Руководство пользователя
системы RS-Discovery (R-Sight)

RS TEAM

rs.team

СОДЕРЖАНИЕ

1 АУТЕНТИФИКАЦИЯ

Этот раздел руководства дает обзор процесса аутентификации для RS-Discovery (R-Sight), включая вход, требования к паролям и двухфакторную аутентификацию (2FA).

1.1 Процесс входа

Процесс входа спроектирован безопасно и просто. Все учетные записи обязаны использовать двухфакторную аутентификацию (2FA).

1.1.1 Первый вход

При первом входе или с устаревшим паролем вас направят на один или оба обязательных шага обновления безопасности:

- обновление пароля: если текущий пароль не соответствует новым строгим требованиям, потребуется создать новый пароль сразу после входа;
- настройка 2FA: после обеспечения безопасности пароля вас попросят настроить 2FA через приложение-аутентификатор (Google Authenticator, Authy, Microsoft Authenticator). Отсканируйте QR-код и введите 6-значный код.

Доступ к приложению невозможен до завершения этих шагов.

1.1.2 Последующие входы

1. **Введите учетные данные:** на странице входа укажите email и пароль.
2. **Предоставьте код 2FA:** после отправки учетных данных введите 6-значный код из приложения-аутентификатора.
3. **Доступ к приложению:** после успешной верификации вы войдете в RS-Discovery (R-Sight).

1.2 Требования к паролям

Для защиты учетной записи все пароли должны соответствовать критериям:

1. **Минимальная длина:** не менее 12 символов.
2. **Сложность:** минимум по одному:

- Заглавная буква (A-Z).
- Строчная буква (a-z).
- Цифра (0-9).
- Специальный символ (!@#$%^&*).

3. **Уникальность:** не может быть распространенным паролем ('password123').
4. **Без повторений:** не содержит последовательностей ('12345') или повторов ('aaaaa').

1.3 Безопасность учетной записи

RS-Discovery (R-Sight) включает функции защиты:

- Блокировка учетной записи: Для предотвращения brute-force после нескольких неудачных попыток аккаунт блокируется на 15-60 минут.
- Тайм-аут сессии: Сессии истекают через 2 часа бездействия.
- Резервные коды: После настройки 2FA выдаются одноразовые коды. Храните их в безопасном месте.

1.4 Устранение неисправностей

Неверные учетные данные: Проверьте email/пароль, отключите Caps Lock. **Неверный код 2FA:** Код истек или рассинхронизировано время. Включите

автообновление времени на устройстве. Используйте резервный код.
Заблокирован аккаунт: Дождитесь истечения блокировки.

Для сложных проблем обратитесь к системному администратору.

2 УСТАНОВКА СКАНЕРОВ

Это руководство содержит инструкции по установке и настройке агента сканера RS-Discovery (R-Sight) для Windows-сред.

2.1 Агент сканера RS-Discovery (R-Sight) (Windows)

Агент сканера RS-Discovery (R-Sight) — комплексный инструмент обнаружения для Windows-сред. Может работать как интерактивное приложение (GUI-режим) или фоновый сервис Windows для автоматизированного непрерывного обнаружения (режим сервиса).

2.2 Системные требования

- **Операционная система:** Windows 7 / Windows Server 2008 R2 или новее.
- **.NET Framework:** Версия 4.8 или новее.
- **PowerShell:** Версия 5.1 или новее.
- **Память:** 100 МБ свободной ОЗУ.
- **Дисковое пространство:** 200 МБ свободного места.

2.3 Сетевые требования

Агент требует исходящий доступ HTTPS (порт 443) к конечной точке API RS-Discovery (R-Sight) (api.RS-Discovery (R-Sight).com).
Для сканирования целевых устройств откройте соответствующие порты (WMI: 135, 445; SSH: 22; SNMP: 161).

2.4 Установка и настройка

1. Скачивание агента

Перейдите в Центр загрузок в UI RS-Discovery (R-Sight) и скачайте ZIP-файл агента сканера.

2. Распаковка файлов

Распакуйте содержимое ZIP в постоянную директорию, например C:\Program Files\RS-Discovery (R-Sight).

3. Выбор режима работы

A) Режим сервиса (рекомендуется)

Идеально для автоматизированного сканирования с выделенного сервера обнаружения.

- Запустите PowerShell или Командную строку от имени администратора.
- Перейдите в директорию с файлами агента.
- Установите как сервис Windows или запустите напрямую в режиме сервиса.

Особенности сервиса:

- Работает непрерывно в фоне.
- Автозапуск с Windows.
- Собственное логирование.
- Интеграция с планировщиком задач.

B) GUI-режим

Для интерактивного сканирования и тестирования.

- Дважды кликните исполняемый файл агента.
- Настройте цели сканирования и запустите вручную.

Планировщик: встроенный планировщик для автоматического сканирования (ежедневно, еженедельно, по IP-диапазонам).

Настройка токена сканера

После установки настройте токен обнаружения для связи с платформой RS-Discovery (R-Sight).

Шаг 1: Получение токена обнаружения

- Войдите в платформу RS-Discovery (R-Sight).
- Перейдите в **Discovery → Discovery Token**.
- Скопируйте существующий токен или создайте новый (+ Создать новый Токен).

Храните токен в безопасности — он дает доступ к отправке данных в вашу среду.

Шаг 2: Настройка интеграции сканера

- Откройте приложение сканера RS-Discovery (R-Sight).
- Перейдите на вкладку **Integrations (Интеграции)**.
- Настройте:

Имя: "RS-Discovery (R-Sight) Production"
API URL: https://api.RS-Discovery (R-Sight).com/api
Agent ID: уникальный идентификатор экземпляра
API Token: вставьте токен обнаружения
WebSocket URL (опционально)

- Нажмите **Add Integration (Добавить интеграцию) → Test Connection (Тест соединения)**.

После успешной настройки сканер готов выполнять обнаружение сети и отправлять данные в CMDB RS-Discovery (R-Sight).

3 ВЫПОЛНЕНИЕ СКАНИРОВАНИЯ ТРЕБОВАНИЯ К ОБНАРУЖЕНИЮ (DISCOVERY)

Это руководство описывает требования для различных методов обнаружения (Discovery), используемых RS-Discovery (R-Sight) для поиска и картирования вашей ИТ-инфраструктуры.

Обзор методов обнаружения (Discovery)

RS-Discovery (R-Sight) использует гибридный подход к обнаружению (Discovery), комбинируя агенто-зависимые и агент-less-методы для полного и точного охвата инфраструктуры.

Агенто-зависимое обнаружение
Развертывание агента сканера RS-Discovery (R-Sight) на Windows-хосте в сети. Обеспечивает глубокую информацию, обновления в реальном времени, сканирование за файрволами.

Агент-less-обнаружение
Сканер сканирует цели по сети через WMI, SSH, SNMP без установки ПО на цели.

Гибридное обнаружение
Сканер выполняет агент-less-сканирование, сочетая глубину агент-based с охватом агент-less.

3.1 Требования к агенто-зависимому обнаружению

Системные требования для хоста агента:

Компонент	Требование
ОС	Windows 10/11 или Server 2016+ (64-bit)
Процессор	Многоядерный (для больших сетей)
Память	2 ГБ минимум, 4 ГБ+ рекомендовано
Диск	1 ГБ свободного места
Права	Административные для установки сервиса

Исходящие сетевые требования:

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

3.2 Требования к агент-less-обнаружению

Windows-системы (WMI)

Порт	Протокол	Назначение	Примечания
135	TCP	RPC Endpoint Mapper	Начальное WMI-соединение
445	TCP	SMB/CIFS	WMI и PAExec fallback
49152-65535	TCP	Dynamic RPC	WMI коммуникация

Совет по файрволу: PAExec fallback использует только порт 445.
Учетные данные: Локальный администратор (рекомендуется доменный).

3.3 Linux/Unix (SSH)

Порт	Протокол	Назначение
22	TCP	SSH

Учетные данные: SSH-пользователь с sudo/root (пароль/ключ).

3.4 Сетевые устройства (SNMP)

Порт	Протокол	Назначение
161	UDP	SNMP

3.5 VMware vCenter

Порт	Протокол	Назначение
443	HTTPS	vCenter API

Учетные данные: Права чтения минимум.

3.6 Обнаружение баз данных SQL Server

Автоматически запускается при WMI-сканировании Windows с SQL Server.

Как работает:

- Обнаружение через реестр Windows.
- Запросы локально через SQLCMD.
- Использует WMI-соединение (порты 135, 445).

Требования на цели:

- SQLCMD установлен.
- Windows-аутентификация для WMI-учетки.

Что обнаруживается:

- Экземпляры SQL (default/named).
- Конфигурация (версия, память, аутентификация).
- Базы данных (размеры, бэкапы, шифрование).
- Активные соединения, связанные серверы.

4 ТРЕБОВАНИЯ К УЧЕТНЫМ ДАННЫМ ДЛЯ ОБНАРУЖЕНИЯ

Для выполнения глубокого аутентифицированного сканирования инфраструктуры агент сканера RS-Discovery (R-Sight) требует соответствующие учетные данные для целевых систем. Это руководство описывает необходимые учетные данные и лучшие практики их безопасного управления.

4.1 Управление учетными данными и безопасность

Локальное хранение: Учетные данные настраиваются во вкладке **Credentials** приложения агента сканера RS-Discovery (R-Sight).
Сильное шифрование: Все учетные данные шифруются с использованием Windows Data Protection API (DPAPI) — привязаны к учетной записи/машине агента.
Без центрального хранения: Учетные данные никогда не отправляются и не хранятся на платформе RS-Discovery (R-Sight).

4.2 Требования по типам систем

4.2.1 Windows-системы (через WMI)

Необходимые привилегии: Локальный администратор на целевых машинах.
Рекомендуемый аккаунт: Доменный администратор или сервисный аккаунт в группе локальных администраторов.

Формат имени пользователя:

- Доменные: DOMAIN\username или username@domain.com
- Локальные: .\username

4.2.2 Linux/Unix-системы (SSH)

Необходимые привилегии: SSH-доступ.
Рекомендуемые: root или sudo для полного инвентаря.
Методы аутентификации: Пароль и SSH-ключи.

4.2 Сетевые устройства (SNMP)

- **SNMPv1/v2c:** Строка сообщества с правами чтения.
- **SNMPv3:** Аккаунт с authPriv (рекомендуется).

4.3 VMware vCenter

Рекомендуемый аккаунт: Сервисный с правами **Global read-only** (администратор не требуется).

4.4 Базы данных SQL Server

Аутентификация: Windows Authentication через WMI-учетку.
Требования: WMI-аккаунт должен иметь SQL Server login.

Уровни доступа SQL Server:

Уровень	Что обнаруживается
Базовый	Instance, версия
Стандартный	+ память, соединения, шифрование
Полный	+ все БД, бэкапы, связанные серверы

Рекомендуемые разрешения SQL Server:

```
-- Connect to master database
USE master;
GO

-- Create login from Windows account (if not exists)
CREATE LOGIN [DOMAIN\ScanAccount] FROM WINDOWS;
GO
```

```
-- Grant server-level permissions
GRANT VIEW SERVER STATE TO [DOMAIN\ScanAccount];
GRANT VIEW ANY DATABASE TO [DOMAIN\ScanAccount];
GRANT VIEW ANY DEFINITION TO [DOMAIN\ScanAccount];
GO

-- Grant msdb read access for backup history
USE msdb;
GO
CREATE USER [DOMAIN\ScanAccount] FOR LOGIN [DOMAIN\ScanAccount];
ALTER ROLE db_datareader ADD MEMBER [DOMAIN\ScanAccount];
GO
```

Замените DOMAIN\ScanAccount на фактическую учетную запись вашей службы сканирования.

4.5 Лучшие практики безопасности

- **Least Privilege:** Минимальные права (read-only для vCenter).
- **Сервисные аккаунты:** Не используйте личные аккаунты администраторов.
- **Ограничение по IP:** Привязывайте учетные данные к IP-диапазонам в настройках агента.
- **Ротация:** Обновляйте пароли/ключи по политике организации.
- **Мониторинг:** Проверяйте логи сканирования на неудачные аутентификации.

5 СПРАВОЧНИК ПО СКАНИРОВАНИЮ SSH

Это руководство содержит справочник по сканеру SSH, который обнаруживает и собирает подробную информацию с систем Linux, Unix и AIX.

5.1 Обзор

Сканер SSH подключается к целевым системам через протокол Secure Shell (SSH) для выполнения команд. Собирает полный инвентарь оборудования, ПО и конфигурации без установки агента на цели.

5.2 Сетевые требования

Порт: TCP 22 открыт от агента сканера RS-Discovery (R-Sight) к целевой системе Linux/Unix/AIX.
Протокол: Secure Shell (SSH).

5.3 Требования к аутентификации

Необходим SSH-аккаунт на целевой системе. Поддерживаются парольная и SSH-ключ аутентификация.
Рекомендация: SSH-ключи для безопасности.

5.4 Требования к привилегиям

Объем данных зависит от привилегий учетной записи. Два режима:

5.5 Базовое обнаружение (не-root пользователь)

Достаточно стандартного непривилегированного аккаунта.
Необходимые разрешения:

- SSH-доступ.
- Чтение /proc, /sys, /etc.
- Выполнение команд: hostname, uname, ip, df, ps.

Собранные данные:

- Идентификация системы (hostname, OS, kernel).
- Базовое оборудование (CPU, память, диски).
- Сеть (IP, интерфейсы, соединения).
- Процессы, пакеты ПО, пользователи.

5.6 Расширенное обнаружение (root или sudo)

Для полного сбора данных.
Дополнительные данные с привилегиями:

- Полные спецификации оборудования (dmidecode).
- Здоровье дисков (smartctl).
- Процессы-соединения (lsof).
- Виртуализация (Docker, KVM).
- AIX: LPAR, VPD (IBM Power).

5.7 Сводка собранных данных

Категория	Примеры	Привилегии
Система	Hostname, OS, Kernel, Serial	Базовые (полные с root)
Оборудование	CPU, RAM, Диски, PCI	Базовые (полные с root)
Сеть	IP, MAC, Gateway, Соединения	Базовые
ПО	Пакеты (rpm/dpkg), версии	Базовые
Процессы	Запущенные, пути, пользователи	Базовые (полные с root)
Пользователи	Локальные аккаунты, логины	Базовые

Хранилище	Файловые системы, SMART	Базовые (SMART с root)
Виртуализация	Docker, KVM VMs	Root

6 СПРАВОЧНИК ПО СКАНИРОВАНИЮ WINDOWS WMI

Это руководство содержит справочник по сканеру Windows Management Instrumentation (WMI), который обнаруживает и собирает подробную информацию с Windows-систем.

6.1 Обзор

Сканер WMI — основной метод глубокого обнаружения Windows-компьютеров. Использует стандартную технологию управления Windows WMI для запроса системной информации.
При ограничительных файрволах применяется fallback-механизм PAExec для сбора тех же данных.

6.2 Сетевые требования

Основной метод (WMI over RPC):

Порт	Протокол	Назначение
135	TCP	RPC Endpoint Mapper
49152-65535	TCP	Dynamic RPC (Vista+)

Fallback-метод (PAExec over SMB):

Порт	Протокол	Назначение
445	TCP	SMB/CIFS

6.3 Требования к аутентификации и привилегиям

Необходимые привилегии: Локальный администратор на целевой Windows-машине.
Рекомендуемый аккаунт: Доменный администратор или сервисный аккаунт в группе локальных администраторов.

Поддерживаемые форматы учетных данных:

- DOMAIN\username (рекомендуется для доменных)
- username@DOMAIN.COM
- username (локальные на не-доменных машинах)

6.4 Сводка собранных данных

Сканер WMI собирает полный инвентарь системы (одинаково для WMI и PAExec).

Категория	Примеры
Система	Hostname, Domain, Manufacturer, Model, Serial Number
ОС	Windows Server 2019, версия, build, SP, дата установки, последний запуск
Оборудование	BIOS, CPU (модель, ядра), RAM-модули, физические диски
Хранилище	Логические диски (C:), ФС, размер, свободное место
Сеть	Адаптеры, IP, MAC, Gateway, DNS, DHCP
Активные соединения	TCP-соединения (лок/удал, порты, PID, состояние)
ПО	Полный список приложений из реестра Windows
Пользователи	Локальные аккаунты (статус, описание)
Дисплей	Адаптеры, разрешение, конфигурация мониторов

7 СПРАВОЧНИК ПО СКАНИРОВАНИЮ VMWARE VCENTER

Это руководство содержит справочник по сканеру VMware vCenter, который обнаруживает и картирует полную виртуализированную инфраструктуру, управляемую vCenter.

7.1 Обзор

Сканер vCenter подключается напрямую к vSphere API на сервере vCenter. Выполняет глубокий инвентарь виртуальной среды: дата-центры, кластеры, хосты ESXi, виртуальные машины (VM) и их связи. Агенты на ESXi/VM не требуются.

7.2 Сетевые требования

Порт	Протокол	Назначение
443	TCP	vSphere API (SOAP/REST over HTTPS)

7.3 Требования к аутентификации и привилегиям

Необходимые права: Аккаунт для чтения данных vCenter (администратор не нужен).

Рекомендуемая роль: Global Read-Only — достаточно для всех операций обнаружения и соответствует лучшим практикам безопасности.

Область прав: Применить на верхнем уровне vCenter с наследованием на дочерние объекты (Datacenters, Clusters).

Минимальные привилегии: System.Anonymous, System.Read, System.View, Global.Licenses, Host.Config.AdvancedConfig, VirtualMachine.Config.AdvancedConfig.

7.4 Сводка собранных данных

Сканер vCenter строит полную картину виртуальной инфраструктуры и связей между компонентами.

Категория	Примеры
vCenter Server	Версия/build, API версия, UUID, статус здоровья
Инфраструктура	Названия дата-центров, структура папок, конфигурация кластеров
Кластеры	Имя, ресурсы CPU/памяти, HA/DRS, EVC Mode
Хосты ESXi	Hostname, производитель/модель, серийный номер, версия гипервизора, состояние питания, CPU/память
Виртуальные машины	Имя VM, UUID, Guest OS, состояние питания, выделенные CPU/память, VMware Tools, IP/MAC, теги
Хранилище	Datastores, тип (VMFS/NFS/vSAN), емкость, свободное место, VM на datastore
Сеть	vSwitches (стандартные/дистрибутированные), Port Groups, VLAN, политики
Resource Pools	Имя пула, резервы/лимиты/доли CPU/памяти

Связи:

- VM → runs on → ESXi Host
- ESXi Host → member of → Cluster
- VM → uses → Datastore
- VM → connected to → Port Group

8 СПРАВОЧНИК ПО СКАНИРОВАНИЮ SNMP

Это руководство содержит справочник по сканеру Simple Network Management Protocol (SNMP), который обнаруживает и собирает информацию с сетевых устройств: роутеры, коммутаторы, файрволы, принтеры.

8.1 Обзор

Сканер SNMP опрашивает устройства с включенным SNMP. Собирает данные об идентичности, конфигурации, интерфейсах сети и связности для построения карты сетевой топологии.

8.2 Сетевые требования

Порт	Протокол	Назначение
161	UDP	SNMP-запросы

8.3 Требования к аутентификации и привилегиям

SNMPv1/v2c: Строка сообщества только для чтения (менее безопасно — передается в открытом виде).
SNMPv3: Аккаунт с уровнем безопасности:

- noAuthNoPriv (наименее безопасно)
- authNoPriv (аутентификация)
- **authPriv** (аутентификация + шифрование) — **рекомендуется**.

8.4 Сводка собранных данных

Сканер автоматически классифицирует устройства и собирает:

Категория	Примеры
Система	Имя устройства, описание, Vendor/Model (System OID), uptime, физическое расположение
Тип устройства	Авто-классификация: Router, Switch, Firewall, Printer, UPS
Интерфейсы	Имя/описание, тип (Ethernet), скорость, статус, MAC-адрес
IP-конфигурация	IP-адреса и маски подсети интерфейсов
Топология сети	ARP-таблица (L2-соседи), таблица маршрутизации (L3-пути)
Vendor-Specific	Cisco: CPU/память; HP/Aruba: PoE; принтеры: уровень тонера

9 РУКОВОДСТВО ПО СКАНИРОВАНИЮ GUI

Это руководство содержит пошаговый обзор графического интерфейса агента сканера RS-Discovery (R-Sight). Логический рабочий процесс: сначала **Integrations (Интеграции) → Credentials (Учетные данные) → Scan (Сканирование) → Scheduler (Расписание) → Service (Сервис)**.

1. Настройка интеграций (вкладка Integrations)

Для загрузки результатов сканирования подключите сканер к платформе RS-Discovery (R-Sight).

Как настроить интеграцию:

- **Name:** "RS-Discovery (R-Sight) Production" (описательное имя).
- **API URL:** https://api.RS-Discovery (R-Sight).com/api
- **Agent ID:** уникальный ID экземпляра сканера.
- **API Token:** вставьте **Discovery Token** из платформы RS-Discovery (R-Sight).
- **WebSocket URL** (опционально).
- **Add Integration (Добавить интеграцию) → Test Connection (Тест соединения)**

2. Управление учетными данными (вкладка Credentials)

Здесь безопасно хранятся учетные данные для доступа к целевым системам.

Добавление учетных данных:
Выберите протокол: WMI, SSH, SNMP, vCenter.

Примеры:

- **WMI:** Username, Password, Domain (опционально).
- **SSH:** Username, Password или путь к SSH-ключу.
- **SNMP:** v1/v2c — Community string; v3 — user/auth/privacy.
- **IP Range** (опционально): 192.168.1.0/24 — ограничивает использование.
- **Active** ✓ → **Save**.

Тестирование: Выберите credential (учетные данные) → **Test Credential** → введите IP цели.

3. Ручное сканирование (вкладка Scan)

Запуск сканирования:
IP Range (поддерживаемые форматы):

```
text
192.168.1.10 (один IP)
192.168.1.10,192.168.1.11 (список)
192.168.1.1-192.168.1.100 (диапазон)
192.168.1.0/24 (CIDR)
```

Опции сканирования:

- ☑ **Ping** — проверка доступности.
- ☑ **Port Scan** — открытые порты TCP/UDP.
- ☑ **WMI/SSH/SNMP/vCenter** — глубокое обнаружение.

Start Scan → мониторинг в таблице результатов в реальном времени.

Таблица результатов:

IP	Status	Services	Details
192.168.1.10	Up	WMI, SSH	SSH success
192.168.1.11	Down	-	Host unreachable

4. Автоматизация сканирования (вкладка Scheduler – расписание)

Добавление расписания:

- **Name:** "Daily Production Scan".
- **IP Range:** 10.0.0.0/16.
- **Frequency (Регулярность):** hourly/daily/weekly/monthly.
- **Time/Interval (Время/Интервал):** 14:00 или каждые 6 часов.
- **Save (Сохранить)** → активировать в Service Tab.

5. Управление сервисом (вкладка Service)

Режимы работы:

Service Mode (Standalone):

- **Start/Stop (Пуск/Стоп) Service Mode** — для тестирования.

Windows Service (рекомендуется):

- **Install Service** — автозапуск с Windows (требует admin).
- **Remove Service** — удаление.
- **Start/Stop Service** — ручное управление.

Для Prod: Установите как Windows Service для автоматического выполнения расписаний.

10 РУКОВОДСТВО ПО СКАНИРОВАНИЮ БЕЗОПАСНОСТИ

Агент сканера RS-Discovery (R-Sight) спроектирован с приоритетом безопасности для защиты учетных данных и данных в процессе обнаружения.

Безопасное хранение учетных данных

Ключевое правило: учетные данные для обнаружения **никогда не покидают машину сканера**.

Как хранятся учетные данные:

- **Локальное хранение:** В зашифрованном файле на машине сканера. **Сильное шифрование:** Файл credentials.enc зашифрован алгоритмом **Fernet** (AES-128-CBC).
- **Уникальный ключ:** Ключ шифрования генерируется локально и хранится отдельно в key.enc.

Как используются учетные данные:

1. Сканер читает зашифрованный credentials.enc.
2. Расшифровывает нужные данные **в память приложения**.
3. Использует их для аутентификации к цели (WMI/SSH).
4. **Никогда** не записывает в plaintext логи и **не передает** на платформу RS-Discovery (R-Sight).

Результат: учетные данные остаются под вашим контролем в локальной сети.

Безопасная коммуникация сканер-сервер

1. Загрузка результатов (HTTPS)

Что отправляется: Только **результаты сканирования** (оборудование, ПО, IP) — **НЕ учетные данные**.
Как: HTTPS (порт 443, TLS 1.2+), проверка SSL-сертификатов против MITM-атак.

2. Реальное время (WebSocket)

Назначение: Статус (Online/Offline/Scanning), удаленное управление.
Безопасность: WSS (WebSocket Secure) по TLS (порт 443).
Аутентификация: Только **API Token** (Discovery Token) из вкладки Integrations (Интеграции).

Возможности удаленного управления

Через безопасный WebSocket администраторы платформы RS-Discovery (R-Sight) могут:

- ✅ Мониторить статус агента (здоровье, CPU, память).
- ✅ Запускать сканирования по IP-диапазонам.
- ✅ Управлять расписаниями.
- ✅ Просматривать конфигурацию агента.

Критично: Ни одна из функций **не раскрывает учетные данные** целевых систем.

11 ИССЛЕДОВАНИЕ CMDB ДОСТУП К CMDB (СПИСОК КЕ)

База данных управления конфигурацией (CMDB) — центральное хранилище всех данных инфраструктуры, обнаруженных RS-Discovery (R-Sight). Это единый источник истины для серверов, сетевых устройств, приложений и виртуальных машин. Все данные от агентов сканеров RS-Discovery (R-Sight) обрабатываются и заполняются здесь.

Основной способ просмотра и управления — **список конфигурационных единиц (CI List – список КЕ)**.

Навигация к списку КЕ

Доступ к инвентарю:

1. В главном меню выберите **CMDB**.
2. В выпадающем меню нажмите **CI List (Список КЕ)**.

Откроется основной интерфейс списка КЕ с инструментами поиска, фильтрации и управления активами.

Интерфейс списка КЕ

Список КЕ состоит из трех основных областей: **Header (Заголовки)**, **Filter Sidebar (Боковая панель фильтров)**, **CI Table (Таблица КЕ)**.

1. Действия в заголовке

Вверху страницы:

- **Total CIs (Всего КЕ):** общее количество КЕ.
- **Export to CSV (Экспорт в CSV):** скачать отфильтрованный список в CSV.
- **Customize Columns (Настройка столбцов):** настроить колонки (показать/скрыть/переставить).
- **New CI (Новая КЕ):** создать новую КЕ вручную.

2. Фильтрация и поиск

Левая панель фильтров:

- **Search Bar (Панель поиска):** свободный поиск по имени КЕ, серийному номеру, IP.
- **Filter by CI Type (Фильтр по типу КЕ):** только Серверы, Рабочие станции, Сетевое оборудование.
- **Filter by Status (Фильтр по статусу):** Active (Активен), Inactive (Неактивен), In Maintenance (На обслуживании).
- **Другие фильтры:** Местоположение, Производитель, Внешний источник.

3. Таблица КЕ

Основная область: список КЕ по текущим фильтрам.

Колонки (настраиваемые): Имя, Тип, Статус, IP, Производитель, Модель, Последнее сканирование.

Сортировка: клик по заголовку колонки.

Пагинация: навигация по страницам внизу.

Действия с КЕ (hover):

- **View Details (Показать подробности)** → полная страница деталей КЕ.
- **Edit (Редактировать)** → редактировать атрибуты.
- **Delete (Удалить)** → удалить из CMDB.

12 ПРОСМОТР ПОДРОБНОСТЕЙ О КЕ

Клик по КЕ в списке КЕ открывает **вид деталей КЕ** — полную 360° картину актива с данными, связями и историей аудита.

Заголовок КЕ

Быстрый обзор идентичности и состояния:

- **Имя КЕ и Тип:** основное имя и тип КЕ.
- **Status (Статус):** чип с текущим статусом (Active – Активен, Inactive – Неактивен, Maintenance – На обслуживании).
- **Edit CI (Редактировать КЕ):** ручное редактирование атрибутов.

Вкладка Overview (обзор) (по умолчанию)

Критическая информация в карточках.

Информационные карточки

General Information (Основная информация): Имя, тип, статус, локация, родительские КЕ.

Integration & Sync Status (Интеграция и статус синхронизации): Последний скан, ручной sync.

System/Hardware/Network (Система/Оборудование/Сеть): OS версия, CPU, память, IP/MAC.

Коллекции КЕ

Таблицы с глубокими данными:

- Установленное ПО
- Запущенные процессы
- Сетевые адаптеры
- Файловые системы

Другие вкладки

Relationships (Связи): Графическая визуализация связей КЕ с другими активами (приложения, серверы, устройства).

Change History (История изменений): Полная история изменений (кто, что, когда).

AI Insights: Анализ и рекомендации от ИИ RS-Discovery (R-Sight) (проблемы, оптимизация).

13 ВИЗУАЛИЗАЦИЯ СВЯЗЕЙ КЕ

Понимание связей между КЕ критично для анализа влияния, устранения неисправностей и безопасности. Вкладка **"Relationships" (Связи)** в деталях КЕ предоставляет мощные инструменты визуализации.

Как формируются связи

Автоматическое обнаружение: Агент сканера RS-Discovery (R-Sight) анализирует сетевой трафик и процессы, обнаруживая связи (service-a.exe → service-b.exe). Данные отправляются на платформу и заполняют граф. **Ручное создание:** Добавляйте связи вручную для логических/бизнес-зависимостей.

Стандартный вид связей

Граф связей

Центральный КЕ с upstream/downstream связями:

- **Nodes (узлы):** Каждый блок — КЕ.
- **Edges (ребра):** Линии со стрелками показывают направление зависимости.
  - Синие: сетевые соединения.
  - Зеленые: зависимости приложений.

Интерактивность: панорамирование, зум, перетаскивание узлов.

Process-Based View (Представление на основе процессов)

Детализация на уровне процессов: ребро подписано исполняемым файлом (nginx.exe, sqlserver.exe), создающим соединение.

Табличный вид

Outbound/Inbound вкладки:

Target/Source CI (Цель/Источник КЕ)	Relationship (Связи)	Process (Процесс)	Application (Приложение)	Software Family (Семейство программ)
DB-Server-01	Connected To	sqlserver.exe	MS SQL	Microsoft SQL Server

Анализ связей ИИ (AI Insights)

"AI Analyze" (ИИ-анализ) отправляет ID связей на сервер, где ИИ RS-Discovery (R-Sight) анализирует и обогащает контекстом.

Оценка рисков ИИ

Critical (Критическая): Критичная для бизнеса (web → primary DB). **High (Высокая):** Важная с частичной избыточностью. **Medium/Low (Средняя/Низкая):** Поддерживающие связи.

Виды ИИ-анализа

Список:

- **Purpose (Цель):** "Authentication", "Database Query".
- **Risk Level & Impact (Уровень риска и влияние):** Критичность.
- **Tags (Тэги):** bidirectional, remote-management.

ИИ-граф: Цвет/толщина ребра = важность (красные толстые = Critical (критические), серые тонкие = Low (низкие)).

14 ПОНИМАНИЕ AI INSIGHTS

Вкладка **AI Insights** в деталях КЕ предоставляет глубокий анализ, рекомендации и оценки безопасности для КЕ. Превращает сырые данные сканирования в actionable intelligence (действенный интеллект).

Как генерируются insights

Backend-процесс (backend/services/scanProcessors/ciai_insights.js):

1. **Сбор данных:** Сырые данные КЕ (система, оборудование, сеть, ПО, процессы).
2. **Очистка:** Удаление чувствительных данных (user accounts → count).
3. **AI Prompt:** Детальный промпт как "expert IT analyst".
4. **Хранение:** Результаты сохраняются в БД, привязанные к КЕ (кеширование).

Что генерирует ИИ

Многоуровневый анализ:

- **Security (Безопасность):** Уязвимости, неправильные конфигурации, устаревшее ПО.
- **Infrastructure (Инфраструктура):** Оборудование, узкие места, планирование мощностей.
- **Software (Программное обеспечение):** Лицензии, конфликты, версии.
- **Network (Сеть):** Зависимости, модели общения.
- **Configuration (Конфигурация):** Оптимизация, compliance.

Вкладки

Advanced Analysis (Расширенный анализ): Конфигурация, связи, проблемы.
Security (Безопасность): Уязвимости безопасности.

Секции Advanced Analysis (Расширенный анализ)

- **Overview (Обзор):** Высокий уровень состояния КЕ.
- **Key Relationships (Ключевые связи):** Критичные связи.
- **Recommendations (Рекомендации):** Действия по улучшению.
- **Risk Factors (Факторы риска):** Риски конфигурации.
- **Anomalies (Аномалии):** Необычные находки.

Интерактивность

- **Regenerate Insights (Восстановление аналитических данных):** Перегенерация при изменении данных.
- **Display Modes (Режим отображения):** Cards / Accordion.
- **Connection Status (Статус соединения):** Проверка backend/AI-сервисов.

Результат: Контекстное понимание инфраструктуры для обоснованных решений.

15 РАБОЧАЯ ПАНЕЛЬ КЕ: КАБИНА СВЯЗЕЙ

Рабочая панель КЕ — это современная полноэкранная панель управления интеллектом для управления и визуализации связей КЕ. Она сочетает функциональность Центра управления сетями (**NOC**) с интуитивно понятным дизайном, предоставляя комплексную среду для анализа, устранения неисправностей и планирования.

Интерфейс рабочей панели

Интерфейс спроектирован для глубокого анализа КЕ и их сложной сети связей. Он предоставляет мощные инструменты для исследования соединений, компонентов ПО и сетевых зависимостей в высоко визуальной и интерактивной форме.

Основная область визуализации: Центральная часть экрана, где можно просматривать связи в виде диаграммы или таблицы.

Верхняя панель инструментов: Содержит элементы управления для переключения видов, обновления данных, поиска и доступа к различным режимам диаграмм.

Панель инспектора (справа): Показывает подробную информацию о выбранной **КЕ** или связи.

Консоль инсайтов (снизу): Многозадачная вкладочная консоль для анализа, управляемого **ИИ**, уведомлений безопасности и журналов активности.

Панель конфигурации: Позволяет настроить вид, включая фильтры, группировку и опции расположения.

Ключевые возможности и сценарии использования

Рабочая панель КЕ — это больше чем инструмент визуализации. Это интерактивный центр управления для исследования и понимания вашей ИТ-среды.

Анализ состава ПО для КЕ

Рабочая панель позволяет провести глубокий анализ инвентаря ПО **для КЕ**. Вместо простого перечисления установленного ПО она визуализирует ПО как связанные компоненты. Движок **ИИ** автоматически категоризирует и группирует это ПО, предоставляя четкий структурированный обзор экосистемы ПО для КЕ.

Умная группировка ПО

Для управления сложностью в средах с большим количеством ПО рабочая панель использует функцию "**умная группировка**" специально для компонентов ПО. Она автоматически группирует связанные экземпляры ПО на основе семейства ПО или имени приложения, определенных **ИИ**, уменьшая загромождение и предоставляя обзор высокого уровня. Вы можете развернуть или свернуть эти группы для погружения в детали.

Сценарий использования: При анализе сервера с десятками установленных приложений вы можете свернуть их в логические группы, такие как "**Microsoft Office**", "**Инструменты безопасности**" и "**Инструменты разработки**", чтобы легко понять роль сервера.

Фокусированный анализ с режимами диаграмм

Помимо группировки, рабочая панель предоставляет несколько режимов диаграмм для фокусировки анализа на конкретных типах соединений. Это позволяет анализировать связи по сети, процессам или другим критериям.

Режим сети: Этот режим отображает только сырые сетевые соединения (**TCP/UDP**) между **КЕ**. Он необходим для понимания сетевой топологии и может использоваться для анализа соединений по сетевому диапазону или протоколу.

Режим зависимостей приложений (процесс): Предоставляет детализированный вид зависимостей на уровне процессов. Помогает точно понять, какие процессы на разных машинах общаются, что бесценно для устранения неисправностей приложений и картирования зависимостей.

Режим фильтра и анализа: Мощный режим позволяет строить сложные фильтры для изоляции очень конкретных **KE** или соединений для глубокого анализа.

Анализ влияния событий

Рабочая панель может интегрироваться с модулем **управления событиями** для визуализации потенциального влияния активного события. Переключившись в режим "**влияние события**", диаграмма выделяет затронутые событием **KE** и их зависимости.

Сценарий использования: Когда получено критическое уведомление о сервере, оператор может немедленно использовать этот вид, чтобы понять, какие бизнес-сервисы, приложения и пользователи могут быть затронуты, ускоряя реагирование на инциденты и повышая точность коммуникации.

Картирование зависимостей приложений (ADM)

Для более детализированного вида режим "**картирование зависимостей приложений (ADM)**" показывает зависимости на уровне процессов. Это позволяет точно увидеть, какие процессы на разных серверах общаются друг с другом.

Сценарий использования: При устранении неисправностей проблем производительности приложения разработчик или **SRE** может использовать этот вид для трассировки потока коммуникации от процесса приложения к процессу базы данных, помогая точно определить сетевую задержку или проблемы конфигурации между ними.

Продвинутая фильтрация и анализ

Рабочая панель включает мощный движок фильтрации, который позволяет разрезать и анализировать данные связей. Вы можете фильтровать по типу **KE**, типу связи, оценкам достоверности **ИИ** и многому другому.

Сценарий использования: Аналитик безопасности может использовать инструменты фильтрации, чтобы найти все серверы, имеющие открытое соединение с публичным интернетом на нестандартном порту, помогая выявить потенциальные риски безопасности.

Продвинутые возможности

Помимо визуализации **рабочая панель KE** предлагает несколько продвинутых функций:

Семантический поиск: Строка поиска на естественном языке позволяет задавать вопросы вроде "**покажи мне все базы данных в Prod**", и рабочая панель автоматически отфильтрует вид.

Сохраненные рабочие пространства: Вы можете сохранить свои настроенные представления — включая фильтры, положения узлов и расположение панелей — как именованное "**рабочее пространство**" для быстрого доступа позже. Это идеально для создания предустановленных видов для общих задач, таких как "**аудит безопасности**" или "**анализ влияния изменений**".

Экспорт: Вы можете экспортировать текущий вид как изображение (**PNG**, **SVG**) или экспортировать исходные данные как файл **CSV** или **JSON** для дальнейшего анализа или отчетности.

16 ГЛОБАЛЬНАЯ РАБОЧАЯ ПАНЕЛЬ ИНФРАСТРУКТУРЫ

Глобальная рабочая панель инфраструктуры (Global Infrastructure Workbench) — ваш центр управления для визуализации, анализа и исследования всего ИТ-ландшафта. В отличие от рабочей панели КЕ, которая фокусируется на одном активе, **глобальная рабочая панель** использует подход "breadth-first" (ширина в первую очередь), позволяя видеть зависимости макроуровня, выявлять системные риски и отслеживать сложные пути соединений по всей организации.

Доступ к рабочей панели

Для доступа к **глобальной рабочей панели инфраструктуры**:

1. Перейдите в **CMDB** в главном меню.
2. Выберите **Infrastructure Workbench** (Рабочая панель инфраструктуры).

AI Command Center (Центр управления ИИ)

В основе рабочей панели находится **центр управления ИИ**. Вместо ручного клика по десяткам фильтров вы можете просто задавать вопросы на обычном языке. **ИИ** переводит ваше намерение в точную визуализацию графа.

Примеры запросов:

- "Покажи все Prod базы данных, подключенные к публичным веб-серверам."
- "Выдели серверы с критическими уязвимостями и их зависимости."
- "Построй карту соединений между дата-центрами Москвы и Анадыря."

При отправке запроса система:

- Парсит намерение: определяет конкретные **КЕ**, среды и типы связей.
- Применяет фильтры: автоматически настраивает панель расширенных фильтров.
- Обновляет граф: отображает релевантные узлы и соединения.
- Выделяет совпадения: применяет эффект "**золотого свечения**" к активам из запроса.

Продвинутая фильтрация

Для детального контроля **сворачиваемая панель фильтров** слева позволяет разрезать данные инфраструктуры.

Фильтры КЕ

Тип КЕ: Фильтр по классам активов (Server, Database, Network Device).
Статус: Active, Maintenance, Inactive (Активен, На обслуживании, Неактивен).
Среда: Production, Staging, DR.
Диапазон IP: CIDR-блок (например, 10.0.0.0/8).
Классификация данных: PHI, PCI.

Фильтры связей

Порт/Протокол: Только трафик на конкретных портах (443, 1433).
Тип соединения: Manual или AI-Discovered.
Уровень риска: Critical, High, Medium, Low (Критический, Высокий, Средний, Низкий).
IP источника/цели: Трассировка между конкретными IP.

Интерактивный граф

Центральное полотно визуализации рассчитано на тысячи узлов без превращения в "hairball".

Умное кластерирование

Автогруппировка "листовых узлов" (endpoints с одной связью) в кластеры:

- **Визуально:** синяя иконка папки с бейджем ("15 Рабочих станций").

- **Интерактивно:** клик по кластеру → **Explode** (развернуть), **Layout** → перекластеризация.

Визуальное кодирование

Статус узла: зеленая точка (Активен), красная (Карантин), оранжевая (Обслуживание).
Уровень риска: пульсирующая красная рамка/линия для Критического.
Достоверность ИИ: пунктир для AI, сплошная для «по умолчанию».

Панель инспектора

Клик по узлу/соединению открывает **панель инспектора** справа:
Детали КЕ: OS, IP, Местоположение, метрики здоровья.
Детали соединения: процесс, порт, протокол.
Быстрые действия: переход к полной странице КЕ или локальной **рабочей панели КЕ**.

17 АНАЛИЗАТОР БИЗНЕС-УСЛУГ

Business Service Analyzer трансформирует управление ИТ-инфраструктурой, смещая фокус с отдельных серверов на целостные **бизнес-услуги**. Использует **ИИ** и продвинутую логику обнаружения для идентификации, картирования и анализа сложной сети компонентов — веб-серверов, баз данных, очередей и инфраструктуры, обеспечивающих критические услуги вроде "**Корпоративная почта**", "**1С**" или "**Интернет-банкинг**".

Зачем использовать Business Service Analyzer?

В современных ИТ-средах "услуга" редко представляет собой один сервер. Это совокупность взаимосвязанных компонентов. Управление ими как отдельными активами (**КЕ**) скрывает бизнес-контекст.

Анализатор бизнес-услуг устраняет этот разрыв:

Автообнаружение услуг: Находит известные паттерны (Exchange, CyberArk) автоматически.

Картирование зависимостей: Показывает точно, какая база данных поддерживает какое приложение.

Классификация ролей: Автоматически тегирует серверы как веб-сервер, база данных, инфраструктура.

Оценка рисков: ИИ выявляет единственные точки отказа и архитектурные риски.

Три способа анализа

Анализатор предлагает три различных рабочих процесса:

1. Анализ инфраструктуры

Режим "Auto-Discovery" (автообнаружение). Сканирует весь инвентарь по библиотеке предустановленных **Service Patterns** (паттернов сервисов), находя все распознаваемые услуги за один проход.

2. Анализ услуги по паттернам

Режим "Targeted Search" (целевое исследование). Использует конкретный паттерн (например, "**Microsoft Exchange**") для поиска экземпляра услуги с помощью **Two-Phase Discovery** (двухфазное обнаружение), отличая ядра серверов от общих зависимостей.

3. Анализ услуги с ручным вводом

Режим "AI-Assisted Custom" (Настроенный ИИ-помощник). Опишите кастомное приложение простым языком, **ИИ** поможет найти и картировать компоненты.

Анализ обнаруженной услуги

После сохранения в **CMDB** услуга становится "живым" объектом для мониторинга и анализа.

Комплексная карта услуги

Финальная карта услуги предоставляет живой вид здоровья и структуры.

Инсайты сервиса ИИ

Вкладка **Insights** — где **ИИ** выступает как архитектор, анализируя услугу на:

Архитектурные паттерны: Стандартные шаблоны.

Риски: Единственные точки отказа, пробелы безопасности.

Бизнес-влияние: Критичность по downstream зависимостям.

18 АНАЛИЗ ИНФРАСТРУКТУРЫ

Анализ инфраструктуры услуг — рекомендуемая отправная точка для картирования вашей среды. Выступает в роли движка "**автообнаружения**", сканирующего весь инвентарь по библиотеке предустановленных **паттернов сервисов** (Exchange, CyberArk, 1C) для автоматической идентификации и классификации бизнес-услуг.

Как это работает

1. Перейдите в **CMDB > Анализатор бизнес-услуг**.
2. Найдите карточку **Анализ инфраструктуры услуг** (помечена **"Рекомендуется"**).
3. Нажмите кнопку **Запустить анализ инфраструктуры**.

Система немедленно начнет многоэтапный процесс анализа.

Логика анализа

Анализ инфраструктуры — это не простой поиск по ключевым словам. Используется сложная многоуровневая логика для точности и снижения шума.

1. Сопоставление паттернов

Система загружает активные **Service Patterns** (паттерны сервисов) из базы данных. Каждый паттерн определяет "**отпечаток**" услуги по комбинации критериев. Сервер идентифицируется при совпадении **hostname patterns** или **software keywords**:

Hostname Patterns (опционально): *sql*, *exch* — регистронезависимый поиск по имени хоста (определяет PRD-SQL-01 как базу данных даже без ПО).
Software Keywords: "Microsoft Exchange Server", "CyberArk Password Vault" — проверка инвентаря ПО.
Process Signatures: Конкретные исполняемые файлы, которые должны работать.

Сканирует все обнаруженные **Server KE** на совпадения с отпечатками.

2. Глубокое обнаружение (Discovery) и валидация

При обнаружении потенциальной услуги (например, "**Возможный Exchange Server**") проводится **Deep Discovery (глубокое обнаружение)**:

Проверка процесса: Проверка живого списка процессов на наличие требуемых компонентов.
Анализ соединений: Анализ сетевого трафика для подтверждения связи по ожидаемым портам (порт 25/443 для Exchange).

3. Классификация и обогащение

ИИ понимает роли серверов:

Role Assignment (назначение роли): Тегирует как веб-сервер, база данных, сервер приложения по процессам.
Tiering: Организует в логические уровни: **frontend** (пользовательский), **application** (бизнес-логика), **data** (хранилище), **infrastructure** (поддержка).

4. Генерация инсайтов ИИ

Результаты передаются движку **ИИ** для оценки здоровья и рисков:

Architectural Risks (риски архитектуры): Единственные точки отказа, нестандартные конфигурации.
Security Gaps (пробелы в безопасности): Незашифрованные соединения, открытые админ-интерфейсы.
Business Impact (влияние на бизнес): Критичность услуги по зависимостям.

Просмотр результатов

После завершения анализа представлен полный список обнаруженных услуг.

Детальная классификация:

- **Service Name (Имя услуги):** Идентифицированная услуга ("Network Monitoring Platform").
- **Server Roles (Роли сервера):** веб-сервер, база данных, сервер приложения (по процессам).
- **Tiers (Уровни):** frontend, приложение, данные, инфраструктура.
- **Confidence (Уверенность):** Оценка достоверности ИИ.

Сохранить в CMDB: Отметьте услуги галочками и сохраните.

19 АНАЛИЗ УСЛУГИ ПО ПАТТЕРНАМ

Если вам нужно найти конкретный экземпляр известной услуги (например, "**Exchange Server** Финансового отдела"), используйте рабочий процесс **обнаружения по паттернам**. Этот метод позволяет выбрать готовый шаблон и запустить целевое обнаружение (discovery) для конкретной услуги.

Понимание паттернов услуг

Паттерн услуги — это чертеж, который говорит системе, как идентифицировать сложную бизнес-услугу. Решает проблему различения обычного сервера от конкретной бизнес-функции.

Как работают паттерны

Система использует подход "**отпечаток**" для идентификации серверов. Сервер считается совпадением, если соответствует критериям паттерна. Логика совпадения использует условие **OR (ИЛИ)** по разным индикаторам:

Software Keywords (Ключевые слова ПО): Проверка инвентаря установленного ПО ("Microsoft Exchange", "Oracle Database").
Process Signatures (Сигнатуры процессов): Проверка запущенных процессов (sqlservr.exe, tomcat.exe).
Hostname Patterns (Паттерны hostname): Проверка имени сервера (*exch*, *sql*).

При совпадении любого индикатора высокого доверия сервер помечается как потенциальный компонент сервиса.

Основной VS зависимый уровни

Для точного картирования **анализатор** различает ядро приложения и поддерживающую инфраструктуру с помощью **двухфазного обнаружения**.

1. Основной уровень (Ядро)

Уникальные компоненты, определяющие услугу.
Пример: Для Exchange — серверы с **MSExchangeFrontendTransport.exe**.
Логика: Сканирует всю сеть для поиска этих серверов **сначала**.

2. Зависимый уровень (Поддержка)

Общие компоненты, поддерживающие услугу, но не уникальные для нее.
Пример: SQL Server или IIS Web Server (многие услуги используют SQL).
Логика: НЕ сканирует всю сеть. Анализирует только исходящие соединения с серверов основного уровня. Включает зависимый сервер, **только** если основной сервер активно с ним общается.

Результат: Картируется конкретный SQL сервер этого экземпляра Exchange, а не все SQL в компании.

Пошаговое руководство

Шаг 1: Выбор паттерна

Из панели мониторинга **Анализатора бизнес-услуг** перейдите в библиотеку **Service Patterns (Паттерны услуги)**. Здесь находятся все шаблоны для обнаружения (discovery) корпоративных услуг.

Шаг 2: Просмотр и настройка

Перед запуском обнаружения (discovery) изучите критерии паттерна:

Основной уровень (синий): Уникальные процессы/ПО ядра услуги.
Зависимый уровень (оранжевый): Общие услуги поддержки (SQL, IIS), релевантные только при соединении с основным уровнем.

Можно отредактировать критерии под вашу среду.

Шаг 3: Запуск обнаружения (discovery)

Нажмите **"Use in Discovery"** или **"Proceed"**. Система выполнит двухфазную логику и покажет картированную карту найденного экземпляра услуги.

20 АНАЛИЗ УСЛУГИ С РУЧНЫМ ВВОДОМ

Для кастомных приложений или услуг без готового паттерна используйте **ИИ-направленное обнаружение** (**Manual Analyzer**). Этот рабочий процесс позволяет описать услугу простым языком, а движок **ИИ** поможет найти, картировать и классифицировать его.

Шаг 1: Определение профиля услуги

Начните с определения идентичности услуги. Поле **Description (Описание)** критично — **ИИ** использует его для вывода архитектурных паттернов и потенциальных компонентов.

Name (Имя): Введите узнаваемое имя (например, "**Портал записей пациентов**").
Description (Описание): Будьте конкретны в технологиях (например, "**Веб-приложение на Java/Tomcat, подключающееся к Oracle DB**").
Category (Категория): Выберите бизнес-функцию (Healthcare).

Шаг 2: Выбор известного ПО

Ищите в каталоге ПО и добавляйте известные компоненты услуги. Это задает **якорь** для поиска **ИИ**.

Шаг 3: Обогащение ИИ и конфигурация

Нажмите **Enrich Service (Обогатить услугу)**. **ИИ** анализирует описание и выбранное ПО:

Suggest Missing Components (Предложить недостающие компоненты): Предложит пропущенные компоненты (веб-сервер, кэш).
Translate to Processes (Переход в процессы): Переведет названия ПО ("PostgreSQL") в исполняемые файлы ("postgres").
Define Tiers (Определение уровня): Классифицирует в **Primary** (основной) и **Dependency** (зависимый) уровни.

Шаг 4: Визуализация и топология

Перед сохранением изучите сгенерированную топологию. Интерактивный граф показывает, как общаются обнаруженные серверы:

Синие узлы: Основные серверы приложений.
Оранжевые узлы: Зависимая инфраструктура (базы данных, auth-серверы).

Шаг 5: Проверка результатов обнаружения (discovery)

Система показывает детальную таблицу всех совпавших серверов:

Verify Roles (Проверка ролей): Убедитесь в правильной классификации (web-server vs app-server).
Check Confidence (Проверка достоверности): Оцените достоверность **ИИ** для каждого совпадения.
Exclude False Positives (Исключение ложных срабатываний): Снимите галочки с нерелевантных серверов.

21 АКТИВНЫЕ УЯЗВИМОСТИ

Страница **активных уязвимостей** — ваш центральный хаб для управления безопасностью, обнаруженной по всей инфраструктуре. Панель мониторинга обеспечивает видимость уровня уязвимости организации в реальном времени и помогает расставить приоритеты для устранения.

Понимание панели мониторинга

Панель мониторинга организована по ключевым секциям:

Статистика по состоянию

Четыре ключевых метрики дают быстрый обзор:

Метрика	Описание
Open Vulnerabilities (Открытые уязвимости)	Общее количество нерешенных уязвимостей по всем активам
Critical/High (Критическая/Высокая)	Количество наиболее критичных уязвимостей
With Known Exploits (Известный Exploit)	Уязвимости с доступным эксплойт-кодом
Overdue / Avg Days Open	Своевременность устранения

Топ уязвимых активов

Выделяет активы с наибольшим количеством уязвимостей:

Актив	Критические	Высокие	Всего
Сервер-01	5	12	27
Рабочая станция-45	2	8	15

Клик по имени актива → детали в **CMDB**.

Наиболее распространенные уязвимости

Панель показывает уязвимости, затрагивающие множество активов:

CVE ID	Риск	Затронутые КЕ
CVE-2025-1234	Критический	156
CVE-2025-5678	Высокий	89

Работа со списком уязвимостей

Фильтры

Поиск: CVE ID или название ПО
Status (Статус): Open (Открыт), In Progress (В процессе), Mitigated (Уменьшенный)
Серьезность риска: Критический, Высокий, Средний, Низкий
Exploit: Только с известными эксплойтами

Колонки таблицы уязвимостей

Колонка	Описание
Checkbox	Массовые действия
CVE ID	Уникальный ID (клик → детали CVE)
Asset (Актив)	Затронутый сервер/рабочая станция

Колонка	Описание
Software (ПО)	Уязвимое ПО и версия
Severity (Серьезность риска)	Цветовой индикатор серьезности риска
CVSS	Числовая оценка (0-10)
Status (Статус)	Текущий статус рабочего процесса
Days Open (Открытых дней)	Дней с обнаружения

Цветовая кодировка серьезности риска

Критическая (CVSS 9.0-10.0) — немедленное внимание
Высокая (CVSS 7.0-8.9) — оперативное устранение
Средняя (CVSS 4.0-6.9) — планировать
Низкая (CVSS 0.1-3.9) — по ресурсам

Детали уязвимости

Клик по **ID уязвимости** показывает:

- Полное описание уязвимости
- Разбивка CVSS scoring
- Затронутые версии ПО
- Доступные патчи
- Внешние ссылки (NVD, vendor advisories)

Экспорт данных

Экспорт CSV — все уязвимости по текущим фильтрам

Обновление данных

Refresh All (Обновить все) — повторное сканирование всех активов

Автоматическое разрешение

RS-Discovery (R-Sight) автоматически помечает уязвимости как **Resolved (Решено)** при устранении:

Сценарий	Метод разрешения	Пример
Обновление ПО	Обновление до безопасной версии	Chrome 119→137
Установка патча	Установка KB-патча	KB5066133
Удаление ПО	Удаление уязвимого ПО	Legacy app удалена

Почему уязвимости могут возвращаться

- **«Откат»** ПО до уязвимой версии
- **Удаление патча**
- **Переустановка** уязвимого ПО

22 БАЗА ДАННЫХ УЯЗВИМОСТЕЙ CVE

База данных уязвимостей CVE предоставляет доступ к полной информации о **Common Vulnerabilities and Exposures (CVE)** (Общие уязвимости и воздействия). Поисковая база содержит детальные данные о безопасностях, которые могут затрагивать ПО в вашей среде.

Понимание базы данных CVE

Статистика по состоянию

Верх страницы показывает ключевые метрики:

Метрика	Описание
Всего CVE	Полное количество CVE в базе
Критические	CVE с CVSS 9.0-10.0
Высокие	CVE с CVSS 7.0-8.9
Средние	CVE с CVSS 4.0-6.9
Known Exploits (Известный Exploit)	CVE с доступным эксплойт-кодом

Поиск и фильтры

Строка поиска: CVE ID ("CVE-2024-1234") или ключевые слова **Серьезность риска:** Критический, Высокий, Средний, Низкий **Known (известный) Exploit:** Только с подтвержденными эксплойтами

Записи CVE в таблице

Колонка	Описание
CVE ID	CVE-YYYY-NNNNN (клик → детали)
Score (Очки)	CVSS 0.0-10.0
Severity (Серьезность)	Цветовой бейдж серьезности риска
Description (Описание)	Краткое объяснение
Published (Опубликовано)	Дата публикации
CPE	Количество затронутых продуктов

Система оценки CVSS

Common Vulnerability Scoring System (CVSS) (Общая система оценки уязвимостей) стандартизирует измерение серьезности угроз и риска:

Диапазон	Серьезность	Действие
9.0-10.0	Критическая	Немедленное устранение
7.0-8.9	Высокая	В течение дней
4.0-6.9	Средняя	Планировать
0.1-3.9	Низкая	По ресурсам

Детали CVE

Клик по **CVE ID** показывает:

Информация об уязвимости

Full Description (Полное описание): Подробное объяснение
Attack Vector (Вектор атаки): Network, Local, Adjacent, Physical (Сетевой, локальный, смежный, физический)
Attack Complexity (Сложность атаки): Низкая, Высокая.
Privileges Required (Требуемые привилегии): Нет, Низкий, Высокий
User Interaction (Взаимодействие с пользователем): Нет, Требуется

Затронутые продукты

Список ПО, версий, CPE идентификаторов

Использование базы CVE

Исследование уязвимостей

Перед развертыванием ПО:

- Поиск по названию/вендору
- Проверка серьезности угроз и рисков
- Наличие патчей

Расследование алертов

При сигналах инструментов безопасности:

- Поиск конкретного CVE ID
- Вектор атаки и влияние
- Затрагивает ли вашу среду

Отчетность compliance

Экспорт для аудитов, отслеживание прогресса устранения

23 СЛОВАРЬ CPE

Словарь CPE (Common Platform Enumeration) (Общее перечисление платформ) — структурированная схема именования для ИТ-систем, ПО и пакетов. **RS-Discovery (R-Sight)** использует идентификаторы CPE для точного сопоставления обнаруженного ПО с известными уязвимостями.

Понимание словаря CPE

Статистика по состоянию

Верх страницы показывает количество по типам CPE:

Метрика	Описание
Total CPEs (Всего CPE)	Полное количество записей CPE
Applications (Приложения)	ПО-приложения (part='a')
Operating Systems (ОС)	Операционные системы (part='o')
Hardware (Оборудование)	Аппаратные устройства (part='h')

Фильтры

Поиск: по вендору, продукту, CPE ID
Тип: Application, Operating System, Hardware (Приложение, ОС, Оборудование)

Структура CPE

Идентификаторы CPE имеют стандартный формат:
cpe:2.3:a:microsoft:edge:120.0.2210.91:*:*:*:*:*:*:*

Разбор компонентов:

Компонент	Значение	Значение
cpe:2.3	Версия спецификации	CPE 2.3
a	**Part**	Application (a), OS (o), Hardware (h)
microsoft	**Vendor**	Вендор ПО
edge	**Product (Продукт)**	Название продукта
120.0.2210.91	**Version (Версия)**	Конкретная версия
*	Update (Обновление)	Уровень патча (любой)
*	Edition	Издание продукта
*	Language	Язык
*	SW Edition	Редакция ПО
*	Target SW	Целевое ПО
*	Target HW	Целевое оборудование
*	Other	Прочие атрибуты

Колонки таблицы CPE

Колонка	Описание
Type (Тип)	Application/OS/Hardware (Приложение, ОС, Оборудование)
Vendor (Вендор)	Вендор/производитель
Product (Продукт)	Название продукта
Version (Версия)	Конкретная версия
Title (Заголовок)	Читаемое название
Status (Статус)	Active/Deprecated (Активно / Устарело)

Использование словаря CPE

Проверка идентификации ПО

При проверке обнаруженного ПО:

- Поиск по названию ПО
- Проверка соответствия CPE версии
- Корректность маппинга вендора

Исследование затронутых продуктов

Для CVE:

- Изучить затронутые CPE
- Поиск в словаре CPE
- Сопоставление с инвентарем

Устранение проблем сопоставления

Если уязвимости не появляются:

- Найти ПО в словаре CPE
- Проверить версионность
- Статус CPE (Active – Активен)
- Связанные CVE

Типы CPE

Приложения (part='a')

- Браузеры: Chrome, Firefox, Edge
- Office: Microsoft Office, LibreOffice
- Серверы: Apache, MySQL, SQL Server

ОС (part='o')

- Windows Server/Desktop
- Linux: Ubuntu, RHEL, CentOS
- macOS, Unix

Оборудование (part='h')

- Сетевое оборудование
- Принтеры, IoT

Как работает сопоставление CPE

RS-Discovery (R-Sight) автоматически сопоставляет:

1. **Discovery (Обнаружение):** Сбор имени/версии ПО
2. **Normalization:** Стандартизация названий
3. **CPE Lookup:** Поиск CPE ID
4. **CVE Correlation (Связи CVE):** Связанные уязвимости

5. **Version Checking (Проверка версий):** Только релевантные версии

Version-Aware Matching (Сопоставление с учетом версий)

Проверка диапазонов версий:

- versionStartIncluding — первая затронутая
- versionEndExcluding — первая исправленная
- versionStartExcluding — после этой затронуты
- versionEndIncluding — последняя затронутая

Обновление словаря

Refresh (Обновление) — синхронизация последних данных CPE:

- Новые продукты
- Обновления версий
- Deprecated CPE (Устаревшие)

Лучшая практика: Автообновление + ручное обновление после крупных развертываний ПО.

24 СОПОСТАВЛЕНИЯ KB-CVE

Страница **KB-CVE Mappings** показывает связь патчей **Microsoft Knowledge Base (KB – Базы знаний (БЗ))** с **CVE**, которые они исправляют. Эта информация критически важна для точного расчета уязвимостей на **Windows**-системах.

Зачем нужны сопоставления KB-CVE

При расчете уязвимостей недостаточно знать, какие **CVE** затрагивают ПО — нужно знать, какие уже исправлены патчами. **KB-CVE mappings** позволяют **RS-Discovery (R-Sight)**:

Reduce False Positives (Уменьшение количества ложных срабатываний): Исключить CVE, уже исправленные установленными патчами
Calculate True Exposure (Расчет истинного риска): Показывать только действительно неисправленные уязвимости
Prioritize Remediation (Приоритет исправлений): Фокус на уязвимостях без доступных фиксов

Понимание сопоставлений KB-CVE

Статистика по состоянию

Метрика	Описание
KB Articles (Статьи БЗ)	Общее количество патчей Microsoft в базе
Unique CVEs (Уникальные CVE)	CVE, исправляемые отслеживаемыми патчами
Critical (Критические)	Патчи для CVE критичной серьезности
Important (Важные)	Патчи для важных CVE

Поиск и фильтры

Поиск: Номер KB или название
Severity (Серьезность): Уровень серьезности патча
Date Range (Диапазон дат): Период выпуска

Детали записи KB

Поле	Описание
KB ID	Идентификатор (KB5034441)
Title (Заголовок)	Описание обновления безопасности
Release Date (Дата релиза)	Дата выпуска патча
Severity (Серьезность)	Общая серьезность
CVEs Fixed (Исправленные CVE)	Список исправляемых CVE
Affected Products (Затронутые продукты)	Версии Windows

Во время оценки уязвимостей

1. **CVE Identification (Идентификация CVE):** Определение CVE для установленного ПО
2. **KB Lookup:** Получение установленных патчей из данных сканирования
3. **Mapping Check (Проверка маппинга):** Проверка каждого KB на исправляемые CVE

4. **Exclusion (Исключения):** Исключение исправленных CVE из отчета
5. **True Exposure (Истинная экспозиция):** Только неисправленные уязвимости

Практический пример

Windows Server 2022 + SQL Server 2019
Потенциальные CVE:

- CVE-2024-21302 (Windows Kernel)
- CVE-2024-21303 (SQL Server)
- CVE-2024-21304 (Windows RDP)

Установленные патчи: KB5034123
KB-CVE Mapping: KB5034123 исправляет CVE-2024-21302 и CVE-2024-21304
Результат: В отчете только CVE-2024-21303

Cumulative Updates (Накопительные обновления)

Включают:

- Все предыдущие исправления безопасности
- Улучшение качества
- Предыдущие cumulative updates (накопительные обновления)

Последнее накопительное обновление защищает от многих старых CVE.

Использование сопоставлений KB-CVE

Проверка покрытия патчами

Для конкретного CVE:

- Поиск CVE ID
- Какие KB его исправляют
- Установлены ли эти KB

Планирование развертывания патчей

- Выявить приоритетные неисправленные CVE
- Найти KB для них
- Проверить совместимость с Windows

Аудит статуса патчей

- Экспорт данных маппинга
- Сопоставление с установленными патчами
- Документация покрытия

Ограничения

Windows-Specific (Специально для Windows): Только для продуктов Microsoft
Mapping Completeness (Полнота сопоставления): Не все KB имеют CVE mappings
Feature Updates (Обновления функций): Отдельное отслеживание

25 РУКОВОДСТВО ПО ДЕМО. ВХОД В ДЕМО-СРЕДУ

Это руководство поможет вам войти в демо-среду **RS-Discovery (R-Sight)**, настроить двухфакторную аутентификацию и персонализировать интерфейс.

Шаг 1: Доступ к странице входа

1. На странице входа введите **Email** и **Password**, предоставленные администратором
2. Нажмите **Sign In** (Войти)

Шаг 2: Настройка двухфакторной аутентификации (2FA)

При первом входе требуется настроить **Two-Factor Authentication (2FA)** для защиты аккаунта.

1. **QR-код** отобразится на экране
2. Откройте приложение-аутентификатор
3. Отсканируйте **QR-код** приложением
4. **Или** вручную введите ключ под QR-кодом
5. Введите **6-значный код** из приложения-аутентификатора
6. Нажмите **Verify & Enable** (Проверить и включить)

Шаг 3: Сохранение резервных кодов

После успешной настройки **2FA** вы получите набор **Backup Codes** (резервных кодов).

- **Назначение:** Доступ к аккаунту при потере устройства-аутентификатора
- **Важно:** Каждый код однократного использования
- **Храните безопасно**
- Нажмите **Continue to Dashboard** (Продолжить к панели мониторинга)

Критично: Обязательно сохраните резервные коды в безопасном месте.

Шаг 4: Добро пожаловать в панель мониторинга

После аутентификации вы попадете в главную панель мониторинга.

Панель мониторинга показывает обзор инфраструктуры:

- **Total Server Count (Общее количество серверов)** — количество обнаруженных серверов
- **Total Workstation Count (Общее количество рабочих станций)** — количество рабочих станций
- **Total Software Instance Count (Общее количество экземпляров ПО)** — все установки ПО
- **Total Hardware Count (Общее количество оборудования)** — физическое и виртуальное оборудование
- **CI Types Distribution (Описание типов КЕ)** — распределение типов КЕ
- **CMDB Data Freshness Score (Показатель актуальности данных CMDB)** — актуальность данных обнаружения

Шаг 5: Настройка темы (опционально)

RS-Discovery (R-Sight) предлагает несколько предустановленных тем:

1. Кликните **Configuration** (Конфигурация) в левой боковой панели
2. Выберите **Theme** (Тема) из подменю
3. **Доступные темы:**
   - **Default Blue** — классическая синяя
   - **Dark Purple** — темная с фиолетовыми акцентами
   - **Ocean Blue** — спокойные океанские тона
   - **Forest Green** — природный зеленый

- **Sunset Orange** — теплые закатные цвета
- **Midnight** — глубокий темный с синими акцентами

4. Кликните любую тему для мгновенного применения

26 ИССЛЕДОВАНИЕ CMDB

База данных управления конфигурацией (CMDB) — центральное хранилище всей обнаруженной инфраструктуры в **RS-Discovery (R-Sight)**. Это руководство поможет изучить **конфигурационные единицы (КЕ)**, использовать фильтры и просматривать детальную информацию об активах.

Доступ к списку КЕ

1. В левой боковой панели кликните **CMDB**
2. Выберите **CI List (Список КЕ)** из развернутого меню

Откроется основная страница **Configuration Items (Конфигурационные единицы)** со всеми обнаруженными активами вашей среды.

Понимание интерфейса

Интерфейс **CI List (Списка КЕ)** состоит из трех основных областей:

Секция заголовков

- Название **Configuration Items (Конфигурационные единицы)** с общим количеством КЕ
- Кнопка **Export to CSV (Экспорт в CSV)** — скачать текущий отфильтрованный список
- Кнопка настройки колонок — показывать/скрывать и менять порядок колонок
- Кнопка **+ New CI (Новая КЕ)** — ручное создание новой КЕ

Боковая панель фильтров (слева)

Мощные возможности фильтрации для сужения списка КЕ.

Таблица КЕ (основная область)

Отображает все КЕ по текущим фильтрам с сортируемыми колонками.

Использование фильтров

Боковая панель фильтров позволяет быстро найти конкретные КЕ.

Доступные фильтры

Строка поиска

Свободный текстовый поиск по:

- Имя КЕ, серийный номер, IP-адрес и другие поля
- Результаты обновляются автоматически при вводе

Типы КЕ

Фильтр по типу КЕ:

Тип КЕ	Описание	Количество
All Types	Все КЕ	N
Server	Физические и виртуальные серверы	N
ESX Server	Хосты VMware ESX	N
Network	Сетевые устройства	N
Storage	Массивы и устройства хранения	N
Business Service	Логические бизнес-сервисы	N
VCenter Datacenter	Дата-центры VMware	N
Workstation	Рабочие станции	N

Тип КЕ	Описание	Количество
VMWare VCenter	Серверы vCenter	N
VCenter Cluster	Кластеры VMware	N
Monitor	Мониторы	N

Статус

Фильтр по эксплуатационному статусу:

- **All Statuses** — все статусы
- **Active** (Активен) — в работе
- **Inactive** (Неактивен) — не используется
- **Maintenance** (На обслуживании) — на обслуживании

External Source (Внешний источник)

Фильтр по статусу интеграции:

- **All** — все КЕ
- **Linked to R-Service (Связан с R-Service)** — синхронизированы с внешним ITSM
- **Not Linked (Не связан)** — не связаны с внешними системами

Manufacturer (Производитель)

Фильтр по производителю оборудования: HP, Dell Inc., Lenovo, VMware

27 ИССЛЕДОВАНИЕ РАБОЧИХ СТАНЦИЙ

Это руководство поможет изучить **рабочие станции** (ноутбуки или настольные ПК) в **CMDB**, включая системную информацию, аппаратные детали и связанные коллекции данных.

Фильтрация по рабочим станциям

1. Перейдите в **CMDB > CI List (Список КЕ)**
2. В боковой панели фильтров разверните **CI Types (Типы КЕ)**
3. Кликните **Workstation (Рабочие станции)**

Таблица теперь показывает **только рабочие станции**.

Открытие деталей Workstation (рабочих станций)

Кликните по любой строке рабочей станции (например, **DEMO-WS01**) для открытия страницы подробностей.

Страница деталей КЕ

CI Details (Подробности КЕ) предоставляет полную информацию о выбранной рабочей станции.

Секция заголовков

- Кнопка **Back (Назад)** — возврат к списку КЕ
- **Имя КЕ** и тип (**Workstation – Рабочая станция**)
- **Бейдж статуса** — текущий статус (active/inactive/maintenance – Активен, Неактивен, На обслуживании)
- Кнопка **Edit CI (Редактировать КЕ)** — изменить атрибуты КЕ

Навигационные вкладки

- **Overview (Обзор)** — общая информация и свойства
- **Relationships (Связи)** — связанные КЕ и зависимости
- **Change History (История изменений)** — аудит изменений
- **AI Insights (Аналитические данные ИИ)** — анализ и рекомендации ИИ
- **Relationships Workbench (Рабочая область связей)** — визуальное картирование связей

Секции вкладки обзора (Overview)

Системная информация

Для рабочих станций включает:

- **Domain (Домен)** — членство в домене Active Directory
- **OS Name (Название ОС)** — ОС (например, **Microsoft Windows 11 Pro**)
- **OS Version (Версия ОС)** — номер версии (например, **10.0.22631**)
- **OS Build (Сборка ОС)** — номер сборки

Аппаратная информация

- **Manufacturer (Производитель)** — производитель (например, **Lenovo**)
- **Model (Модель)** — модель (например, **ThinkPad X1 Carbon Gen 9**)
- **Serial Number (Серийный номер)** — уникальный идентификатор
- **CPU Model (Модель процессора)** — процессор (например, **11th Gen Intel Core i7-1165G7**)
- **CPU Cores (Ядра процессора)** — физические ядра
- **CPU Threads (Потоки процессора)** — логические потоки
- **Memory GB (Память)** — общий объем RAM

Сетевая информация

- **IP Address** — назначенный IP-адрес
- **MAC Address** — аппаратный адрес адаптера

- **MAC Addresses** — все сетевые адаптеры

Коллекции (связанные данные)

Внизу вкладки обзора **(Overview)** — вкладочные коллекции с данными, обнаруженными на рабочей станции.

Доступные коллекции для рабочей станции (Workstation)

Disks (Диски)

- Буквы дисков и точки монтирования
- Общий объем и свободное место
- Тип диска (**SSD**, **HDD**)
- Тип файловой системы

User Accounts (Пользовательские аккаунты)

- Имя пользователя
- Тип аккаунта (**Admin**, **Standard – Администратор, Стандартный**)
- Дата последнего входа

Network Connections (Сетевые соединения)

- Удаленные IP-адреса
- Порты и протоколы
- Состояние соединения

Installed Applications (Установленные приложения)

- Название приложения
- Издатель
- Версия
- Дата установки

Network Adapters (Сетевые адаптеры)

- Название и тип адаптера
- IP-конфигурация
- Статус DHCP

Physical Disks (Физические диски)

- Модель диска
- Емкость
- Интерфейс (**SATA**, **NVMe**)

Connected Monitors (Подключенные мониторы)

- Производитель и модель монитора
- Серийный номер
- Размер экрана (дюймы)
- Разрешение
- Год выпуска

Peripheral Devices (Периферийные устройства)

- Тип устройства
- Производитель
- Статус подключения

28 ИССЛЕДОВАНИЕ СЕРВЕРА

Это руководство поможет изучить **сервер** в **CMDB**, включая аппаратные детали, установленные приложения, сетевые соединения и связи, обогащенные **ИИ**.

Фильтрация по серверам

1. Перейдите в **CMDB > CI List (Список КЕ)**
2. В боковой панели фильтров разверните **CI Types (Типы КЕ)**
3. Кликните **Server (Серверы)**

Таблица показывает **только серверы КЕ.** В демо-среде вы увидите SAP HANA базы данных, серверы приложений и инфраструктурные серверы.

Открытие деталей сервера

Кликните по **HANADB01** — сервер базы данных **SAP HANA** на **VMware**.

Обзор сервера

Страница подробностей сервера показывает полную информацию:

Аппаратная информация

- Manufacturer: VMware, Inc.
- Model: VMware Virtual Platform
- Serial Number: DELL-HANA-001
- CPU Model: Intel(R) Xeon(R) Gold 6348 CPU @ 2.60GHz
- CPU Cores: 24 физических ядра
- CPU Threads: 48 логических потоков
- Memory GB: 128 GB RAM

Сетевая информация

- IP Address: 120.120.120.51
- MAC Address: Аппаратные адреса адаптеров
- Network Adapter Manufacturer: Broadcom

Коллекции для серверов

Серверы имеют дополнительные коллекции по сравнению с рабочими станциями.

Сетевые соединения

Вкладка Network Connections (Сетевые соединения) показывает активные соединения:

Поле	Описание
Protocol (Протокол)	TCP/UDP
Local Address (Локальный адрес)	IP сервера
Local Port (Локальный порт)	Порт прослушивания
Remote Address (Удаленный адрес)	IP удаленного хоста
Remote Port (Удаленный порт)	Удаленный порт
State (Состояние)	ESTABLISHED, LISTENING
PID	ID процесса
Process Name (Имя процесса)	hdbindexserver, hdbwebdispatcher

Установленные приложения

Вкладка Installed Applications (Установленные приложения) — инвентарь ПО:

Поле	Описание
Name (Имя)	SAP HANA Database, SAP Host Agent
Vendor (Вендор)	SAP SE
Version (Версия)	Номер версии
Install Date (Дата установки)	Дата установки
Install Location (Место установки)	/usr/sap/HDB
CPE Name (Имя CPE)	Идентификатор для сопоставления уязвимостей
Software Instance CI Id (ID экземпляра ПО КЕ)	Ссылка на КЕ в CMDB

Другие коллекции серверов

- **Disks (Диски)** — физическое и логическое хранилище
- **User Accounts (Аккаунты пользователей)** — локальные и доменные аккаунты
- **Network Adapters (Сетевые адаптеры)** — конфигурация интерфейсов
- **Events (События)** — системные события и логи

Вкладка Relationships (Связи)

Показывает, как сервер связан с другими компонентами инфраструктуры.

Как обнаруживаются связи

RS-Discovery (R-Sight) автоматически анализирует сетевые соединения из сканирований:

- **Active TCP/UDP connections** — все установленные соединения
- **Listening ports** — сервисы сервера
- **Process information** — приложение/процесс для каждого соединения

Колонки таблицы связей

Колонка	Описание
Target CI (Целевая КЕ)	Сервер/устройство на другом конце
Type (Тип)	Тип КЕ цели
Relationship (Связь)	Connected To, Runs On, Depends On
Port/Direction (Порт/Направление)	Сервисный порт и направление (IN/OUT)
Process (Процесс)	Процессы: S: (source), T: (target)
Application (Приложение)	Приложение по версии ИИ
Software Family (Семейство ПО)	Категория ИИ (Database, Enterprise Apps)

Понимание информации о портах и процессах

Информация о портах

Port: 3200 — известный сервисный порт **L:30013** → **R:50001** — локальный порт → удаленный порт

→ **OUT** — оранжевый бейдж (исходящее соединение)
← **IN** — зеленый бейдж (входящее соединение)

Информация о процессах

S: hdbindexserver — исходный процесс (на исходной КЕ)
T: disp+work.exe — целевой процесс (на целевой КЕ)

Примеры процессов SAP:

- **hdbindexserver** — сервер индексов SAP HANA
- **hdbwebdispatcher** — веб-диспетчер SAP HANA
- **disp+work.exe** — диспетчер SAP application server

Визуальная карта зависимостей

Верхняя секция показывает **интерактивную диаграмму** связей сервера:

- **Узлы серверов** — подключенные серверы (SAPPI01, SAPBW01, GATEWAY01)
- **Линии соединений** — связи "Connected To" со стрелками направления
- **Легенда** — типы Server (Сервер), Software (ПО), Software Instance (Экземпляр ПО)
- **Управление зумом** — увеличение/уменьшение, подгонка под экран

Связи, обогащенные ИИ

RS-Discovery (R-Sight) использует **ИИ** для автоматического обогащения данных связей бизнес-контекстом:

Идентификация приложений

ИИ анализирует:

- Имена процессов
- Номера портов
- Известные паттерны ПО
- Установленные приложения

Группировка по семействам

В таблице связей соединения сгруппированы по **семействам ПО** (accordion секции):

- Все **database (базы данных)** соединения вместе
- Зависимости корпоративных приложений
- Связи систем мониторинга

Почему это важно?

Понимание связей помогает:
Impact Analysis (Анализ влияния) — что зависит от сервера перед изменениями
Troubleshooting (Устранение неполадок) — трассировка проблем соединений
Change Management (Менеджмент изменений) — планирование окон обслуживания
Security Analysis (Анализ безопасности) — паттерны сетевой коммуникации
Documentation (Документация) — актуальная документация зависимостей

29 ПРЕДСТАВЛЕНИЕ СВЯЗЕЙ ИИ

При множестве связей **Представление связей ИИ** предоставляет глубокий анализ с оценкой рисков.

Доступ к AI Relations

На вкладке **Relationships (Связи)** нажмите на переключатель **AI Relations** (между Table View – Табличное Представление и Risk/Impact – Риск/Влияние).

Интерфейс AI Relations

Показывает:

AI Relationships for [Server Name] (Связи ИИ для Имя Сервера) — заголовок
Connection count (Количество соединений): "9 сетевых соединений (только Connected To)"
Analysis status (Статус анализа): "AI Analyzed (9) – Анализируется ИИ" / серый "Pending (0) – В ожидании"
AI Analyze (Анализ ИИ) — запуск/обновление анализа

Запуск анализа ИИ

Клик на **AI Analyze (9) (Анализ ИИ)** анализирует:

- Паттерны сетевых соединений
- Процессы и порты
- Сигнатуры приложений
- Топологию инфраструктуры
- Бизнес-контекст из ПО

Карточки связей ИИ

Каждая связь — **карточка** с анализом **ИИ**:

Заголовок карточки

CI Name (Имя КЕ): подключенный сервер (HANADB01, SAPPRD01)
Relationship Badge (Бейдж связей): "Connected To" (оранжевый)

Детали соединения

Source (Источник) → **Target (Цель)** | **Type (Тип):** Connected To

AI Insights (Аналитические данные ИИ)

Purpose (Цель):

- "Сетевое шлюзовое соединение к SAP HANA"
- "База данных SAP HANA ↔ SAP Solution Manager"
- "Службы базы данных для SAP Production"

Risk Level (Уровень риска):
Critical (Критический) — критическая инфраструктура
High (Высокий) — важные бизнес-соединения
Medium (Средний) — стандартные операции
Low (Низкий) — некритичные

Business Impact (Бизнес-влияние):
Critical (Критическое) — остановка бизнеса
High (Высокое) — значительное нарушение
Medium (Среднее) — частичное влияние
Low (Низкое) — минимальное

Description (Описание):
Подробное объяснение каждой связи

Примеры результатов анализа ИИ

ИИ идентифицирует различные типы соединений:

Соединение	Назначение	Риск	Бизнес-влияние
GATEWAY01 → HANADB01	Сетевое шлюзовое соединение к БД	**Критический**	**Критический**
SOLMAN01 ↔ HANADB01	Мониторинг SAP Solution Manager	**Высокий**	**Высокий**
SAPPI01 → HANADB01	SAP Process Integration	**Высокий**	**Высокий**
SAPBW01 → HANADB01	SAP Business Warehouse	**Высокий**	**Высокий**
SAPPRD01 ↔ HANADB01	Службы продакшен БД	**Критический**	**Критический**
SAPPRD03 → HANADB01	Обработка данных app-сервера	**Критический**	**Критический**
HANADB02 ↔ HANADB01	Репликация БД/HA	**Высокий**	**Средний**
SAPPRD02 → HANADB01	Prod обработка данных	**Критический**	**Критический**
DIALOG01 → HANADB01	Dialog instance → БД	**Критический**	**Критический**

Как работает анализ ИИ

AI relationship выполняет:

1. **Collects Connection Data (Сбор данных о подключении)** — собирает сетевые соединения из сканирований
2. **Correlates with CIs (Связи с КЕ)** — сопоставляет IP с известными КЕ
3. **Analyzes Context (Анализ контекста)** — анализирует процессы, порты, установленные приложения
4. **Generates Insights (Генерация аналитических данных)** — **ИИ** определяет:
   - Бизнес-назначение каждой связи
   - Уровень риска (критичность + избыточность)
   - Бизнес-влияние (затронутые услуги)
   - Релевантные теги
5. **Stores Results (Сохранение результатов)** — сохраняет метаданные ИИ

Использование AI Relations для Change Management (Управления изменениями)

Перед изменениями на сервере:

- Просмотреть **критические и высокие связи**
- Определить зависимые бизнес-услуги
- Запланировать окна обслуживания
- Подготовить коммуникацию для заинтересованных сторон
- Создать процедуры отката

Обновление анализа ИИ

Клик **AI Analyze** при:

- Новых обнаруженных соединениях
- Изменениях конфигурации сервера
- Модификации установленных приложений

Статус анализа:
AI Analyzed (N) — проанализировано соединений
Pending Analysis (N) — ожидают анализа

Вкладка AI Insights (Аналитические данные ИИ)

AI Insights (Аналитические данные ИИ) — комплексный анализ сервера **ИИ** по оборудованию, ПО, безопасности, связям и рекомендациям. В отличие от **AI Relations** (фокус на связях), это **анализ** всех КЕ как **единого целого**.

Доступ к AI Insights (Аналитическим данным ИИ)

На странице сервера → вкладка **AI Insights**
Regenerate Insights (Восстановить аналитические данные) — если инсайтов нет
Refresh/Regenerate (Обновить/Восстановить) — обновить существующие

Генерация и обновление

Ручной запуск (не авто при discovery – обнаружении):

- Контроль времени анализа ИИ
- Перегенерация после изменений
- Управление затратами на ИИ

Категории инсайтов

Вкладка	Фокус
Advanced Analysis (Расширенный анализ)	Инфраструктура, оборудование, ПО, операции
Compliance	Оценка соответствия нормативным требованиям
Security (Безопасность)	Безопасность и уязвимости

Вкладка Advanced Analysis (Расширенный анализ)

Расширенный анализ предоставляет комплексные инсайты, организованные по секциям:

Обзор

Высокий уровень назначения и роли сервера:

"HANADB01 — высокопроизводительный виртуальный сервер **VMware** на **SUSE Linux Enterprise Server 15 SP3**, выполняющий роль базы данных **SAP HANA** в домене **sap.local**. С мощным оборудованием (24 ядра CPU, 48 потоков, 128GB RAM) предназначен для высокоскоростной обработки данных и аналитики в реальном времени. Обеспечивает критические услуги БД для приложений SAP (транзакционные и аналитические нагрузки)".

Аппаратная часть и производительность

Анализ конфигурации:

- **CPU:** Intel Xeon Gold 6348 (24 ядра, 48 потоков)
- **Memory:** 128GB RAM для in-memory computing
- **VMware** виртуальная платформа
- Ресурсы для требований **SAP HANA**
- **Broadcom NetXtreme II** для высокопроизводительной сети

ПО и безопасность

Анализ стека ПО:

- **SUSE Linux Enterprise Server 15 SP3**
- Сертификация и оптимизация **SAP HANA**
- Database engine, system/tenant databases
- Административный пользователь (**hdbadm**)
- Шифрование, аутентификация, аудит

Сеть и подключения

- IP/MAC конфигурация
- Высокопроизводительная сеть для транзакций БД
- Репликация и бэкапы данных
- Соединения с **SAPPRD01**, **GATEWAY01**
- Поток данных SAP landscape

Безопасность учетных записей

- Настройка **hdbadm**
- Интеграция с доменом **sap.local**
- Контроли доступа БД
- SQL permissions
- Шифрование БД и безопасность бэкапов

Резервирование и доступность

- Требования высокой доступности
- System replication (Репликация системы)
- Рекомендации по бэкапам/восстановлению
- Point-in-time recovery (Восстановление в определенной временной точке)
- Zero-downtime операции (Отсутствие простоев)

Ключевые связи

Сервер	Влияние	Описание
SAPPRD01	**Critical**	Основной app-сервер SAP
GATEWAY01	**Critical**	Шлюз для внешнего доступа SAP/Fiori
SOLMAN01	**High**	Solution Manager мониторинг
SAPBW01	**High**	Business Warehouse аналитика

Рекомендации ИИ

1. **SAP HANA system replication** для HA/DR
2. **Автоматические бэкапы** с point-in-time recovery
3. **HANA performance monitoring (Мониторинг производительности)**
4. **Шифрование данных** (at rest/in transit)
5. **HANA audit logging (ведение журнала аудита)**
6. **Tenant database optimization (Оптимизация базы данных тенанта)**
7. **Backup verification/testing (Проверка/Тестирование резервных копий)**
8. **HANA Cockpit** для администрирования

Факторы риска

Единая точка отказа для всех SAP данных
Риск потери данных без бэкапов/репликации
Узкое место в производительности при высокой нагрузке
Риск для непрерывности бизнеса без DR

Аномалии

HANA без репликации/кластеризации системы
Virtual platform (виртуальная платформа) для in-memory БД
Ограниченная видимость HANA-конфигурации

Точки отказа

Сбой HANA → полное отключение SAP
Исчерпание памяти → деградация производительности
Сбой хранилища → потеря данных
Проблемы с сетью → изоляция БД
Сбой хоста VM → недоступность HANA

Какие данные анализируются

AI Insights processor обрабатывает:

- **Raw Scan Data** (WMI/SSH): ОС, оборудование, сеть, ПО, пользователи (только количество)
- **CI Relationships (Связи КЕ)** — связанные серверы
- **Installed Applications (Установленные приложения)** — инвентарь с версиями
- **Network Connections (Сетевые соединения)** — активные соединения

Как работает анализ

1. **Data Collection (Коллекция данных)** — сбор всех данных КЕ
2. **Data Cleaning (Очистка данных)** — удаление чувствительных данных
3. **AI Processing (Обработка ИИ)** — анализ **AI**
4. **Insight Generation** — структурированные инсайты
5. **Storage (Хранение)** — сохранение привязки к КЕ

Использование AI Insights

- Понимание роли сервера
- Оценка уровня безопасности
- Планирование мощностей
- Приоритизация действий
- Автоматическая документация
- Подготовка к изменениям

Лучшие практики

- **Регенерация** после крупных изменений
- **Регулярный обзор**
- **Критическое в первую очередь** → Высокое → Среднее
- Комбинировать с **AI Relations**

30 АНАЛИЗАТОР БИЗНЕС-УСЛУГ

Business Service Analyzer — инструмент на базе **ИИ**, который автоматически обнаруживает бизнес-услуги и их зависимости, анализируя данные инфраструктуры. Преобразует сырые данные соединений в осмысленные карты бизнес-услуг.

Что такое Business Service Analyzer (Анализатор бизнес-услуг)?

Помогает:

Автоматическое обнаружение бизнес-услуг — автообнаружение бизнес-услуг из данных инфраструктуры
Зависимости карты — картирование зависимостей между серверами, приложениями, базами данных
Классификация компонентов по уровням — классификация по уровням (**frontend**, **приложение**, **данные**, **инфраструктура**)
Визуализация архитектуры — визуализация архитектуры интерактивными графами топологии
Генерация идей — инсайты о рисках, рекомендациях, узких местах

Три способа анализа

Метод	Лучше всего для	Как работает
Анализ инфраструктуры	Комплексное обнаружение	Сканирование всей инфраструктуры по всем паттернам
Обнаружение на основе паттернов	Известные типы сервисов (Exchange, CyberArk)	Выбор конкретного паттерна для поиска
Ручной ввод	Конкретные известные серверы	Ручной выбор серверов для бизнес-услуги

Панель мониторинга Business Services (Бизнес-услуги) показывает два основных варианта:
Perform Infrastructure Analysis (Выполнение анализа инфраструктуры) — рекомендуется для полного обнаружения
Analyze a Business Service (Анализ бизнес-услуги) — паттерны или ручное обнаружение

Панель мониторинга отображает:

- Общее количество обнаруженных услуг
- **Карточки услуг** с категорией, критичностью, количеством серверов и соединений
- **Фильтры** для поиска и фильтрации по категории/статусу
- **Подробности** для изучения услуг

31 АНАЛИЗ ИНФРАСТРУКТУРЫ

Infrastructure Analysis (Анализ инфраструктуры) — рекомендуемая отправная точка для картирования вашей среды. Автоматически сканирует всю инфраструктуру по всем доступным паттернам сервисов для обнаружения и классификации бизнес-услуг без ручного выбора паттернов.

Как это работает

Анализ выполняется в **4 фазы**:

1. **Fetch Configuration Items (Извлечение КЕ)** — загрузка всех КЕ типа «сервер» из CMDB
2. **Load Installed Software (Загрузка установленного ПО)** — получение инвентаря ПО для сопоставления паттернов
3. **Pattern Matching (Сопоставление паттернов)** — сопоставление КЕ со всеми активными паттернами (Exchange, CyberArk и др.)
4. **Deep Analysis (Глубокий анализ)** — для каждого найденного сервиса: discovery (обнаружение), классификация, генерация AI insights

Запуск Анализа инфраструктуры

Шаг 1: Доступ к **Анализатору бизнес-услуг** Левая панель → **CMDB** → **Анализатор бизнес-услуг**

Шаг 2: Клик **"Perform Infrastructure Analysis" (Выполнить анализ инфраструктуры)**

Синяя кнопка вверху страницы. Анализ начинается сразу с отображением прогресса в реальном времени.

Прогресс анализа

Экран прогресса показывает этапы:

Фаза 1: Сбор данных

Шаг	Описание
Начало анализа инфраструктуры	Инициализация анализатора
Получение КЕ сервера	Загрузка КЕ сервера
Найдено X конфигурационных единиц	Общее кол-во серверов для анализа
Загрузка данных об установленном ПО	Инвентарь ПО
Найдено X установленных приложений	Пакеты для сопоставления

Фаза 2: Сопоставление паттернов

Шаг	Описание
Идентификация паттернов сервисов	Сопоставление по всем паттернам
Идентифицировано X паттернов сервисов	Кол-во найденных сервисов

Фаза 3: Обработка сервисов

Для каждого сервиса **4 шага:**

1. **КЕ и обнаружение соединений** — поиск серверов и связей
2. **Классификация ролей и уровней** — роли (веб-сервер, база данных) и уровни (frontend, данные)
3. **AI insights** — бизнес-влияние, безопасность, рекомендации

4. **Сохранение записи сервиса** — сохранение в CMDB

Результаты анализа

Обнаруженные сервисы отображаются как **карточки** на панели мониторинга:

Элементы карточки сервиса

Элемент	Описание
Service Name (Имя сервиса)	Название
Category Badge (Бейдж категории)	Категория (Инфраструктура, Безопасность, Предприятие)
Auto Discovered (Автоматическое обнаружение)	Найден через Анализ инфраструктуры
Description (Описание)	Назначение сервиса
Criticality (Критичность)	Критичность (Критичный, Высокий, Средний, Низкий)
Server Count (Количество серверов)	Кол-во серверов
Connection Count (Количество соединений)	Кол-во соединений
Last Analyzed (Последний анализ)	Дата последнего анализа

Детали сервиса

"Показать подробности" на карточке показывает:

- **Servers Tab (Вкладка Серверы)** — серверы с ролями/уровнями
- **Connections Tab (Вкладка Соединения)** — сетевые связи
- **Insights Tab (Вкладка Insights)** — AI-анализ, рекомендации, риски
- **Visualization Tab (Вкладка визуализации)** — интерактивный граф топологии

Когда использовать Анализ инфраструктуры

Использовать когда:

- Нужен полный обзор всех услуг
- Начинаете с нуля и не знаете, что имеется
- Валидация каталога услуг по инфраструктуре
- Поиск по всем категориям сразу

Pattern-Based Discovery (Обнаружение на основе паттернов) — когда знаете конкретный сервис или нужна кастомизация.

Лучшие практики

Перед запуском:

- Актуальные discovery scans
- Проверка паттернов в **CMDB > Business Service Patterns (Паттерны бизнес-услуг)**
- Время на анализ (2-3 мин для больших сред)

После анализа:

- Проверка найденных сервисов
- Верификация ролей/уровней
- Выполнение рекомендаций AI

- Регулярный повторный анализ

32 ОБНАРУЖЕНИЕ ПО ПАТТЕРНАМ

Pattern-Based Discovery (Обнаружение на основе паттернов) позволяет обнаружить конкретную бизнес-услугу, выбрав предопределенный паттерн. Метод дает полный контроль над критериями обнаружения — идеален, когда точно знаете, какую услугу картировать.

Что такое Паттерны услуг (Паттерны сервисов)?

Service Patterns (Паттерны сервисов/услуг) — преднастроенные шаблоны для идентификации бизнес-услуг. Каждый паттерн содержит:

- **Process signatures (Сигнатуры процессов)** — уникальные исполняемые файлы
- **Software keywords (Ключевые слова для ПО)** — связанные установленные приложения
- **Hostname patterns (Паттерны имен хостов)** — конвенции именования серверов
- **Port ranges (Диапазоны портов)** — используемые сетевые порты
- **Component tiers (Уровни компонентов)** — Primary (основные) vs Dependency (поддерживающие)

Доступные паттерны

Категория	Примеры
Enterprise (Предприятие)	SAP ERP, Oracle EBS, Microsoft Dynamics
Security (Безопасность)	CyberArk PAM, Active Directory, SIEM
Database (База данных)	Oracle DB, MS SQL Server, PostgreSQL
Monitoring (Мониторинг)	SolarWinds, Prometheus, Nagios
Email	Microsoft Exchange, Postfix
Web	IIS, Apache, Nginx

Запуск Pattern-Based Discovery (Обнаружения на основе паттернов)

Шаг 1: Доступ к **Анализатору бизнес-услуг**
Левая панель → **CMDB** → **Анализатор бизнес-услуг** → **"Проанализировать"**

Шаг 2: Выбор паттерна сервиса
Просмотр библиотеки по категориям → клик по карточке (напр. **"1C"**)

Шаг 3: Проверка критериев обнаружения

Критерий	Примеры
Processes (Процессы)	disp+work, sapwebdisp, jstart.exe
Software (ПО)	Установленные приложения сервиса
Ports (Порты)	Сетевые порты сервиса

Модифицируйте критерии под вашу среду при необходимости.

Шаг 4: Запуск Discovery (Обнаружения)
"Proceed to Discovery" → 2 фазы:

1. **Primary Discovery (Обнаружение основных)** — поиск основных компонентов
2. **Dependency Discovery (Обнаружение поддерживающих)** — связанные инфраструктурные компоненты

Результаты обнаружения

Метрика	Пример
Servers (Серверы)	11/11 выбранных
Connections (Соединения)	34 соединения
Processes (Процессы)	21 процесс
Software (ПО)	16 пакетов
Ports (Порты)	10 портов

Классификация серверов

Колонка	Описание
Hostname (Имя хоста)	Имя сервера (SOLMAN01, WEBDISP01)
Tier (Уровень)	**Primary (Основной)** (синий) или **Dependency (Поддерживающий)** (оранжевый)
IP Address (IP адрес)	Сетевой адрес
OS (ОС)	Операционная система
Running Processes (Запущенные процессы)	Ключевые процессы

Сопоставление соединений

Колонка	Описание
Source Server	Инициирующий сервер
Source Process	Процесс-инициатор
Target Server	Целевой сервер
Target Process	Целевой процесс
Port (Порт)	Порт
Protocol (Протокол)	TCP/UDP

Советы по выбору

- Деселект сервера → автоудаление его соединений
- Индивидуальный переключатель соединений
- Только выбранное → в финальную визуализацию

"Продолжить с X серверами и Y соединениями" → результаты.

Результаты обнаружения

После выбора инфраструктуры система предоставляет детальный анализ, организованный по вкладкам.

Вкладка Серверы — Классификация по уровням

Серверы организованы по **архитектурным уровням**:

Результаты двухэтапного исследования

Primary Servers (Основные серверы) (Фаза 1): 8 основных компонентов сервиса

Dependency Servers (Поддерживающие серверы) (Фаза 2): 3 поддерживающих сервера

Уровни архитектуры

Уровень	Бейдж	Примеры серверов
Frontend Tier	Синий	**WEBDISP01** (load balancer, sapwebdisp), **GATEWAY01** (Fiori gateway, gwrd.exe)
Application Tier (Уровень приложений)	Зеленый	**DIALOG01**, **SAPPRD01/02/03** (S/4HANA), **SAPBW01** (Analytics), **SAPPI01** (PI/Middleware)
Data Tier (Уровень данных)	Оранжевый	**HANADB01** (primary HANA), **HANADB02** (secondary HANA)
Infrastructure Tier (Уровень инфраструктуры)	Фиолетовый	**SOLMAN01** (Solution Manager)

Каждый сервер показывает:

- **Hostname (Имя хоста)** — имя сервера
- **Role (Роль)** — классификация (балансировщик нагрузки, сервер приложения, база данных)
- **OS (ОС)** — операционная система
- **Key Processes (Ключевые процессы)** — основные процессы
- **Confidence (Уверенность)** — уверенность ИИ в классификации

Insights Tab (Вкладка Insights) — Анализ ИИ

Обзор сервиса

"Умеренно крупное развертывание **SAP ERP** с 11 серверами по традиционной **4-уровневой архитектуре**. **SOLMAN01** — **единственная точка отказа** (38% всех соединений)".

Бизнес-влияние

- **Criticality (Критичность)**: Критичное, Высокое, Среднее, Низкое
- **Affected Users (Затронутые пользователи)**: 500-5000+ пользователей
- **Outage Cost (Стоимость простоя)**: $100K-$1M+ в час
- **Departments (Департаменты)**: Финансы, Поставки, HR, Производство, Продажи

Технический анализ

- **Architecture (Архитектура)**: 4-уровневая структура
- **Redundancy (Резервирование)**: Высокое, Среднее, Низкое, оценка HA
- **Scalability (Масштабирование)**: возможности масштабирования
- **Connection Density (Плотность соединений)**: анализ сетевого трафика

Рекомендации

Срочно

- **Резервирование** для единственной точки отказа
- Документация неизвестных соединений

Высокий приоритет

- Валидация HA базы данных
- Дополнительные **экземпляры веб-диспетчера**
- Стандартизация нестандартных портов

Средний приоритет

- Автоматическое масштабирование серверов приложений
- Агенты сетевого мониторинга
- Оптимизация плотности подключения

Низкий приоритет

- Анализ прямого взаимодействия с сервером приложений

Критические зависимости

- **SOLMAN01** — хаб с 13 соединениями (**единственная точка отказа**)
- Зависимости уровня базы данных
- Требования уровня внешнего интерфейса
- Зависимости службы шлюза

Проблемы безопасности

Уровень	Проблемы
Критический	Неизвестные соединения, несанкционированные пути
Высокий	Отсутствие сегментации сети, нестандартные порты
Средний	Неоднородная компоновка, отсутствие SIEM/IDS
Низкий	Плотность соединений, микросегментация

Узкие места производительности

- **SOLMAN01**: 38% всех соединений
- Узкие места на уровне базы данных
- Перегрузка фронтенда при пиках
- Задержки синхронных RFC

33 ВКЛАДКА VISUALIZATION (ВИЗУАЛИЗАЦИИ)

Вкладка визуализации предоставляет интерактивный граф топологии бизнес-услуги.

Понимание графа

Цвета узлов по уровням

Цвет	Уровень	Примеры серверов
Синий	**Frontend**	**WEBDISP01**, **GATEWAY01**
Зеленый	**Приложение**	**DIALOG01**, **SAPPRD01/02/03**, **SAPBW01**, **SAPPI01**
Оранжевый	**Данные**	**HANADB01**, **HANADB02**
Фиолетовый	**Инфраструктура**	**SOLMAN01**

Линии соединений

- **Стрелки** показывают направление соединения
- **Метки** отображают порты и протоколы (30015/TCP, 8005/TCP)

Легенда (правая панель)

frontend: 2 сервера
приложение: 6 серверов
данные: 2 сервера
инфраструктура: 1 сервер

Управление графом

Панель инструментов:

Инструмент	Функция
Layers (Слои)	Переключение видов
Fit (Соответствовать)	Подогнать под экран
Auto-layout (Авто-раскладка)	Перерасположить узлы
Zoom (Зум)	Масштаб +/-
Center (Центр)	Центрировать граф
Refresh (Обновить)	Сброс вида
Show Processes (Показать процессы)	Показать процессы на соединениях

Взаимодействие с графом

- **Перетащите** узлы для перемещения
- **Нажмите на** узел → детали сервера
- **Наведите на** соединение → детали подключения
- **Колесо мыши** → зум

Сохранение бизнес-услуги

После проверки всех вкладок (Серверы, Соединения, Insights, Визуализация):

"Save as Business Service" (Сохранить как бизнес-услугу) → сохранение в **CMDB** с:

- Все серверы и классификации
- Картирование соединений
- **AI insights**
- Топология визуализации

Сохраненная услуга используется для:

- Мониторинга изменений
- Анализа влияния
- Управления изменениями
- Отчетности по соответствию нормативным требованиям (compliance)

Лучшие практики

Выбор паттерна

- Конкретные паттерны для известных сервисов (**Exchange**, **CyberArk**)
- Клонировать/кастомизировать при необходимости

Проверка результатов

- Верификация **основных серверов**
- Релевантность **поддерживающих серверов**
- Удаление ложных срабатываний (деселект)
- Проверка соединений

Использование Insights

- **Критические/Высокие** рекомендации первыми
- Проблемы безопасности → compliance
- Узкие места → операционная команда