически создает следующие типы связей для построения актуальной карты зависимостей:

Иерархические связи

- **vCenter** → **manages** → Datacenter (управляет дата-центром)
- **Datacenter** → **contains** → Cluster (содержит кластер)
- **Datacenter** → **contains** → Host (содержит хост)
- **Cluster** → **contains** → Host (содержит хост)
- **Host** → **hosts** → VM (размещает VM)
- **vCenter** → **manages** → Datastore (управляет хранилищем)
- **vCenter** → **manages** → Network (управляет сетью)

Ресурсные связи (Resource Relationships)

- **VM** → **uses** → Datastore (использует хранилище)
- **VM** → **connected to** → Network (подключена к сети)
- **Host** → **mounts** → Datastore (монтирует хранилище)
- **Host** → **uses** → Network (использует сеть)

Сервисные связи (Service Relationships)

- **VM** → **runs on** → Host (запущена на хосте)
- **VM** → **member of** → Resource Pool (является участником пула ресурсов)
- **Host** → **member of** → Cluster (является участником кластера)

Рекомендации по производительности

Метрики сканирования:

- **Типичное время сканирования:** 2–10 минут (зависит от размера инфраструктуры).
- **Оптимизация API:** использование массового сбора свойств (Bulk property collection).
- **Потребление памяти:** 100–500 МБ.
- **Сетевой трафик:** минимальный (только вызовы API).

17 СПРАВОЧНОЕ РУКОВОДСТВО ПО SNMP-СКАНЕРУ

Этот документ представляет собой подробное описание сканера протокола SNMP (Simple Network Management Protocol), используемого в RS-Discovery (R-Sight). Сканер SNMP предназначен для обнаружения и мониторинга сетевых устройств: маршрутизаторов, коммутаторов, брандмауэров, принтеров и другого оборудования с поддержкой SNMP.

Обзор

Сканер SNMP является основным инструментом для обнаружения сетевой инфраструктуры. Он использует протокол SNMP для сбора исчерпывающей информации об устройствах, их конфигурациях, интерфейсах и связях. Сканер поддерживает версии SNMP v1, v2c и v3 с полным набором функций безопасности.

Сетевые порты и протоколы

Взаимодействие по SNMP

- **Порт 161 (UDP)** — SNMP-агент (обязательно).
- **Порт 162 (UDP)** — SNMP-ловушки (трапы/уведомления) (опционально).
- **Протокол** — Simple Network Management Protocol через UDP.
- **Версии** — SNMPv1, SNMPv2c, SNMPv3.

Триггер обнаружения Сканер SNMP запускается автоматически, когда:

1. В ходе сканирования сети обнаружен открытый порт 161 (UDP).
2. Вручную настроена цель SNMP с соответствующими учетными данными.
3. Устройство отвечает на запросы (пробы) со строками сообщества (community strings).

Обзор сбора данных

Стандартная информация MIB-II

Сканер собирает данные из стандартных баз управляющей информации (Management Information Bases — MIB), которые поддерживаются большинством сетевых производителей.

Системная информация

Базовые системные данные

- **Описание системы (sysDescr):** описание аппаратного и программного обеспечения, версия операционной системы, информация о прошивке.
- **Идентификатор системного объекта (sysObjectID):** уникальный идентификатор производителя/устройства, используемый для определения типа устройства.
- **Время работы системы (sysUpTime):** время с момента последней перезагрузки (в сотых долях секунды).

Административная информация

- Контактное лицо системы.

- Имя системы (hostname).
- Физическое местоположение.

Классификация устройств

Сканер автоматически классифицирует устройства на основе:

- Паттернов System Object ID.
- Ключевых слов в описании системы.
- Идентификаторов конкретных производителей.

Поддерживаемые типы устройств

Сетевые устройства

- Маршрутизаторы.
- Коммутаторы (уровня 2/3).
- Брандмауэры (Firewalls).
- Балансировщики нагрузки.
- Беспроводные точки доступа.

Инфраструктурные устройства

- Системы ИБП (UPS).
- Датчики мониторинга окружающей среды.
- Блоки распределения питания (PDU).

Конечные устройства

- Принтеры и МФУ.
- IP-телефоны.
- Системы хранения данных.
- Серверы с SNMP-агентами.

Обнаружение интерфейсов

Свойства интерфейса

- **Идентификация интерфейса:** индексный номер, описание/имя, тип (Ethernet, Serial и т. д.), MAC-адрес (если применимо).
- **Конфигурация интерфейса:** MTU (максимальная единица передачи), скорость (бит/с), режим дуплекса, назначенные VLAN.

Статус интерфейса

- **Административный статус:** Up (включен администратором), Down (выключен администратором), Testing (в режиме тестирования).
- **Операционный статус:** Up (функционирует нормально), Down (не функционирует), Unknown (статус не может быть определен).

Информация об IP-адресах

- **IPv4-адреса:** IP-адрес, маска подсети, привязка к интерфейсу.
- **IPv6-адреса (если поддерживаются):** IPv6-адрес, длина префикса, тип адреса.

Обнаружение сетевых связей

Анализ таблицы ARP

Обнаруживает устройства, подключенные напрямую:

- **Записи ARP:** IP-адреса соседей, MAC-адреса, привязки к интерфейсам, типы записей (динамические/статические).

Анализ таблицы маршрутизации

Сопоставляет сетевые пути и шлюзы:

- **Записи маршрутов:** целевые сети, шлюзы следующего перехода (next hop), метрики маршрутов, типы маршрутов (прямые/косвенные).

Типы создаваемых связей

- **Connected To** — прямое соседство на уровне Layer 2.
- **Routes To** — связь маршрутизации на уровне Layer 3.
- **Member Of** — членство в VLAN/подсети.

Система каталога OID

Обзор каталога

RS-Discovery (R-Sight) поддерживает централизованный каталог OID, который:

- Определяет тысячи стандартных и вендорских OID.
- Сопоставляет числовые OID с именами, понятными человеку.
- Предоставляет профили для конкретных устройств.
- Обновляется автоматически через запланированную синхронизацию.

Синхронизация каталога

- **Частота:** ежедневная автоматическая синхронизация.
- **Резервный вариант:** использует кэшированный каталог, если синхронизация не удалась.
- **Общий ресурс:** все агенты используют один и тот же каталог.

Неизвестные устройства

При обнаружении устройств, отсутствующих в каталоге:

- **Поведение Discovery:** базовый сбор данных MIB-II, попытка сопоставления по паттернам, использование стандартного профиля сетевого устройства, опциональный полный опрос дерева MIB (OID Walk).
- **Обработка в бэкенде:** создает KE типа «Unknown Network Device», сохраняет необработанные данные OID для анализа, помечает для ручной классификации, использует ИИ для попытки определения типа устройства.

Добавление поддержки устройств

Автоматическое создание ожидающих устройств (Pending Devices)

При обнаружении неизвестного устройства:

- **Автоматическая запись:** информация об устройстве сохраняется в очереди ожидания.
- **Отслеживание частоты:** система фиксирует, сколько раз встретился данный тип устройства.
- **Расчет приоритета:** большее количество обнаружений = более высокий приоритет для проверки.
- **Сбор OID:** все обнаруженные OID сохраняются для последующего анализа.

Ручное создание профиля

1. Перейдите в **Settings** → **Discovery** → **SNMP Pending Devices**.
2. Изучите устройства, отсортированные по приоритету (количеству обнаружений).
3. Выберите устройство для просмотра обнаруженных OID.
4. Утвердите и создайте профиль, указав:

- Классификацию типа устройства.
- Информацию о производителе и модели.
- Выбор поддерживаемых OID.
- Правила обнаружения (паттерны sysObjectID).

5. Используйте массовое утверждение для похожих устройств с одинаковым sysObjectID.

Преимущества

Видимость сети

- **Полная топология:** обнаружение всех SNMP-устройств.
- **Статус в реальном времени:** текущее состояние устройства.
- **Маппинг интерфейсов:** видимость на уровне портов.
- **Обнаружение связей:** понимание соединений.

Операционные преимущества

- **Автоматизированное обнаружение:** отсутствие ручного документирования.
- **Обнаружение изменений:** отслеживание изменений конфигурации.
- **Планирование мощностей:** мониторинг использования ресурсов.
- **Устранение неполадок:** быстрая идентификация проблем.

Соответствие требованиям (compliance) и безопасность

- **Инвентаризация активов:** полный список устройств.
- **Отслеживание конфигураций:** обнаружение несанкционированных изменений.
- **Сегментация сети:** проверка зон безопасности.
- **Контроль доступа:** мониторинг доступности устройств.

Преимущества интеграции

- **Единая платформа:** единственный источник истины.
- **ИИ-анализ:** интеллектуальные выводы.
- **Автоматизированные рабочие процессы:** запуск действий при изменениях.
- **Отчетность:** комплексные отчеты по сети.

18 СПРАВОЧНОЕ РУКОВОДСТВО ПО ОБНАРУЖЕНИЮ БАЗ ДАННЫХ MICROSOFT SQL SERVER

Этот документ представляет собой подробное руководство по обнаружению баз данных SQL Server в системе RS-Discovery (R-Sight). Сканер баз данных автоматически обнаруживает экземпляры SQL Server, базы данных, соединения и связанные серверы (linked servers) на системах Windows во время WMI-сканирования.

Обзор

Функция обнаружения баз данных SQL Server расширяет возможности WMI-сканирования Windows для сбора исчерпывающей информации об инфраструктуре баз данных. При обнаружении SQL Server на сканируемом сервере Windows сканер автоматически собирает данные о конфигурации экземпляров, инвентаризации баз данных, деталях соединений и настройках безопасности.

Ключевые преимущества

- **Полная инвентаризация БД** — автоматическое обнаружение всех экземпляров и баз данных SQL Server во всей вашей инфраструктуре.
- **Маппинг зависимостей** — определение того, какие приложения и серверы подключаются к вашим базам данных.
- **Видимость безопасности** — отслеживание режимов аутентификации, статуса шифрования и сервисных учетных записей.
- **Контроль резервного копирования** — мониторинг статуса бэкапов и выявление баз данных с отсутствующими резервными копиями.
- **Управление уязвимостями** — генерация CPE позволяет отслеживать CVE (уязвимости) для конкретных версий SQL Server.
- **Планирование мощностей** — отслеживание размеров баз данных и паттернов их роста.

Автоматический запуск

Обнаружение баз данных запускается автоматически, когда:

- Сервер Windows сканируется через **WMI**.
- SQL Server обнаружен в реестре Windows.
- Утилита **SQLCMD** доступна в целевой системе.

Никакой дополнительной настройки не требуется — если SQL Server существует на сканируемом Windows-сервере, он будет обнаружен.

Сетевые требования

Обнаружение SQL Server использует те же сетевые подключения, что и сканирование Windows через WMI:

Порт	Протокол	Назначение
135	TCP	RPC Endpoint Mapper (WMI)

445	TCP	SMB/CIFS (резервный вариант для PAExec)
49152-65535	TCP	Динамический диапазон RPC

Примечание: Сканер подключается к SQL Server локально на целевой машине с помощью SQLCMD, поэтому TCP-порт SQL Server (1433) не обязательно должен быть доступен со стороны сканера.

Требования к учетным данным

Windows Authentication (по умолчанию) Сканер использует Windows-аутентификацию с теми же учетными данными, которые были предоставлены для WMI-сканирования. Отдельные учетные данные для SQL не требуются.

- Аккаунт для WMI-сканирования должен иметь логин в SQL Server.
- Интегрированная аутентификация Windows используется автоматически.
- Бесшовная работа с доменными учетными записями.

Необходимые разрешения SQL Server

Для полного обнаружения баз данных учетной записи сканирования требуются следующие разрешения SQL Server:

Разрешение	Назначение	Для чего требуется
VIEW SERVER STATE	Метрики уровня сервера	Конфигурация памяти, соединения, службы, шифрование.
VIEW ANY DATABASE	Перечисление баз данных	Составление списка всех БД.
VIEW ANY DEFINITION	Объекты сервера	Обнаружение связанных серверов (Linked servers).
db_datareader (в msdb)	История бэкапов	Даты последнего резервного копирования.

Собираемые данные

Информация об экземпляре SQL Server

Для каждого обнаруженного экземпляра SQL Server:

Точка данных	Описание
Имя экземпляра	Идентификатор именованного экземпляра (например, MSSQLSERVER, SQLEXPRESS)
Версия	Полная строка версии (например, 15.0.4153.1)
Редакция	Enterprise, Standard, Express, Developer, Web
Режим аутентификации	Только Windows или смешанный режим (Mixed mode)
Кодировка (Collation)	Серверная кодировка по умолчанию
Кластеризация	Членство в отказоустойчивом кластере

Конфигурация памяти	Настройки минимальной/максимальной памяти
Учетная запись службы	Учетная запись Windows, под которой запущен SQL Server
CPE	Common Platform Enumeration для поиска уязвимостей

Информация о базах данных

Для каждой базы данных в экземпляре:

Точка данных	Описание
Имя базы данных	Название базы данных
Владелец	Учетная запись владельца базы данных
Состояние	Online, Offline, Restoring и т. д.
Модель восстановления	Full, Bulk-Logged, Simple
Уровень совместимости	Совместимость с версией SQL Server
Размер	Общий размер в МБ (данные + лог)
Размер данных	Размер файла данных в МБ
Размер лога	Размер файла лога транзакций в МБ
Зашифрована	Статус шифрования TDE
Только чтение	Статус режима «Read-only»
Системная БД	master, msdb, model, tempdb
Последний бэкап	Дата последнего полного резервного копирования
Последний бэкап лога	Дата последнего резервного копирования лога

Информация о соединениях

Сканер обнаруживает, кто подключен к вашим базам данных:

Точка данных	Описание
Client IP	IP-адрес подключающегося клиента
Client Hostname	Имя хоста подключающегося сервера
Application Name	Имя подключающегося приложения
Login Name	SQL-логин, используемый для соединения
Database	Целевая база данных
Connection Count	Количество соединений

Связанные серверы (Linked Servers)

Для связанных серверов SQL Server:

Точка данных	Описание

Имя связанного сервера	Локальное имя связанного сервера
Удаленный сервер	Имя или адрес целевого сервера
Провайдер	Провайдер OLE DB (например, SQLNCLI11)
БД по умолчанию	База данных по умолчанию на удаленном сервере

Создаваемые типы КЕ

DatabaseInstance

Представляет экземпляр SQL Server, запущенный на сервере.

- **Родительский тип КЕ:** Server
- **Правило именования:** ИмяСервера\ИмяЭкземпляра (например, SQLPROD01\MSSQLSERVER)

Database

Представляет отдельную базу данных внутри экземпляра.

- **Родительский тип КЕ:** DatabaseInstance
- **Правило именования:** ИмяСервера\ИмяЭкземпляра\ИмяБазыДанных

Создаваемые связи

Сканер автоматически создает следующие типы связей:

Тип связи	Источник	Цель	Описание
Runs On	DatabaseInstance	Server	Экземпляр запущен на сервере
Part Of	Database	DatabaseInstance	База данных принадлежит экземпляру
Connected To	Server	Database	Клиентский сервер подключается к БД
Linked To	DatabaseInstance	DatabaseInstance	Связанный сервер SQL Server (Linked server)

Поддержка именованных экземпляров

Сканер автоматически обнаруживает все экземпляры SQL Server на сервере:

- **Экземпляр по умолчанию** — MSSQLSERVER (подключение как localhost).
- **Именованные экземпляры** — пользовательские имена (подключение как localhost\ИМЯ_ЭКЗЕМПЛЯРА).

Интеграция с управлением уязвимостями

Генерация CPE

Сканер автоматически генерирует идентификаторы CPE (Common Platform Enumeration) для сопоставления с уязвимостями:

- **Формат:** cpe:2.3:a:microsoft:sql_server:{year}:*:*:*:{edition}:*:*:*

Примеры:

- SQL Server 2019 Enterprise: cpe:2.3:a:microsoft:sql_server:2019:*:*:*:enterprise:*:*:*
- SQL Server 2017 Standard: cpe:2.3:a:microsoft:sql_server:2017:*:*:*:standard:*:*:*
- SQL Server 2016 Express: cpe:2.3:a:microsoft:sql_server:2016:*:*:*:express:*:*:*

19 РАЗВЕРТЫВАНИЕ АГЕНТА СКАНЕРА RS-DISCOVERY (R-SIGHT)

Сканер RS-Discovery (R-Sight) — это агент сетевого обнаружения на базе Windows, который автоматически сканирует вашу инфраструктуру, собирает системную информацию и интегрируется с платформой RS-Discovery (R-Sight). Он обеспечивает всестороннюю видимость вашей сети посредством автоматизированного сканирования и связи в реальном времени с бэкендом RS-Discovery (R-Sight).

Обзор

Сканер RS-Discovery (R-Sight) работает как автономное приложение Windows в двух режимах:

- **GUI Mode:** интерактивное десктопное приложение для ручного сканирования и настройки.
- **Service Mode:** служба Windows для запланированного автоматического сканирования.

Компоненты сканера

- **Network Scanner:** Обнаруживает устройства в вашей сети, определяет открытые порты и выбирает подходящие протоколы для сканирования.
- **Protocol Scanners:** Собирают детальную информацию, используя соответствующий протокол:
  - **WMI Scanner:** Собирает исчерпывающие данные из систем Windows (оборудование, ПО, сетевые соединения, пользователи).
  - **SSH Scanner:** Собирает информацию из систем Linux/Unix (пакеты, процессы, состояние сети).
  - **SNMP Scanner:** Обнаруживает сетевые устройства и их конфигурации.
  - **vCenter Scanner:** Интегрируется с инфраструктурой VMware для обнаружения виртуальных машин и хостов.
- **WebSocket Client:** Поддерживает постоянное соединение с RS-Discovery (R-Sight) для управления в реальном времени и обновления статуса.

Системные требования

Минимальные требования

Компонент	Требование
Операционная система	Windows 10/11 или Windows Server 2016+ (64-бит)
Процессор	Многоядерный процессор (рекомендуется для сканирования крупных сетей)
Память	Минимум 2 ГБ ОЗУ, рекомендуется 4 ГБ+
Дисковое пространство	1 ГБ свободного места (для приложения, логов и результатов)
Привилегии	Требуются права администратора для работы в режиме службы

Требования к сетевым портам

Для выполнения операций сканирования и связи сканеру RS-Discovery (R-Sight) требуются определенные сетевые порты.

Исходящие соединения (Сканер → Платформа RS-Discovery (R-Sight))

Порт	Протокол	Назначение
443	HTTPS/WSS	API-взаимодействие и WebSocket-соединение с api.RS-Discovery (R-Sight).com

Порты сканирования (Сканер → Целевые устройства)

Системы Windows (WMI-сканирование)

Порт	Протокол	Назначение	Примечания
135	TCP	RPC Endpoint Mapper	Требуется для WMI
445	TCP	SMB/CIFS	Требуется для WMI и резервного режима
49152-65535	TCP	Динамический RPC	Используется WMI (настраиваемый диапазон)

Резервный режим PAExec

Если порты RPC заблокированы, сканер автоматически переключается в режим PAExec, для которого требуется только порт 445 (SMB). Это полезно в средах с жесткими ограничениями брандмауэра.

Системы Linux/Unix (SSH-сканирование)

Порт	Протокол	Назначение
22	TCP	SSH

Сетевые устройства (SNMP-сканирование)

Порт	Протокол	Назначение
161	UDP	SNMP-запросы

VMware vCenter

Порт	Протокол	Назначение
443	HTTPS	vCenter API

Процесс развертывания

Шаг 1: Загрузка сканера

Загрузите портативную версию сканера RS-Discovery (R-Sight) с вашей платформы:

1. Войдите в свой экземпляр RS-Discovery (R-Sight).
2. Перейдите в раздел **Discovery** → **Agents**.
3. Нажмите кнопку **Download Agent**.
4. Распакуйте ZIP-файл в выбранную вами папку (например, C:\RS-Discovery (R-Sight)\Scanner).

Шаг 2: Первоначальная настройка

1. **Запуск приложения:** запустите исполняемый файл RS-Discovery (R-Sight) Scanner.exe из распакованной папки.
2. **Настройка интеграции:**
   - Перейдите на вкладку **Integrations**.
   - Введите URL API вашей платформы RS-Discovery (R-Sight) (например, https://api.RS-Discovery (R-Sight).com/api).
   - Введите **Discovery API Key** (токен), сгенерированный на платформе RS-Discovery (R-Sight) в разделе *Discovery Token*.
   - Введите **Agent ID** — уникальный идентификатор для этого экземпляра сканера.
3. **Проверка:** Нажмите кнопку **Test Connection**, чтобы убедиться, что сканер может связаться с платформой.

Шаг 3: Настройка учетных данных

Для сбора информации с целевых систем необходимо предоставить соответствующие учетные данные:

Системы Windows:

- Перейдите на вкладку **Credentials**.
- Добавьте учетные данные доменного или локального администратора.
- Формат: domain\username или username@domain.com.

Системы Linux/Unix:

- Добавьте учетные данные SSH (логин/пароль или SSH-ключи).
- Для полной инвентаризации рекомендуется доступ root или права sudo.

VMware vCenter:

- Добавьте учетные данные администратора vCenter или учетную запись с правами только на чтение.

Безопасность учетных данных: Все учетные данные шифруются с использованием Fernet (AES-128-CBC) с локальным файлом ключа и хранятся локально. Учетные данные никогда не отправляются на платформу RS-Discovery (R-Sight).

Шаг 4: Настройка сканирования

1. Перейдите на вкладку **Scan**.
2. Введите сетевые диапазоны (поддерживается нотация CIDR: 192.168.1.0/24).
3. Выберите протоколы для использования (WMI, SSH, SNMP, vCenter).
4. Нажмите **Start Scan** для выполнения сканирования вручную.

Шаг 5: Настройка сканирования по расписанию (опционально)

Для автоматизации процесса:

1. Перейдите на вкладку **Scheduler**.
2. Добавьте конфигурации сканирования: укажите диапазоны сетей и расписание (ежедневно, еженедельно, настраиваемое время).
3. Перейдите на вкладку **Service**.
4. Установите (**Install**) и запустите (**Start**) службу Windows. После этого сканирование будет выполняться автоматически согласно расписанию.

Режимы работы

GUI Mode (Графический интерфейс)

Десктопное приложение обеспечивает:

- **Интерактивное сканирование:** запуск вручную и просмотр прогресса в реальном времени.
- **Управление учетными данными:** добавление, редактирование и проверка прав доступа.
- **Настройка расписания:** создание графиков автоматического сканирования.
- **Управление службой:** установка, запуск, остановка и мониторинг службы Windows.
- **Статус и мониторинг:** просмотр истории сканирования и состояния WebSocket-соединения.

Лучше всего подходит для: первоначальной настройки, разового сканирования, тестирования подключений и устранения неполадок.

Service Mode (Режим службы)

Служба Windows обеспечивает:

- **Автоматизированное сканирование:** выполнение задач по расписанию без участия пользователя.
- **Связь в реальном времени:** поддержка WebSocket-соединения для удаленного управления.
- **Фоновая работа:** работа независимо от пользовательских сессий.
- **Автозапуск:** запуск при загрузке ОС Windows.

Лучше всего подходит для: продуктовых сред, непрерывного обнаружения активов и удаленного управления сканированием.

Связь в режиме реального времени

Соединение WebSocket

Сканер RS-Discovery (R-Sight) поддерживает постоянное WebSocket-соединение с платформой для оперативного управления и контроля в режиме реального времени.

Возможности удаленного управления

Благодаря WebSocket-соединению платформа RS-Discovery (R-Sight) может:

- **Мониторинг статуса агента:** Отслеживание работоспособности и связности в реальном времени.
- **Запуск сканирования:** Инициирование сканирования по требованию удаленно.
- **Обновление расписаний:** Изменение графиков сканирования без прямого доступа к агенту.
- **Получение метрик:** Сбор системных показателей (CPU, память, диск).
- **Просмотр конфигурации:** Проверка текущих настроек и возможностей агента.

Системные метрики

Агент передает на платформу следующие показатели:

Метрика	Описание
Загрузка CPU	Текущее использование процессора
Использование памяти	Процент потребления ОЗУ
Дисковое пространство	Доступное место для результатов сканирования
Локальный IP	Основной сетевой адрес агента
Статистика сканирования	Количество завершенных сканирований, процент успеха

Безопасность и соответствие (Compliance)

Аутентификация и авторизация

- **Аутентификация по API-ключу:** Сканер использует ключ API Discovery, сгенерированный на платформе RS-Discovery (R-Sight), для всех коммуникаций.
- **Безопасность WebSocket:** Все соединения используют протокол **WSS** (WebSocket Secure) поверх TLS 1.2+ для шифрования связи.
- **Защита учетных данных:** Данные для доступа к целевым системам шифруются с помощью **Windows DPAPI** и хранятся локально — они никогда не покидают систему агента.

Сетевая безопасность

- **Настройка брандмауэра:** Сканеру требуется только исходящий доступ по HTTPS (порт 443) к платформе RS-Discovery (R-Sight). Входящие соединения не требуются.
- **Шифрование данных:** Все данные, передаваемые на платформу, шифруются при транспортировке с помощью TLS.
- **Проверка SSL:** Проверка SSL-сертификатов включена по умолчанию (можно настроить при использовании самоподписанных сертификатов).

Сбор данных

Для каждого обнаруженного устройства сканер собирает следующий набор информации:

Системы Windows (WMI):

- **Системная информация:** производитель, модель, серийный номер.
- **Данные ОС:** версия, уровень обновлений (patch level).
- **Инвентаризация оборудования:** ЦП, память, диски, сетевые адаптеры.
- **Программное обеспечение:** установленные программы и приложения.
- **Службы и процессы:** список запущенных сервисов и активных процессов.
- **Сетевые соединения:** текущие активные сессии.
- **Учетные записи:** пользователи (с определением домена).

Системы Linux/Unix (SSH):

- **Системная информация:** версия ядра, дистрибутив.
- **Детали оборудования:** ЦП, память, хранилища данных.
- **Сетевые интерфейсы:** конфигурации IP и сетевые настройки.
- **Установленные пакеты:** данные из менеджеров dpkg или rpm.
- **Процессы и службы:** активные системные процессы.
- **Пользователи:** только несистемные учетные записи.

Инфраструктура VMware (vCenter):

- **vCenter Server:** общая информация о сервере управления.
- **Структура:** дата-центры и кластеры.
- **Хосты ESXi:** полная инвентаризация физических серверов.
- **Виртуальные машины:** детали конфигурации VM.
- **Ресурсы:** аллокация и фактическое использование ресурсов.
- **Маппинг связей:** логические отношения между объектами инфраструктуры.

Сетевые устройства (SNMP):

- **Идентификация:** производитель и тип устройства.
- **Интерфейсы:** конфигурация портов.
- **Метрики:** время непрерывной работы (uptime) и показатели производительности.

Мониторинг и управление

Мониторинг статуса агента

Вы можете отслеживать состояние ваших сканеров RS-Discovery (R-Sight) напрямую через платформу:

В интерфейсе RS-Discovery (R-Sight): Перейдите в раздел **Discovery → Agents**. Здесь отображаются все зарегистрированные агенты и их текущий статус:

- **Online:** агент подключен через WebSocket.
- **Offline:** агент давно не выходил на связь.
- **Scanning:** в данный момент выполняется сканирование.
- **Error:** агент столкнулся с проблемами в работе.

Отображаемая информация об агенте:

- Имя и уникальный идентификатор (UID).
- Время последнего подключения.
- Системные метрики (загрузка ЦП, ОЗУ, диска).
- Количество завершенных сканирований.
- Текущая конфигурация расписаний.
- Качество сетевого соединения.

Удаленное управление

С платформы RS-Discovery (R-Sight) вы можете выполнять следующие действия:

- **Запуск сканирования:** инициируйте немедленное сканирование без доступа к системе агента.
  - Выбор целевых IP-диапазонов.
  - Выбор конкретных протоколов.
  - Мониторинг прогресса в реальном времени.
- **Обновление расписаний:** дистанционно изменяйте график работ.
  - Добавление или удаление запланированных сканирований.
  - Изменение частоты опроса.
  - Включение/выключение отдельных задач.
- **Мониторинг производительности:** просмотр трендов использования ресурсов агента.
  - Графики загрузки ЦП и памяти.
  - Статистика длительности сканирований.
  - Соотношение успешных и неудачных попыток.
- **Просмотр логов:** доступ к журналам работы агента для устранения неполадок (если функция включена).

Руководство по настройке брандмауэра

Система сканера (Исходящие правила / Outbound)

Обязательно:

- **TCP 443** на api.RS-Discovery (R-Sight).com (HTTPS/WSS).
- **TCP 22, 135, 445** во внутренние сети (сканирование).
- **UDP 161** во внутренние сети (SNMP).

Опционально:

- **TCP 443** на серверы vCenter.

Целевые системы (Входящие правила со стороны сканера / Inbound)

Тип системы	Порты и протоколы	Описание

Windows	TCP 135, 445, TCP 49152-65535	RPC, SMB и динамический RPC
Linux/Unix	TCP 22	SSH
Сетевые устройства	UDP 161	SNMP

Часто задаваемые вопросы (FAQ)

В: Можно ли запустить несколько сканеров в одной среде?

О: Да! Вы можете развернуть любое количество сканеров в разных сегментах сети. Каждый агент подключается независимо со своим API-ключом.

В: Что произойдет, если сканер потеряет связь с платформой во время работы?

О: Сканирование продолжится локально, а результаты будут сохранены на диске. Как только связь восстановится, данные будут автоматически загружены на платформу.

В: Сколько сетевой полосы потребляет сканирование?

О: Зависит от объема. Опрос одного устройства обычно генерирует **1–5 МБ** трафика. Сканирование портов потребляет минимум полосы, основной трафик идет в момент сбора детальной инвентаризации.

В: Нужны ли права администратора на всех целевых системах?

О: Для получения полных данных (ПО, серийные номера, службы) — **да**. Без прав администратора объем собираемой информации будет значительно ограничен.

В: Какие исключения для антивируса (AV) рекомендуются?

О: Добавьте директорию установки сканера в исключения. Активность по сканированию портов может быть ошибочно принята антивирусом за атаку.

20 УСТРАНЕНИЕ НЕПОЛАДОК ПРИ ОБНАРУЖЕНИИ ИНФРАСТРУКТУРЫ (TROUBLESHOOTING DISCOVERY)

Это руководство поможет вам диагностировать и устранять распространенные проблемы обнаружения инфраструктуры (Troubleshooting Discovery) в RS-Discovery (R-Sight). Используйте предоставленный систематический подход и инструменты для быстрого выявления и устранения проблем, которые могут возникнуть во время обнаружения инфраструктуры.

Проверка работоспособности системы обнаружения (Discovery Health Check)

Платформа RS-Discovery (R-Sight) предоставляет встроенные средства самодиагностики, позволяющие убедиться, что ваша система сбора данных функционирует корректно и эффективно.

Ключевые области проверки

1. Статус служб Discovery

- Проверка активности всех установленных агентов RS-Discovery (R-Sight) Scanner.
- Контроль стабильности WebSocket-соединения с платформой.
- Мониторинг фоновых процессов обработки данных на стороне сервера.

2. Сетевая связность

- Тестирование доступности API-эндпоинтов платформы (api.RS-Discovery (R-Sight).com).
- Проверка сетевых маршрутов до целевых подсетей.
- Аудит правил брандмауэров на предмет блокировки портов сканирования (22, 135, 445, 161).

3. Хранилище учетных данных (Credential Vault)

- Массовое тестирование сохраненных учетных данных (Validation).
- Проверка уровня доступа (например, достаточно ли прав для чтения реестра или выполнения sudo).
- Отслеживание учетных записей с истекающим сроком действия пароля.

4. Активность последних сканирований

- Анализ истории запусков (Run History) на предмет аномалий в длительности.
- Контроль метрик успеха (Success/Failure rates).
- Выявление закономерностей в сбоях (например, все сбои происходят в одном сегменте сети).

5. Анализ ошибок

- Просмотр последних записей в журналах ошибок.
- Идентификация повторяющихся проблем.
- Отслеживание статуса устранения выявленных инцидентов.

6. Использование ресурсов

- Мониторинг нагрузки на ЦП и ОЗУ сервера сканера во время пиковой нагрузки.
- Проверка свободного места на диске для хранения временных результатов и логов.
- Анализ влияния процесса сканирования на пропускную способность сети.

Распространенные проблемы:

Отсутствие данных (No Discovery Data)

Симптомы

- Новые конфигурационные единицы (КЕ) не появляются в CMDB.
- В результатах сканирования отображается статус «No devices found».
- Пустые отчеты после завершения работы расписания.

Сбои аутентификации

Симптомы

- Ошибки «Доступ запрещен»
- Сообщения «Неверные учетные данные»
- Частичное обнаружение с ошибками аутентификации

Неполное обнаружение

Симптомы

- Отсутствует информация о программном обеспечении
- Частичная информация об оборудовании
- Отсутствие данных о взаимосвязях
- Неполные атрибуты

Проблемы с производительностью

Симптомы

- Медленное завершение обнаружения
- Высокая загрузка ЦП/памяти
- Перегрузка сети
- Ошибки тайм-аута

Проблемы с качеством данных

Симптомы

- Создание дублирующихся доверительных интервалов
- Неправильная классификация
- Отсутствие связей
- Устаревшие данные

21 АНАЛИЗ СЕГМЕНТАЦИИ СЕТИ (NETWORK SEGMENTATION ANALYSIS)

Network Segmentation Analysis в RS-Discovery (R-Sight) обеспечивает полный контроль над потоками трафика между сетевыми зонами. Это позволяет командам безопасности оперативно выявлять несанкционированные взаимодействия, нарушения политик и потенциальные риски безопасности во всей инфраструктуре.

Что такое анализ сегментации сети?

Это автоматизированный процесс, включающий в себя:

- **Визуализацию потоков трафика:** Построение наглядных карт взаимодействия между различными сегментами сети.
- **Обнаружение несанкционированных связей:** Выявление попыток обмена данными между зонами, которые должны быть изолированы.
- **Идентификацию нарушений в реальном времени:** Мгновенное оповещение о трафике, который идет вразрез с установленными правилами безопасности.
- **Детальное расследование (Drill-down):** Возможность изучить каждое конкретное соединение на уровне отдельных IP-адресов.
- **Контроль границ безопасности:** Проверка эффективности установленных барьеров между сегментами.

Ключевые особенности

Визуализация потоков трафика

Просматривайте трафик между зонами в нескольких форматах:

Режим просмотра	Лучшее применение	Описание
Диаграмма Санки	Обзор для руководства	Наглядная диаграмма потоков, показывающая объемы трафика между зонами.
Матричный вид	Детальный анализ	Табличное представление с указанием соединений, портов и статуса нарушений.
Список	Быстрое сканирование	Карточный вид для оперативной оценки ситуации.

Исследование на уровне IP

Детализируйте конкретные нарушения, чтобы увидеть:

- **Исходные IP-адреса**
- **Целевые IP-адреса**
- **Количество соединений**
- **Порты назначения**
- **Имена процессов** (при наличии)

Обзор панели мониторинга (Dashboard)

Карточки сводки

На панели управления отображаются ключевые метрики для быстрого ознакомления:

Метрика	Описание
Всего зон	Количество настроенных сетевых зон
Настроено	Зоны с определенными политиками безопасности
Межзональный трафик	Общее количество соединений между различными зонами
Нарушения	Количество обнаруженных нарушений политики

Вкладка конфигурации зон

Управляйте настройками безопасности зон:

Настройка	Назначение
Тип зоны	Классификация (Prod, DMZ и т. д.)
Уровень безопасности	Уровень приоритета (Критический, Высокий, Средний, Низкий)
Разрешенные входящие	Зоны, которым разрешено подключаться к (to) данной зоне
Описание	Понятное человеку описание зоны
Цвет	Визуальный идентификатор для панелей управления

Вкладка нарушений

Исследуйте нарушения безопасности:

- **Список нарушений:** Все обнаруженные нарушения политик с указанием степени важности.
- **Панель исследования:** Подробная информация о соединении.
- **Рекомендации по устранению:** Предлагаемые действия для решения проблемы.

Как создаются зоны

Сетевые зоны создаются автоматически на основе ваших расписаний обнаружения (Discovery Schedules).

Каждое расписание обнаружения определяет:

- **IP-диапазон:** Сетевая подсеть (например, 10.160.160.0/24).
- **Имя зоны:** Автоматически сгенерированное или пользовательское имя.
- **Агент:** Агент обнаружения, управляющий этой зоной.

Правила нарушений

Как обнаруживаются нарушения

Нарушения рассчитываются в режиме реального времени на основе конфигурации зоны.

Уровни важности

Важность	Триггер	Требуемое действие

Высокая	Трафик к зонам с критическим уровнем безопасности	Немедленное расследование
Средняя	Трафик к другим защищенным зонам	Проверка в течение 24 часов
Низкая	Незначительные отклонения от политики	Мониторинг и оценка

Интеграция с другими модулями

Модуль Discovery (Обнаружение)

Сетевые зоны создаются на основе расписаний обнаружения, что обеспечивает:

- Автоматическое создание зон по мере обнаружения сетей.
- Актуальную информацию об IP-диапазонах.
- Согласованное именование и организацию.

Управление событиями

Нарушения могут генерировать события для:

- Автоматического создания инцидентов.
- Корреляции алертов.
- Запуска рабочих процессов реагирования.

22 БЫСТРЫЙ СТАРТ: СЕГМЕНТАЦИЯ СЕТИ

Настройте и запустите анализ сегментации сети всего за несколько шагов.

Предварительные требования

Прежде чем начать, убедитесь, что у вас есть:

- Развернутые агенты Discovery, собирающие данные.
- Настроенные расписания обнаружения (Discovery schedules) с указанием IP-диапазонов.
- Данные о сетевых соединениях, собираемые с серверов.

Шаг 1: Доступ к сегментации сети

1. Перейдите в раздел **CMDB** в главном меню.
2. Нажмите на подпункт **Network Zones** (Сетевые зоны).
3. Загрузится панель мониторинга анализа сегментации сети.

Шаг 2: Проверка ваших зон

На панели мониторинга автоматически отображаются все сетевые зоны, полученные из ваших расписаний обнаружения:

Столбец	Описание
Имя зоны	Автоматически сгенерировано из расписания обнаружения
IP-диапазон	Охваченная сетевая подсеть
Агент	Агент обнаружения, управляющий этой зоной
Тип зоны	Классификация (если настроена)
Уровень безопасности	Уровень приоритета (если настроен)

Шаг 3: Настройка типов зон

Для каждой зоны нажмите кнопку **Edit** (Редактировать), чтобы настроить:

- **Тип зоны:** Выберите соответствующую классификацию
  - Production, DMZ, Management, Workstation, IoT, Guest, Development, Staging, Backup
- **Уровень безопасности:** Установите приоритет защиты
  - Critical, High, Medium, Low
- **Разрешенные входящие:** Выберите зоны, которым разрешено подключаться к (to) данной зоне
  - Оставьте пустым, чтобы разрешить всё (нарушения не будут генерироваться)
  - Выберите конкретные зоны для применения строгих политик
- **Нажмите Save Configuration** (Сохранить конфигурацию)

Шаг 4: Просмотр анализа трафика

Перейдите на вкладку **Traffic Analysis**, чтобы увидеть:

- Визуализацию межзональных потоков трафика
- Количество соединений между зонами
- Порты, используемые для связи
- Статус нарушений для каждого потока

Использование фильтров

- **Зоны-источники:** Выберите одну или несколько зон для фильтрации по происхождению
- **Целевые зоны:** Выберите одну или несколько зон для фильтрации по назначению
- **Мин. соединений:** Отрегулируйте ползунок, чтобы показывать только высоконагруженный трафик
- **Только нарушения:** Переключитесь, чтобы сосредоточиться на нарушениях политик

Выбор режимов просмотра

- **Диаграмма потоков:** Лучше всего подходит для презентаций и общего обзора
- **Матричный вид:** Лучше всего подходит для детального анализа (рекомендуется)
- **Список:** Лучше всего подходит для быстрого сканирования

Шаг 5: Исследование нарушений

Перейдите на вкладку **Violations**:

1. Просмотрите список обнаруженных нарушений
2. Обратите внимание на важность (**High** или **Medium**)
3. Нажмите **Investigate** (Исследовать) на любом нарушении
4. Просмотрите детали соединений на уровне IP:
   - Исходные IP-адреса
   - Целевые IP-адреса
   - Количество соединений
   - Порты назначения

Шаг 6: Принятие мер

Для каждого нарушения примите решение:

Если трафик является легитимным

- Отредактируйте конфигурацию целевой зоны.
- Добавьте зону-источник в список **Allowed Inbound** (Разрешенные входящие).
- Сохраните конфигурацию.
- Нарушение больше не будет отображаться.

Если трафик является несанкционированным

- Задокументируйте находку.
- Исследуйте системы-источники.
- Внедрите правила брандмауэра для блокировки.
- При необходимости создайте тикет инцидента.

Сводные метрики

После настройки отслеживайте следующие ключевые метрики:

Метрика	Цель	Действие при превышении
Нарушения (Violations)	0	Немедленно расследовать
Межзональный трафик	Ожидаемые паттерны	Проверить новые потоки
Ненастроенные зоны	0	Завершить настройку зон

23 КОНФИГУРАЦИЯ ЗОН

В этом руководстве описывается, как настраивать сетевые зоны для применения политик безопасности и обнаружения несанкционированного трафика.

Понимание зон

Что такое сетевая зона?

Сетевая зона представляет собой логическую группировку IP-адресов, имеющих общие требования к безопасности. Зоны создаются автоматически на основе ваших расписаний обнаружения.

Свойства зоны

Свойство	Источник	Описание
Имя	Расписание обнаружения	Идентификатор зоны
IP-диапазон	Расписание обнаружения	Нотация CIDR (например, 10.160.160.0/24)
Агент	Расписание обнаружения	Управляющий агент обнаружения
Тип зоны	Конфигурация	Классификация безопасности
Уровень безопасности	Конфигурация	Приоритет защиты
Разрешенные входящие	Конфигурация	Разрешенные зоны-источники
Цвет	Конфигурация	Визуальный идентификатор
Описание	Конфигурация	Заметки в свободной форме

Типы зон

Выберите тип зоны, который лучше всего описывает сетевой сегмент:

Production

Использовать для: Бизнес-критичных систем, баз данных, серверов приложений.

Характеристики:

- Содержит реальные бизнес-данные
- Требует высокой доступности
- Подлежит контролю изменений
- Требует строгого контроля доступа

DMZ

- **Использовать для:** Сервисов, обращенных в интернет, веб-серверов, шлюзов API.
- **Характеристики:**

- Доступна из внешних сетей
- Первая линия обороны
- Должна иметь ограниченный внутренний доступ
- Требует частых обновлений безопасности

Management (Управление)

- **Использовать для:** Административного доступа, систем мониторинга, джамп-серверов.
- **Характеристики:**
  - Точка привилегированного доступа
  - Должна иметь доступ ко всем остальным зонам
  - Жестко контролируемый состав участников
  - Критически важен аудит логов

Workstation (Рабочая станция)

- **Использовать для:** Устройств конечных пользователей, десктопов, ноутбуков.
- **Характеристики:**
  - Высокий риск компрометации
  - Должна иметь ограниченный доступ к серверам
  - Зависит от активности пользователей
  - Требует защиты конечных точек

IoT

- **Использовать для:** Камер, датчиков, смарт-устройств, промышленных контроллеров.
- **Характеристики:**
  - Часто не имеют патчей или не подлежат обновлению
  - Ограниченные возможности безопасности
  - Должны быть сильно изолированы
  - Потенциальная точка входа для злоумышленников

Guest (Гостевая)

- **Использовать для:** Сетей посетителей, публичного WiFi, доступа подрядчиков.
- **Характеристики:**
  - Недоверенные устройства
  - Должна иметь доступ только в интернет
  - Нет доступа к внутренним системам
  - Ограниченная пропускная способность/сервисы

Development (Разработка)

- **Использовать для:** Рабочих станций разработчиков, серверов сборки, тестовых сред.
- **Характеристики:**
  - Ожидаются быстрые изменения
  - Может содержать чувствительный код

- Не должна иметь доступа к продуктовым данным
- Отделена от продуктовых сетей

Staging

- **Использовать для:** Предпродуктового тестирования, сред UAT.
- **Характеристики:**
  - Зеркальное отражение продуктовой конфигурации
  - Может содержать данные, похожие на продуктовые
  - Используется для финального тестирования
  - Не должна быть доступна из интернета

Backup (Резервное копирование)

- **Использовать для:** Серверов резервного копирования, архивных хранилищ, аварийного восстановления.
- **Характеристики:**
  - Содержит копии всех данных
  - Критически важна для восстановления
  - Должна иметь ограниченный сетевой доступ
  - Часто изолируется для защиты от программ-вымогателей

Уровни безопасности

Critical (Критический)

- **Когда использовать:** Зоны, содержащие самые конфиденциальные данные или системы.
- **Примеры:**
  - Системы обработки платежей
  - Медицинские записи
  - Финансовые базы данных
  - Серверы аутентификации
- **Нарушения:** Генерируют оповещения ВЫСОКОЙ (HIGH) степени важности.

High (Высокий)

- **Когда использовать:** Важные системы, требующие сильной защиты.
- **Примеры:**
  - Серверы приложений
  - Почтовые системы
  - Файловые серверы
  - Службы каталогов
- **Нарушения:** Генерируют оповещения СРЕДНЕЙ (MEDIUM) степени важности.

Medium (Средний)

- **Когда использовать:** Стандартные бизнес-системы.
- **Примеры:**
  - Среды разработки

- Внутренние инструменты
- Системы совместной работы
- **Нарушения:** Генерируют оповещения СРЕДНЕЙ (MEDIUM) степени важности.

Low (Низкий)

- **Когда использовать:** Менее чувствительные системы.
- **Примеры:**
- Гостевые сети
- Общедоступная информация
- Некритические сервисы
- **Нарушения:** Генерируют оповещения НИЗКОЙ (LOW) степени важности.

Настройка разрешенных входящих подключений (Allowed Inbound)

Понимание Allowed Inbound

Настройка **Allowed Inbound** определяет, каким зонам разрешено инициировать соединения к (to) данной зоне.

Правила конфигурации

Состояние Allowed Inbound	Поведение
Пусто (ничего не выбрано)	Разрешены все зоны — нарушения не генерируются
Выбрана одна или несколько	Разрешены только выбранные зоны — остальные генерируют нарушения

Рабочий процесс настройки

Шаг 1: Оценка текущего состояния

1. Перейдите в раздел **Network Zones** (Сетевые зоны).
2. Просмотрите все обнаруженные зоны.
3. Проверьте **Traffic Analysis** (Анализ трафика), чтобы увидеть текущие потоки данных.
4. Определите, какие зоны должны быть защищены.

Шаг 2: Классификация зон

Для каждой зоны:

1. Нажмите кнопку **Edit** (Редактировать).
2. Выберите подходящий тип зоны (**Zone Type**).
3. Выберите соответствующий уровень безопасности (**Security Level**).
4. Добавьте полезное описание (**Description**).
5. Выберите отличительный цвет (**Color**).
6. Нажмите **Save** (Сохранить).

Шаг 3: Определение политик

Для зон с высоким уровнем безопасности:

1. Нажмите кнопку **Edit** (Редактировать).
2. В поле **Allowed Inbound** (Разрешенные входящие) выберите разрешенные зоны.
3. Внимательно проверьте сделанный выбор.
4. Нажмите **Save** (Сохранить).

Шаг 4: Мониторинг нарушений

1. Перейдите на вкладку **Violations** (Нарушения).
2. Просмотрите все обнаруженные нарушения.
3. Расследуйте каждое нарушение.
4. Обновите политики или заблокируйте трафик соответствующим образом.

24 УПРАВЛЕНИЕ СОБЫТИЯМИ

Превратите шум алертов в полезную аналитику

Платформа управления событиями RS-Discovery (R-Sight) совершает революцию в подходе организаций к ИТ-операциям, преобразуя тысячи разрозненных алертов в значимые и практически применимые инсайты. Наша система на базе ИИ снижает утомляемость от алертов, прогнозирует сбои до того, как они повлияют на ваш бизнес, и автоматизирует решение проблем для бесперебойной работы ваших услуг.

Ключевые бизнес-преимущества

- **Снижение шума алертов на 90%** — Вы видите только то, что важно
- **Прогнозирование сбоев за 2–4 часа** — Устраняйте проблемы до их возникновения
- **Автоматизация устранения на 60%** — Самовосстанавливающаяся инфраструктура
- **Ускорение MTTR на 70%** — Разрешайте инциденты за минуты, а не часы
- **100% бизнес-контекст** — Мгновенно понимайте влияние на бизнес

Почему стоит выбрать управление событиями от RS-Discovery (R-Sight)?

Проблема

Современные ИТ-среды ежедневно генерируют тысячи событий из различных инструментов мониторинга, облачных платформ и приложений. Операционные группы сталкиваются с:

- Утомляемостью от избыточных уведомлений (alert fatigue)
- Сложностью выявления первопричин в комплексных системах
- Ручным, трудоемким процессом устранения инцидентов
- Отсутствием прогностических возможностей
- Разрозненными «силосами» мониторинга

Наше решение

Платформа управления событиями RS-Discovery (R-Sight) решает эти проблемы с помощью:

- **Единого сбора событий** — Единое окно для всех данных мониторинга
- **Интеллектуальной корреляции** — Автоматическая группировка связанных событий
- **Анализа на базе ИИ** — Выявление паттернов и прогнозирование сбоев
- **Автоматизированного исправления** — Возможности самовосстановления снижают объем ручной работы
- **Маппинга бизнес-услуг** — Связь технических событий с их влиянием на бизнес
- **Непрерывного обучения** — Повышение точности со временем

Как это работает

1. **Сбор** — Потоки событий поступают изо всех ваших инструментов мониторинга и платформ.
2. **Нормализация** — Различные форматы преобразуются в единую унифицированную модель.
3. **Корреляция** — Связанные события автоматически группируются с использованием нескольких стратегий.
4. **Анализ** — ИИ изучает паттерны, обнаруживает аномалии и выявляет первопричины.
5. **Действие** — Запускаются соответствующие ответные меры на основе влияния и политик.

Основные возможности

Универсальный хаб интеграций

Подключите все ваши инструменты мониторинга и платформы в одну единую систему:

- **Корпоративные инструменты мониторинга**
- **Облачные и современные платформы**
- **Логи и аналитика**

Интеллектуальная корреляция событий

Наша платформа использует четыре параллельные стратегии корреляции, чтобы гарантировать, что ни одно связанное событие не будет пропущено:

- **Временная корреляция:** Группирует события, происходящие в пределах настраиваемых временных окон. Если несколько систем выходят из строя в быстрой последовательности, они автоматически связываются.
- **Топологическая корреляция:** Использует связи из вашей CMDB для понимания зависимостей инфраструктуры. При сбое базы данных все события зависимых приложений коррелируются автоматически.
- **Распознавание паттернов:** Идентифицирует схожие сигнатуры событий с помощью ИИ. Повторяющиеся проблемы обнаруживаются, даже если они проявляются по-разному.
- **Корреляция с услугами:** Связывает события, влияющие на одну и ту же бизнес-услугу, независимо от используемого технологического стека.

Интеллект на базе ИИ

Обнаружение аномалий

- **Изучение базовых показателей** — Понимает ваши нормальные операционные паттерны.
- **Динамические пороги** — Регулирует чувствительность в зависимости от времени суток и бизнес-циклов.
- **Статистический анализ** — Использует продвинутые алгоритмы для выявления выбросов.

Прогнозная аналитика

- **Прогнозирование сбоев** — Предупреждает за 2–4 часа до критических отказов.
- **Прогнозирование мощностей** — Проектирует исчерпание ресурсов.
- **Анализ трендов** — Выявляет паттерны постепенной деградации.

Машинное обучение

- **Непрерывное обучение** — Повышает точность с каждым решенным инцидентом.
- **Обнаружение паттернов** — Автоматически находит новые схемы корреляции.
- **Предложения по решению** — Рекомендует исправления на основе исторических данных.

Влияние на бизнес-услуги

Понимание влияния на бизнес имеет решающее значение для приоритезации.

Жизненный цикл обработки событий

1. Интеллектуальный прием

События поступают на платформу через множество каналов и немедленно обрабатываются:

Методы сбора

- Прием вебхуков в реальном времени для мгновенных оповещений
- Опрос по API (polling) для устаревших систем
- Приемники Syslog и SNMP-трапов
- Интеграция с очередями сообщений
- Прямые подключения к базам данных

Умная обработка

- Автоматическое распознавание и проверка формата
- Синхронизация временных меток между часовыми поясами
- Аутентификация и проверка источника
- Первичное назначение важности и категории

2. Обогащение контекстом

Каждое событие автоматически дополняется бизнес- и операционным контекстом:

Интеграция с CMDB

- Идентификация затронутых конфигурационных единиц
- Привязка к бизнес-услугам и приложениям
- Добавление информации о владельцах и ответственных командах
- Включение данных о местоположении и критичности

Исторические данные

- Связывание с предыдущими похожими инцидентами
- Предоставление истории решений
- Корреляция с недавними изменениями
- Выявление повторяющихся паттернов

Осведомленность о среде

- Проверка статуса окон техобслуживания
- Сверка с календарями развертывания
- Учет текущей нагрузки на систему
- Обзор связанных активных событий

3. Анализ на базе ИИ

Наш ИИ-движок параллельно выполняет несколько видов анализа:

Шумоподавление

- Устранение дубликатов событий
- Подавление «дребезга» (flapping) алертов
- Фильтрация оповещений, связанных с техобслуживанием
- Сведение «штормов» алертов к единичным инцидентам

Корреляционный анализ

- Группировка связанных событий во временных окнах
- Обход зависимостей инфраструктуры
- Выявление общих первопричин
- Формирование полной картины инцидента

Идентификация первопричины

- Анализ последовательностей событий
- Отслеживание цепочек зависимостей
- Расчет показателей достоверности
- Предоставление выводов на основе доказательств

4. Автоматизированное реагирование

На основе анализа запускаются соответствующие действия:

Умные уведомления

- Маршрутизация нужным командам на основе их компетенций
- Эскалация в соответствии с требованиями SLA
- Объединение нескольких алертов в сводные отчеты
- Предоставление бизнес-контекста в уведомлениях

Действия по самовосстановлению

- Выполнение предварительно утвержденных сценариев исправления
- Автоматическое масштабирование ресурсов
- Перенаправление трафика во время сбоев
- Активация резервных систем

Управление знаниями

- Создание тикетов инцидентов с полным контекстом
- Ссылки на соответствующие регламенты (runbooks)
- Автоматическое обновление базы знаний
- Документирование решения для использования в будущем

Классификация событий

Категории событий

Платформа интеллектуально классифицирует события для правильной маршрутизации и обработки:

- **Инфраструктурные события:** Состояние и сбои оборудования, сетевое соединение и производительность, емкость хранилищ, условия среды в ЦОД.
- **События приложений:** Доступность и состояние сервисов, метрики производительности и деградация, уровни ошибок и исключений, проблемы обработки транзакций.
- **События безопасности:** Попытки несанкционированного доступа, нарушения политик безопасности, отклонения от требований compliance, проблемы с сертификатами и учетными данными.
- **Бизнес-события:** Статус соблюдения SLA, оповещения о планировании мощностей, управление лицензиями, отслеживание бюджета и затрат.

Структура уровней важности

События автоматически классифицируются по степени важности с соответствующими протоколами реагирования:

Важность	Время реакции	Уведомление	Эскалация	Влияние на бизнес
Критический	15 минут	Немедленно — все каналы	Автоматически	Простой Prod, потеря данных, взлом
Значительный	1 час	Срочно — основные каналы	30 минут	Деградация услуги, высокий уровень ошибок
Незначительный	4 часа	Стандартно — каналы команд	2 часа	Некритические ошибки, предупреждения
Предупреждение	8 часов	Плановая сводка	По необходимости	Назревающие проблемы, прогнозы
Информация	По возможности	Ежедневный отчет	Нет	Обновления системы, подтверждения

Продвинутые интеллектуальные функции

Умное шумоподавление

Платформа значительно снижает утомляемость от алертов с помощью интеллектуальной фильтрации:

- **Технология дедупликации:** Автоматически группирует идентичные события, отслеживает количество повторений в одном алерте и использует алгоритмы сопоставления для объединения схожих событий.
- **Управление штормами событий:** Обнаруживает паттерны лавинообразных алертов, автоматически ограничивает избыточные уведомления и предоставляет сводки по «шторму» вместо сотен отдельных оповещений.
- **Интеллект режима техобслуживания:** Автоматически подавляет ожидаемые алерты во время работ, пропуская при этом критические сбои, и автоматически возобновляет мониторинг по завершении окна обслуживания.

Прогнозный анализ сбоев

Опережайте проблемы благодаря прогностическим возможностям:

- **Система раннего предупреждения:** Обнаруживает аномалии за 2–4 часа до сбоев, выявляет постепенную деградацию и предупреждает о трендах исчерпания мощностей.
- **Оценка рисков:** Рассчитывает вероятность будущих инцидентов, предоставляет показатели достоверности прогнозов и предлагает превентивные действия.
- **Изучение паттернов:** Самостоятельно обучается на уникальных особенностях вашей среды, учитывает сезонные тренды и распознает «сигнатуры» сбоев, повышая точность со временем.

Платформа автоматически:

- Анализирует последовательность событий для поиска триггера
- Обходит зависимости инфраструктуры
- Рассчитывает показатели достоверности для каждой гипотезы
- Предоставляет доказательства, подтверждающие выводы
- Предлагает варианты исправления на основе первопричины

Метрики успеха

Отслеживайте уровень зрелости управления событиями с помощью этих KPI:

Операционная эффективность

Метрика	Цель	Типовое достижение
Снижение шума алертов	80%	85–95%
Ср. время обнаружения (MTTD)	< 5 мин	2–3 мин
Ср. время решения (MTTR)	Снижение на 50%	Снижение на 60–70%
Уровень автоматич. решения	40%	50–60%

Влияние на бизнес

Метрика	Цель	Типовое достижение
Предотвращено инцидентов	20 в месяц	30–40 в месяц
Предотвращено простоев	10 ч/мес	15–20 ч/мес
Уровень ложных срабатываний	< 5%	2–3%
Соблюдение SLA	99.9%	99.95%

Производительность платформы

Метрика	Цель	Типовое достижение
Скорость обработки событий	10к / мин	15к / мин
Точность корреляции	> 90%	92–95%
Точность прогнозов	> 80%	85–90%
Задержка анализа	< 1 сек	0.5–0.8 сек

Реальные примеры использования

Финансовые услуги

- **Проблема:** Крупный банк, обрабатывающий более 50 000 событий ежедневно в 500+ приложениях.
- **Решение:** Внедрение управления событиями RS-Discovery (R-Sight) с фокусом на транзакционные системы.
- **Результаты:**
  - Снижение шума на 92%.
  - Предупреждение о сбоях БД за 4 часа.
  - Экономия $2 млн ежегодно за счет предотвращения простоев.

Платформа электронной коммерции

- **Проблема:** Онлайн-ритейлер, испытывающий трудности с подготовкой к «Черной пятнице».
- **Решение:** Внедрение прогнозной аналитики и автомасштабирования.
- **Результаты:**
  - Нулевой простой в пиковый сезон.
  - Снижение ручного вмешательства на 65%.
  - В 3 раза более быстрое разрешение инцидентов.

Здравоохранение

- **Проблема:** Сеть больниц, требующая доступности систем в режиме 24/7.
- **Решение:** Развертывание с упором на критически важные системы жизнеобеспечения пациентов.
- **Результаты:**
  - Аптайм критических систем 99.99%.
  - Снижение количества звонков в нерабочее время на 78%.
  - Успешность аудитов соответствия выросла до 100%.

25 ИСТОЧНИКИ СОБЫТИЙ И ИНТЕГРАЦИЯ

RS-Discovery (R-Sight) обеспечивает универсальное подключение ко всей вашей экосистеме мониторинга. Наша платформа поглощает события из любых инструментов, нормализует различные форматы и создает единое операционное представление всех ваших систем.

Нормализация событий

Унифицированная модель событий

Любое событие, независимо от источника, приводится к нашему стандартному формату:

Поле	Описание	Примеры
source	Идентификатор инструмента мониторинга	"nagios", "zabbix", "prometheus"
sourceId	Уникальный ID из исходной системы	"NAG-12345", "ZBX-67890"
severity	Нормализованный уровень важности	critical, major, minor, warning, info
title	Краткое описание события	"Database Connection Failed"
description	Подробная информация о событии	"MySQL connection timeout after 30s"
timestamp	Время возникновения события	Формат ISO 8601
hostname	Затронутый хост	"db-prod-01.example.com"
service	Затронутый сервис	"mysql", "apache", "redis"
category	Классификация события	hardware, software, network, security

Маппинг уровней важности

Уровни важности каждого источника сопоставляются автоматически:

Источник	Critical	Major	Minor	Warning	Info
Nagios	CRITICAL, DOWN	—	UNKNOWN	WARNING	OK, UP
Zabbix	Disaster	High	Average	Warning	Information
Prometheus	critical	error	—	warning	info
CloudWatch	ALARM	—	INSUFFICIENT_DATA	—	OK
Syslog	Emergency, Alert, Critical	Error	—	Warning	Notice, Info, Debug

Методы интеграции

1. Интеграция через Webhook (Рекомендуется)

Самый быстрый и эффективный метод для событий в реальном времени.

Процесс настройки:

1. Сгенерируйте URL webhook в консоли RS-Discovery (R-Sight).
2. Настройте источник на отправку событий на этот URL.
3. Установите токен аутентификации.
4. Протестируйте на тестовом событии.

2. Опрос по API

Для систем, которые не поддерживают webhook.

- **Интервал опроса:** от 30 секунд до 5 минут.
- **Кейсы:** Устаревшие системы, ограничения фаервола, импорт исторических данных.

3. Протокольные слушатели (Protocol Listeners)

Для стандартных сетевых протоколов:

- **Syslog:** UDP/TCP порты 514, 1514.
- **SNMP Traps:** UDP порт 162.
- **Особенности:** Высокопроизводительные приемники с автоматическим определением формата.

Пользовательская интеграция через API

RS-Discovery (R-Sight) предоставляет REST API для систем, способных отправлять HTTP POST запросы.

- **Аутентификация:** Используйте Bearer token в заголовке Authorization.
- **Формат данных:** JSON.
- **Структура:** Должна включать source, severity, title и hostname/service.

Продвинутые возможности

Обогащение событий (Event Enrichment)

События автоматически дополняются следующими данными:

- **Контекст CMDB:** Детали конфигурационных единиц, маппинг бизнес-услуг, информация о владельцах/командах и зависимости.
- **Исторический контекст:** Предыдущие случаи возникновения, история решений, связанные изменения и сравнение с базовыми показателями.

Фильтрация и маршрутизация

- **Препроцессинг:** Фильтрация по важности, подавление во время техобслуживания и обнаружение дубликатов на входе.
- **Умная маршрутизация:** Назначение ответственных команд на основе владения услугой, навыков (skill-based routing) и путей эскалации.

Производительность и лимиты

Скорость обработки (Ingestion Rates)

Тариф	Событий в минуту	Пиковая нагрузка	Хранение
Standard	1	5	90 дней
Professional	10	50	180 дней
Enterprise	100	500	365 дней

Гарантии обработки

- **Доставка «хотя бы один раз»** — события никогда не теряются.
- **Сохранение порядка** — в рамках одного источника.
- **Идемпотентность** — предотвращение дублирования.
- **Dead Letter Queue (DLQ)** — очередь для восстановления событий, которые не удалось обработать.

Безопасность и соответствие (Security & Compliance)

- **Аутентификация:** Поддержка API-токенов, OAuth 2.0 и взаимного TLS (mTLS) на базе сертификатов.
- **Защита данных:** Шифрование TLS 1.2+ при передаче и AES-256 при хранении. Автоматическое маскирование персональных данных (PII).

26 ИНТЕЛЛЕКТУАЛЬНАЯ КОРРЕЛЯЦИЯ СОБЫТИЙ

Превратите тысячи алертов в значимые инциденты с помощью многоуровневого движка корреляции RS-Discovery (R-Sight). Наша платформа автоматически группирует связанные события, выявляет первопричины и снижает уровень «шума» алертов до 90%.

Как работает корреляция

RS-Discovery (R-Sight) использует четыре параллельные стратегии корреляции, которые работают совместно, гарантируя, что ни одно связанное событие не будет упущено.

Четыре стратегии корреляции

1. Временная корреляция (На основе времени)

Как это работает: События, происходящие в пределах 5-минутного скользящего окна, автоматически оцениваются на предмет корреляции. Система интеллектуально группирует события на основе их близости во времени: чем меньше интервал между событиями, тем выше их коэффициент корреляции.

Ключевые особенности:

- Настраиваемые временные окна (по умолчанию: 5 минут).
- Автоматическое обнаружение «всплесков» для часто повторяющихся алертов.
- Подавление штормов алертов для предотвращения перегрузки уведомлениями.
- Распознавание паттернов последовательности событий.

Реальный пример: Если база данных выходит из строя в 10:00, все ошибки приложений, возникшие в период с 09:55 до 10:05, автоматически объединяются в один инцидент, отображая полную хронологию воздействия.

Преимущества:

- Сводит штормы алертов к единичным инцидентам.
- Предоставляет полную временную шкалу событий.
- Выявляет каскадные сбои.
- Сохраняет последовательность событий.

2. Топологическая корреляция (Интеллект CMDB)

Как это работает: Использует обнаруженные взаимосвязи инфраструктуры из CMDB для понимания зависимостей сервисов. При возникновении события система автоматически проверяет связанные конфигурационные единицы (КЕ) на наличие коррелирующих проблем.

Ключевые особенности:

- Использует обнаруженные связи между КЕ.
- Проходит по цепочке зависимостей глубиной до 3 уровней.

- 10-минутное окно корреляции для инфраструктурных событий.
- Критические связи получают более высокий балл корреляции (0.9 против 0.7).

Анализируемые типы связей:

- **Runs On (Запускается на)** — Приложения на серверах.
- **Depends On (Зависит от)** — Зависимости между сервисами.
- **Connects To (Подключается к)** — Сетевые соединения.
- **Hosted By (Размещен на)** — Виртуальная инфраструктура.

Когда сервер базы данных выходит из строя, система автоматически коррелирует:

- Ошибки подключения приложений
- Оповещения о таймаутах веб-серверов
- Сбои проверок состояния (health checks) балансировщика нагрузки
- Все оповещения зависимых сервисов

Преимущества:

- Автоматически отображает влияние на всю инфраструктуру
- Отделяет истинную первопричину от симптомов
- Понимает сложные зависимости сервисов
- Драматически сокращает время на поиск неисправностей

3. Корреляция на основе паттернов (Сопоставление сигнатур)

Как это работает: События с идентичными сигнатурами корреляции автоматически группируются. Система генерирует сигнатуры на основе MD5 из характеристик событий и сопоставляет их в пределах 1-часового окна ретроспективного анализа.

Ключевые особенности:

- Точное сопоставление на основе сигнатур
- Самый высокий показатель достоверности (0.9) для совпадений по паттернам
- 1-часовое окно распознавания
- Автоматическая дедупликация

Примеры распознавания паттернов:

- Повторяющиеся ошибки приложений с одинаковым стеком вызовов (stack trace)
- Идентичные проблемы сетевого подключения
- Повторяющиеся ошибки аутентификации

Преимущества:

- Устраняет дублирование инцидентов
- Мгновенно распознает повторяющиеся проблемы

- Группирует идентичные проблемы в разных системах

4. Сервисная корреляция (Бизнес-контекст)

Как это работает: Группирует события, влияющие на одну и ту же бизнес-услугу или приложение, независимо от базовой инфраструктуры. Использует 15-минутное окно для фиксации проблем, связанных с услугой.

Ключевые особенности:

- Группировка с учетом специфики услуг и приложений
- 15-минутное окно корреляции
- Показатель достоверности 0.8 для совпадений по услугам
- Учет влияния на бизнес

Сервисная корреляция в действии: Когда возникают проблемы с платежным сервисом:

1. Таймауты платежного шлюза
2. Сбои транзакций в базе данных
3. Задержки ответов API
4. Сообщения об ошибках для клиентов — Все это объединяется в один инцидент.

Оценка корреляции и объединение

Как рассчитываются баллы

Каждая стратегия корреляции выдает показатель достоверности (confidence score) от 0 до 1:

Стратегия	Диапазон баллов	Порог	Вес
Temporal	0.5–1.0	>0.5	На основе близости во времени
Topology	0.6–0.9	>0.6	Критичность связей
Pattern	0.9	Точное совпадение	Максимальное доверие
Service	0.8	Совпадение сервиса	Фиксированный балл

Процесс интеллектуального слияния

Когда событие соответствует нескольким стратегиям:

- **Побеждает максимальный балл** — берется самая высокая достоверность из всех стратегий.
- **Отслеживание причин** — фиксируется, какие именно стратегии сработали.
- **Сбор доказательств** — собираются подтверждающие данные от каждой стратегии.

- **Финальный порог** — события с итоговым баллом >0.7 коррелируются в инцидент.

Анализ первопричин

Автоматическое определение первопричины

Движок корреляции автоматически определяет наиболее вероятную первопричину, используя несколько техник:

1. **Временной анализ**
   - Поиск самого раннего события уровня **Критический** или **Значительный** в группе корреляции.
   - Идентификация событий, запустивших каскад последующих алертов.
2. **Обход топологии**
   - Анализ зависимостей инфраструктуры.
   - Маппинг взаимосвязей услуг.
   - Отслеживание путей распространения влияния.
3. **Распознавание паттернов**
   - Использование исторических паттернов решения инцидентов.
   - Данные о зафиксированных ранее первопричинах.
   - Сигнатуры известных проблем.

Достоверность первопричины

Каждая определенная первопричина включает в себя:

- Показатель достоверности (0–100%).
- Подтверждающие доказательства.
- Визуализацию цепочки влияния.
- Рекомендации по устранению.

Группы корреляции и управление ими

Особенности групп корреляции

Когда события коррелируются, система:

Создает единое представление инцидента:

- Единый **ID корреляции** для всех связанных событий.
- Полная временная шкала (timeline) инцидента.
- Агрегированная информация о важности и влиянии.
- Объединенный бизнес-контекст.

Предоставляет глубокую аналитику:

- Количество и распределение событий.
- Длительность инцидента.
- Разбивку по уровням важности.
- Список затронутых конфигурационных единиц (КЕ).
- Идентификацию общих паттернов.

Позволяет выполнять «умные» действия:

- Единое уведомление для всей группы событий.
- Создание одного консолидированного запроса.
- Групповые действия по исправлению (remediation).
- Унифицированная отчетность.

Производительность и оптимизация

Возможности масштабирования

Платформа RS-Discovery (R-Sight) спроектирована для работы в высоконагруженных средах:

- **Обработка больших объемов:** Параллельное выполнение стратегий корреляции позволяет обрабатывать тысячи событий в минуту без задержек.
- **Оптимизация:** Использование эффективных алгоритмов оценки (scoring) и оптимизированных запросов к базе данных гарантирует минимальный отклик.

KPI	Цель	Описание
Снижение шума	> 85%	Процент коррелированных событий
Точность корреляции	> 90%	Правильно сгруппированные события
Ложные срабатывания	< 5%	Ошибочно связанные события
Точность RCA	> 80%	Правильное определение первопричины

Непрерывное обучение

Движок корреляции RS-Discovery (R-Sight) постоянно совершенствуется, используя данные о прошлых инцидентах для повышения точности будущих прогнозов:

Изучение паттернов

- **Анализ решенных инцидентов:** Система запоминает, какие цепочки событий привели к подтвержденным сбоям.
- **Идентификация новых закономерностей:** ИИ находит скрытые зависимости, которые не были описаны в правилах.
- **Корректировка баллов достоверности:** Автоматическое повышение веса стратегий, которые чаще всего оказывались верными.
- **Обновление библиотеки сигнатур:** Автоматическое создание новых «цифровых отпечатков» проблем.

Интеграция обратной связи

- **Ручные корректировки:** Когда оператор объединяет или разделяет события вручную, система учитывает это как обучающий сигнал.
- **Валидация первопричины:** Подтверждение того, что RCA (анализ первопричин) был выполнен верно.

- **Отслеживание паттернов решения:** Сопоставление успешных сценариев восстановления с конкретными группами алертов.

Примеры сценариев использования

Пример 1: Сбой базы данных

Сценарий: Отказ основного сервера базы данных.

- **Сгенерированные события:**
  - База данных недоступна (**Critical**)
  - 15 ошибок подключения приложений (**Major**)
  - 3 таймаута веб-сервера (**Major**)
  - 50+ ошибок пользовательских сессий (**Warning**)
  - Сбои проверки состояния (health check) балансировщика нагрузки (**Major**)

Результат корреляции:

- **Единый инцидент:** «Сбой базы данных, влияющий на Production»
- **Первопричина:** Аппаратный сбой сервера БД
- **Эффективность:** 70 событий → 1 инцидент
- **Использованные стратегии:** Топологическая (0.9), Временная (0.8), Сервисная (0.8)
- **Время корреляции:** 0,3 секунды

Пример 2: Сбой сетевого коммутатора

Сценарий: Периодические сбои в работе центрального сетевого коммутатора.

- **Сгенерированные события:**
  - Оповещения о «дребезге» (flapping) портов коммутатора
  - 200+ алертов о потере связи с устройствами
  - Ошибки таймаута приложений
  - Предупреждения о деградации услуг

Результат корреляции:

- **Единый инцидент:** «Нестабильность центрального коммутатора SW-01»
- **Первопричина:** Баг в прошивке коммутатора
- **Эффективность:** 247 событий → 1 инцидент
- **Использованные стратегии:** Топологическая (0.9), Паттерны (0.9), Временная (0.7)
- **Время корреляции:** 0,5 секунды

Пример 3: Утечка памяти в приложении

Сценарий: Приложение постепенно потребляет память в течение 2 часов.

- **Сгенерированные события:**
  - Предупреждения об использовании памяти (каждые 10 мин)

- Оповещения об увеличении длительности сборки мусора (GC)
- Деградация времени ответа
- Итог: ошибка OutOfMemory

Результат корреляции:

- **Единый инцидент:** «Исчерпание памяти приложения»
- **Первопричина:** Утечка памяти в платежном сервисе
- **Эффективность:** 15 событий → 1 инцидент
- **Использованные стратегии:** Сервисная (0.8), Паттерны (0.9), Временная (0.6)
- **Прогноз:** Система предсказала отказ за 90 минут до критического падения.

Интеграция с другими функциями

Интеграция с ИИ-анализом

Скоррелированные события автоматически направляются для:

- **Оценки аномалий** — определение степени отклонения инцидента от нормы.
- **Прогнозного анализа** — расчет вероятности каскадного расширения проблемы.
- **Предложений по решению** — поиск аналогичных случаев в базе знаний.
- **Оценки влияния** — определение масштаба последствий для системы.

Интеграция с автоматизацией

Группы корреляции запускают:

- **Рабочие процессы автоисправления** — выполнение скриптов для устранения типовых сбоев.
- **Интеллектуальную маршрутизацию** — доставку уведомлений именно тем специалистам, которые отвечают за данный узел.
- **Эскалацию по приоритетам** — повышение уровня важности при отсутствии реакции.
- **Исполнение Runbook** — предоставление инженерам пошаговых инструкций.

Маппинг бизнес-услуг

Корреляции обогащаются следующими данными:

- Контекст бизнес-услуги (какой бизнес-процесс затронут).
- Анализ влияния на клиентов.
- Отслеживание соблюдения SLA.
- Расчет потерь выручки в режиме реального времени.

Измерение успеха

Ключевые показатели эффективности (KPI)

Отслеживайте эффективность корреляции с помощью этих метрик:

KPI	Цель	Описание
Снижение шума	>85%	Процент событий, объединенных в группы.
Точность корреляции	>90%	Доля правильно сгруппированных событий.
Ложные срабатывания	<5%	Ошибочно связанные между собой события.
Точность RCA	>80%	Правильное определение первопричины с первого раза.
Время корреляции	<1 сек	Задержка обработки движком.
Улучшение MTTD	-50%	Сокращение времени обнаружения проблем.

27 АНАЛИЗ СОБЫТИЙ НА БАЗЕ ИИ

Превратите управление событиями из реактивного «тушения пожаров» в проактивное предотвращение с помощью интегрированных возможностей ИИ RS-Discovery (R-Sight). Наша платформа использует машинное обучение для обнаружения аномалий, прогнозирования сбоев и предложения вариантов решения на основе особенностей вашей среды.

Обзор ИИ-анализа

Движок ИИ RS-Discovery (R-Sight) работает непрерывно в фоновом режиме, анализируя каждое событие на предмет паттернов, аномалий и прогностических сигналов.

Ключевые возможности ИИ

1. Обнаружение аномалий

Изучение статистических базовых показателей

Система непрерывно анализирует нормальные паттерны поведения вашей инфраструктуры:

- **Экспоненциальное скользящее среднее (EMA):** Использование коэффициента сглаживания **0.1** для адаптации к изменениям.
- **Отслеживание стандартного отклонения:** Расчет волатильности для каждой метрики.
- **Поддержка границ Min/Max:** Установление динамического «коридора» нормальных значений.
- **Валидация данных:** Для построения точного прогноза требуется минимум **10 образцов** данных.

Оценка аномальности (0-100) Каждое событие получает оценку на основе степени отклонения от базовой линии:

Диапазон баллов	Интерпретация	Действие
0-20	Нормальное поведение	Мониторинг
20-50	Незначительное отклонение	Отслеживание тренда
50-80	Значительная аномалия	Оповещение команд
80-100	Критическая аномалия	Немедленное реагирование

Примеры из практики:

- **Процессор:** Обычно загружен на 30-40%, резкий скачок до 95% → **Балл: 85**
- **База данных:** Обычно 100 запросов/сек, падение до 5 запросов/сек → **Балл: 78**
- **Память:** Постепенное увеличение потребления в течение нескольких дней → **Балл: 45-60**

2. Система обучения паттернам

Отслеживание сценариев решения ИИ обучается на каждом закрытом инциденте:

- **Генерация сигнатур паттернов:** Создание уникальных цифровых отпечатков для событий.
- **Фиксация способов решения:** Запоминание того, как именно была устранена проблема.
- **Анализ длительности:** Расчет среднего времени, необходимого для восстановления (MTTR).
- **Отслеживание успеха:** Мониторинг эффективности принятых мер для исключения повторных сбоев.

Чему обучается система:

1. **Связи между событиями:** Какие алерты обычно предшествуют критическому сбою.
2. **Эффективность действий:** Какие скрипты автоматизации или ручные действия приводят к самому быстрому результату.
3. **Временные зависимости:** Как время суток или день недели влияют на критичность определенных событий.

Развитие библиотеки паттернов

ИИ не просто накапливает данные, он классифицирует их по мере накопления опыта:

- **После 3 случаев:** Появление базовых рекомендаций.
- **После 10 случаев:** Рекомендации с высоким уровнем достоверности.
- **После 50 случаев:** Паттерн становится кандидатом на **полную автоматизацию решения**.

3. Прогнозный анализ сбоев

Раннее предупреждение (за 2–4 часа)

Система анализирует косвенные признаки, чтобы предсказать критический сбой до того, как он затронет пользователей.

Изучение «сигнатур» сбоев:

- **Ретроспективный анализ:** ИИ изучает события за 2 часа до каждого критического сбоя.
- **Поиск предвестников:** Идентификация предупреждающих событий, которые регулярно предшествуют инциденту.
- **Расчет времени упреждения:** Определение среднего интервала между «предвестником» и «катастрофой».

Категории прогнозов:

- **Исчерпание памяти:** На основе паттернов постепенного роста потребления RAM.

- **Перегрузка CPU:** Длительная высокая нагрузка в сочетании с ростом очереди задач.
- **Переполнение диска:** Тренды потребления дискового пространства.
- **Проблемы со связью:** На основе учащающихся кратковременных разрывов соединения.
- **Падение приложений:** На основе ускорения темпа роста ошибок.

Пример вывода прогноза:

Оповещение о прогнозе:

- **Тип:** Сбой базы данных
- **Вероятность:** 85%
- **Время до сбоя:** 2.5 часа
- **Достоверность:** Высокая (на основе 15 похожих случаев)

Доказательная база:

- Пул соединений заполнен на 80%
- Время ответа на запросы растет
- Тренд потребления памяти направлен вверх

Превентивные действия:

- Увеличить размер пула соединений
- Перезапустить сервис БД в период низкой нагрузки
- Очистить кэш запросов

4. Анализ первопричин на базе ИИ

Многофакторный анализ

При возникновении критических событий ИИ проводит комплексную диагностику, объединяя технические метрики и логику:

Подготовка контекста

- **Сбор данных о КЕ:** Идентификация затронутых конфигурационных единиц.
- **Анализ временного окна:** Сбор всех событий за последние 24 часа.
- **Исторический поиск:** Проверка паттернов за последние 30 дней для поиска аналогий.

Интеграция с генеративным ИИ

- Предоставляет выводы на естественном языке, понятном человеку.
- Выдает структурированные инсайты (JSON/Text).
- Включает резервные алгоритмы анализа на случай недоступности основного сервиса ИИ.

Пример вывода анализа:

Событие: Пул соединений базы данных исчерпан

Анализ ИИ:

- **Первопричина:** Утечка соединений в приложении сервиса платежей.
- **Сопутствующие факторы:**
  - Недавнее развертывание (деплой) 3 часа назад.
  - Постепенное накопление соединений.
  - Отсутствие настроенного таймаута соединений.
- **Доказательства:**
  - Линейный рост количества соединений.
  - Все соединения исходят от payment-service-v2.1.
  - Проблема началась сразу после деплоя в 14:00.
- **Рекомендуемые действия:**

1. Перезапустить сервис платежей (немедленно).
2. Настроить таймаут соединений (приоритет 1).
3. Исправить утечку в коде (приоритет 2).

- **Достоверность:** 92%

Особенности машинного обучения

Цикл непрерывного обучения

Платформа не остается статичной — она умнеет с каждым закрытым инцидентом:

1. **Сбор данных:** Фиксация каждого алерта и реакции инженера на него.
2. **Оценка обратной связи:** Если инженер отметил рекомендацию как «полезную», вес этого паттерна в модели увеличивается.
3. **Обновление модели:** Регулярное переобучение на новых данных для учета изменений в архитектуре вашей сети.
4. **Валидация точности:** Автоматическое сравнение предсказанных первопричин с фактическими результатами расследований.

Механизмы обучения

1. Эволюция базовых показателей (Baselines)

ИИ RS-Discovery (R-Sight) не просто фиксирует статистику, он адаптируется к изменениям вашей среды в реальном времени:

- **Экспоненциальное скользящее среднее:** Обновляет «норму» при каждом новом событии, что позволяет системе не реагировать на естественный, плавный рост нагрузки.
- **Распознавание сезонности:** ИИ понимает цикличные паттерны (например, пики трафика каждый понедельник утром или в конце месяца) и не считает их аномалиями.
- **Сохранение состояний:** Базовые показатели фиксируются каждые 100 выборок, что гарантирует сохранность накопленного «опыта» системы.

2. Обучение паттернам корреляции

Система запоминает, как события связаны между собой:

- Фиксирует успешные группировки событий, подтвержденные операторами.
- Выявляет типичные цепочки событий, ведущие к конкретным первопричинам.
- Отслеживает эффективность принятых решений, чтобы в будущем предлагать только проверенные методы.

3. Распознавание признаков сбоя

ИИ выступает в роли «детектива», анализируя события, которые предшествовали аварии:

- Категоризирует типы отказов (база данных, сеть, приложение).
- Рассчитывает коэффициент сходства текущей ситуации с прошлыми инцидентами.
- Постоянно повышает точность прогнозов, обучаясь на каждом новом инциденте.

Триггеры ИИ-анализа

Автоматический запуск

События автоматически ставятся в очередь на глубокий ИИ-анализ при выполнении следующих условий:

Триггер	Условие запуска	Тип анализа
Высокая важность	События уровней Critical или Major	Полный ИИ-анализ инцидента
Обнаружение аномалии	Отклонение метрик от базовой линии	Оценка аномальности и скоринг
Группа корреляции	Появление нескольких связанных событий	Поиск первопричины (Root Cause)
Совпадение паттерна	Сходство с известными ранее проблемами	Рекомендация проверенного решения
Трендовые проблемы	Постепенная деградация показателей	Прогнозный анализ времени до сбоя

Практическое применение и кейсы

Кейс 1: Обнаружение утечки памяти

Сценарий: Приложение с постепенной утечкой памяти, которую сложно заметить обычными порогами.

Процесс ИИ-детекции:

1. **Baseline:** Система определяет норму потребления (например, **2 ГБ**).
2. **Обнаружение:** Фиксируется аномальный рост в течение 4 часов.
3. **Скоринг:** Оценка аномальности растет: 20→40→60.
4. **Прогноз:** ИИ сопоставляет текущий тренд с прошлыми инцидентами и прогнозирует **OutOfMemory** через 2 часа.

Результат ИИ:

- Генерация оповещения за 2 часа до падения.
- Идентификация конкретного сервиса-виновника.
- Рекомендация перезапуска в окно низкой активности.

Кейс 2: Деградация производительности базы данных

Сценарий: Резкое замедление выполнения запросов.

Анализ ИИ:

- **Baseline:** Время ответа 50 мс. **Текущее:** 500 мс (Балл аномалии: 78).
- **Корреляция:** ИИ находит связанные события:
  - Высокая нагрузка на CPU сервера БД.
  - Ожидания блокировок (Lock wait timeouts).
  - Предупреждения пула соединений.
- **Первопричина:** Отсутствие индекса после недавнего деплоя.

Рекомендации ИИ:

- **Срочно:** Завершить длительные блокирующие запросы.
- **Краткосрочно:** Добавить предложенный индекс.
- **Долгосрочно:** Провести ревью оптимизации запросов в CI/CD.

Кейс 3: Каскадный сбой услуги

Сценарий: Проблемы с платежным шлюзом вызывают отказ всей платформы.

Корреляция и анализ:

- **Масштаб:** 50+ событий сгруппированы за 30 секунд.
- **Идентификация:** Первопричина — таймаут внешнего платежного шлюза.
- **Маппинг влияния:** Визуализация того, как задержка в одном API парализовала корзину и личный кабинет.

Действия ИИ:

- Объединение всех 50 алертов в один инцидент.
- Предложение перенаправить трафик на резервный шлюз.
- Прогноз восстановления системы через 15 минут после переключения.

Эффективность ИИ-анализа (Metrics)

Метрика	Цель	Типовой результат
Точность обнаружения аномалий	>85%	88–92%
Уровень предсказания сбоев	>70%	75–80%
Точность определения первопричины	>80%	82–85%

Успешность предложенных решений	>60%	65–70%
Уровень ложных срабатываний	<10%	5–7%

Показатели производительности обработки

- **Задержка анализа (Analysis Latency):** 0.8–1.2 сек (Цель: <2 сек).
- **Событий проанализировано в минуту:** 150–200 (Цель: >100).
- **Скорость сопоставления паттернов:** 50–80 мс (Цель: <100 мс).
- **Генерация прогноза:** 2–3 сек (Цель: <5 сек).

Конфигурация и тонкая настройка

Настройка базовых показателей (Baselines)

- **Минимальное количество выборок:** 10 (для формирования первичной «нормы»).
- **Коэффициент сглаживания (Alpha): 0.1** (баланс между чувствительностью и стабильностью).
- **Интервал сохранения:** каждые 100 выборок.
- **Хранение данных baseline:** 90 дней (позволяет учитывать сезонность).

Чувствительность к аномалиям

Вы можете регулировать чувствительность системы в зависимости от типа среды:

Тип среды	Рекомендуемая настройка	Описание
Стабильный Production	Высокая (2 sigma)	Реагирует на малейшие отклонения от нормы.
Динамическое облако	Средняя (3 sigma)	Игнорирует незначительные колебания при масштабировании.
Разработка / Тест	Низкая (4 sigma)	Минимум уведомлений, только при явных сбоях.
Высоконагруженные услуги	Адаптивная	Система сама подбирает порог на основе волатильности.

Параметры обучения

Распознавание паттернов (Pattern Recognition)

- **Минимум повторений:** 3 (для создания базового паттерна).
- **Порог высокой уверенности:** 10 повторений.
- **Срок жизни паттерна:** 180 дней (устаревшие паттерны удаляются автоматически).
- **Порог сходства: 0.7** (допускает небольшие вариации в данных событий).

Прогноз сбоев (Failure Prediction)

- **Окно ретроспективного анализа:** 2 часа до сбоя.
- **Минимум улик:** 3 предшествующих события-предвестника.
- **Порог уверенности:** 0.7.

- **Окно прогноза:** за 2–4 часа до предполагаемого инцидента.

Интеграция с управлением событиями

Автоматизированный рабочий процесс

ИИ не просто анализирует данные, он инициирует действия:

1. **Trigger:** Обнаружение критической аномалии или группы корреляции.
2. **Analysis:** Запуск RCA (Root Cause Analysis) и поиск похожих инцидентов.
3. **Enrichment:** Добавление в инцидент инструкций (Runbooks) и ссылок на прошлые решения.
4. **Action:** Передача данных в систему автоматизации (например, запуск скрипта исправления).

ИИ-усиление функционала платформы

Интеграция искусственного интеллекта в RS-Discovery (R-Sight) значительно повышает эффективность стандартных инструментов управления событиями.

Улучшение корреляции

- **Валидация групп:** ИИ проверяет логичность объединения событий движком корреляции.
- **Дополнение связей:** Предлагает добавить в группу события, которые были пропущены из-за жестких правил.
- **Идентификация ложных связей:** Указывает на ошибочно сгруппированные алерты.
- **Оптимизация правил:** Анализирует эффективность текущих правил корреляции и предлагает правки.

Интеллектуальные уведомления

- **Приоритизация по риску:** Сортировка алертов на основе оценки риска (AI Risk Score), а не только статической важности.
- **Инсайты в сообщениях:** Включение кратких выводов ИИ непосредственно в текст уведомления (Telegram, Email).
- **Подбор экспертов:** Предложение получателей на основе их опыта решения подобных инцидентов в прошлом.
- **Руководство по решению:** Ссылка на наиболее релевантный Runbook прямо в оповещении.

Доверие к автоматизации

Уровень уверенности ИИ (AI Confidence) напрямую определяет сценарий реагирования:

- **Высокая уверенность (>85%):** Автоматическое исправление (Auto-remediation) без участия человека.
- **Средняя уверенность (60–85%):** Требуется подтверждение оператора (One-click approval).

- **Низкая уверенность (<60%):** Только ручное вмешательство, ИИ предоставляет данные для анализа.

ROI и бизнес-ценность

Измеримые выгоды

Преимущество	Метрика	Типовое улучшение
Предотвращение инцидентов	Предотвращенные сбои / мес.	20–30%
Ускорение решения	Сокращение MTTR	60–70%
Снижение шума	Сокращение количества алертов	85–90%
Уровень автоматизации	Авто-решенные инциденты	40–50%
Точность прогнозов	Верные предсказания	75–85%

Пример годовой экономии (на среду из 1000 серверов)

- **Предотвращение простоев:** $2–3 млн экономии на убытках.
- **Снижение трудозатрат:** Высвобождение ≈2000 часов ручной работы инженеров.
- **Эффективность операций:** Снижение операционных расходов (Ops Cost) на **30%**.

28 АВТОМАТИЗАЦИЯ И ПРАВИЛА КОРРЕЛЯЦИИ СОБЫТИЙ

Перейдите от реактивного «тушения пожаров» к проактивному управлению с помощью интеллектуального движка правил корреляции RS-Discovery (R-Sight). Платформа автоматически обнаруживает сложные паттерны, выявляет первопричины и предлагает конкретные действия по устранению инцидентов.

Интеллектуальная корреляция на основе правил

Движок RS-Discovery (R-Sight) выходит за рамки простой группировки по времени, идентифицируя сложные технологические взаимосвязи.

Расширенное обнаружение паттернов

- **Проблемы с подключениями к БД:** При исчерпании пула соединений система автоматически связывает алерты пула с таймаутами приложений, определяет нехватку мощностей БД как первопричину и группирует события в 5-минутном окне.
- **Каскадные сбои сервисов:** Платформа отслеживает зависимости, выявляет «виновника» в верхней части цепочки (upstream) и соотносит его со всеми дочерними сбоями (downstream) в течение 3 минут.
- **Обнаружение утечек памяти:** Система мониторит тренды и распознает цепочку «рост памяти → нагрузка на GC → Out of Memory», предсказывая время до падения.

Категории правил корреляции

Инфраструктурные паттерны

- **Сетевое разделение (Split-Brain):** Идентифицирует сценарии потери связности в распределенных кластерах, когда затронуто более 30% узлов.
- **Периодические сбои:** Выявляет проблемы, возникающие по расписанию (ежечасно, ежедневно), связывая их с фоновыми задачами или батч-процессами (требуется минимум 3 повторения).

Прикладные паттерны

- **Отслеживание зависимостей услуг:** Использует данные CMDB для распространения анализа первопричин по цепочке зависимостей.
- **Деградация производительности:** Отслеживает паттерны эскалации (warning → major → critical) и анализирует тренды в 30-минутном окне до наступления полного отказа.

Как работают правила корреляции

Процесс оценки включает четыре ключевых этапа:

1. **Анализ паттернов событий:** Поиск ключевых слов в заголовках и описаниях (регистронезависимый поиск с достоверностью до 90%).
2. **Временная корреляция:** Анализ последовательностей событий в настраиваемых окнах (обычно 5 минут).

3. **Топологический анализ:** Проверка связей в CMDB для определения направления распространения сбоя.
4. **Детекция трендов:** Расчет времени до достижения критического порога на основе метрик.

Оценка влияния на бизнес и поиск первопричин

Автоматизированный анализ влияния

Каждое правило корреляции включает оценку критичности для бизнеса:

Уровень влияния	Описание	Примеры
Критический	Полная остановка сервиса	Сбои платежей, аутентификации, повреждение данных
Высокий	Деградация UX	Замедление работы, частичная доступность, сбои бэкапов
Средний	Внутренние/некритичные проблемы	Замедление внутренних систем, ошибки в dev-среде

Идентификация первопричины (RCA)

Система восстанавливает истинную причину через:

- **Upstream-анализ:** Поиск инициирующего сервиса и первого критического события в цепочке.
- **Реконструкция таймлайна:** Хронологическое упорядочивание событий для выделения триггеров и предотвратимых сбоев.

Рекомендации по устранению инцидентов

На основе выявленных паттернов система RS-Discovery (R-Sight) предоставляет конкретные инструкции по восстановлению работоспособности сервисов:

Интеллектуальные рекомендации

- **Проблемы с базами данных:**
  - Увеличение размера пула соединений.
  - Оптимизация медленных запросов.
  - Добавление реплик базы данных.
- **Сбои сервисов:**
  - Перезапуск затронутых компонентов.
  - Горизонтальное масштабирование инфраструктуры.
  - Активация автоматических прерывателей (Circuit Breakers).
  - Перенаправление трафика на здоровые экземпляры.
- **Исчерпание ресурсов:**
  - Очистка кэша.
  - Перезапуск приложений с утечкой памяти.
  - Увеличение лимитов ресурсов или активация политик автомасштабирования.

Обучение паттернам

Движок корреляции постоянно совершенствуется за счет анализа накопленных данных:

1. **Исторический анализ:** ИИ изучает паттерны прошлых инцидентов, выявляет наиболее успешные действия по их устранению и пополняет библиотеку паттернов для повышения точности будущих детекций.
2. **Интеграция обратной связи:** Система «наблюдает» за действиями оператора, корректирует пороги достоверности и уточняет правила анализа первопричин (RCA) на основе реального опыта команды.

Производительность и масштабируемость

Возможности обработки

- **Анализ в реальном времени:** Правила оцениваются за миллисекунды. Система способна обрабатывать тысячи событий в минуту, сохраняя задержку корреляции менее одной секунды.
- **Точность корреляции:** Достигается точность сопоставления паттернов более **90%** при уровне ложных срабатываний менее **5%**.

Метрика	Производительность	Описание
Скорость оценки правила	<100 мс	Время на проверку одного правила.
Сопоставление паттернов	<50 мс	Производительность поиска по паттернам.
Окно корреляции	5–30 мин	Настраиваемые временные интервалы.
Порог достоверности	0.7	Минимальный балл для объединения событий.
Исторический поиск	20 событий	Глубина анализа прошлых событий для одного правила.

Рекомендации по внедрению

Для достижения максимальной эффективности корреляции RS-Discovery (R-Sight) рекомендуется следовать поэтапному подходу:

Этапы внедрения

1. **Фаза 1: Обнаружение паттернов** — Включите движок правил, мониторьте точность автоматических группировок и проверяйте правильность определения первопричин.
2. **Фаза 2: Уточнение правил** — Скорректируйте пороги достоверности, настройте временные окна под специфику вашей сети и определите маппинг влияния на бизнес-процессы.
3. **Фаза 3: Оптимизация** — Анализируйте эффективность корреляции, расширяйте охват правил и интегрируйте их с системами автоматизации.

Примеры практических сценариев

1. Корреляция сбоя базы данных

- **Сценарий:** Исчерпание пула соединений БД.
- **Детекция:** Первичное событие «Limit reached» + каскад «Connection timeout» в окне 5 минут. Достоверность: **95%**.
- **Анализ:** Затронуто 12 приложений (выявлено через топологию). Влияние на бизнес: **Высокое**.
- **Устранение:** Увеличение размера пула (немедленно), перезапуск пула (краткосрочно), оптимизация запросов (долгосрочно).

2. Каскадный сбой микросервисов

- **Сценарий:** Сбой платежного сервиса, влияющий на всю цепочку заказов.
- **Детекция:** Каскад зависимостей «Платежи → Заказы → Склад → Уведомления» в течение 3 минут. Эскалация статуса до **Критический**.
- **Анализ:** Первопричина — таймаут внешнего платежного шлюза.
- **Устранение:** Активация «прерывателя» (Circuit Breaker), переключение на резервный шлюз, прогрев кэша после восстановления.

Выгоды и возврат инвестиций (ROI)

Операционная эффективность

- **Снижение шума (на 85%):** Операторы видят один инцидент вместо сотен разрозненных алертов, что избавляет от «усталости от уведомлений».
- **Ускорение решения (на 70%):** Сокращение MTTR благодаря мгновенному RCA и готовым рекомендациям по исправлению.
- **Проактивная защита:** Выявление трендов и предсказание сбоев до того, как они затронут пользователей.

Преимущество	Типовое улучшение	Годовой эффект (пример)
Снижение числа инцидентов	-30%	Экономия $500K–2 млн
Ускорение восстановления	–70% MTTR	Экономия 1000+ часов работы
Снижение шума	–85% алертов	Рост эффективности команды на 50%
Точность паттернов	95% точность	Непрерывное самообучение системы

29 КАНАЛЫ УВЕДОМЛЕНИЙ И РАСПРЕДЕЛЕНИЕ АЛЕРТОВ

Инфраструктура уведомлений RS-Discovery (R-Sight) гарантирует, что критические алерты дойдут до нужных специалистов в нужное время. Благодаря интеллектуальной маршрутизации, многоканальной доставке и снижению уровня «шума», команды остаются в курсе событий без риска развития «усталости от алертов» (alert fatigue).

Стратегия уведомлений

Интеллектуальная маршрутизация

Система RS-Discovery (R-Sight) спроектирована для достижения трех ключевых целей:

1. **Снижение нагрузки:** Группировка связанных событий, подавление дубликатов и пакетная отправка низкоприоритетных алертов.
2. **Гарантия доставки:** Поддержка нескольких каналов для резервирования, автоматическое переключение (failover) и отслеживание подтверждений.
3. **Ускорение отклика:** Прямая маршрутизация к экспертам, предоставление контекста для действий и подтверждение (acknowledgment) в один клик.

Поддерживаемые каналы связи

Корпоративные платформы

- **Microsoft Teams:** Адаптивные карточки с богатым форматированием и интеграция с графиками дежурств.

Традиционные каналы

- **Email:** HTML-отчеты с визуализацией, ссылками на подтверждение и ежедневными сводками.
- **SMS и голосовые вызовы**.

Управление эскалациями

Если инцидент не подтвержден в течение заданного времени, RS-Discovery (R-Sight) запускает многоуровневую эскалацию:

- **Уровень 1 (0–5 мин):** Первичный дежурный инженер.
- **Уровень 2 (5–15 мин):** Резервный дежурный и уведомление тимлида.
- **Уровень 3 (15+ мин):** Уведомление руководства и кросс-командная координация.

Снижение шума и аналитика

Стратегии фильтрации

- **Дедупликация:** Группировка идентичных алертов в один с указанием счетчика (count).
- **Окна обслуживания:** Подавление алертов во время плановых работ.

- **Smart Grouping:** Объединение событий на основе общей первопричины.

Метрики эффективности

- **MTTA (Time to Acknowledge):** Время от отправки до подтверждения.
- **Alert Quality:** Соотношение полезного сигнала к шуму.
- **Уровень нагрузки:** Количество уведомлений на одного инженера для предотвращения выгорания.

Метрика	Улучшение	Ценность
Шум алертов	-80%	Фокус на важных задачах
Время отклика	-65%	Сокращение времени простоя (downtime)
Ложные тревоги	-75%	Снижение числа ненужных прерываний работы
Удовлетворенность	+40%	Снижение текучести кадров в Ops-командах