Руководство оператора

Системы управления сетевой инфраструктуры RockITNet

Версия 0.0.1

Листов 24

Москва 2025

Оглавление

1. Глоссарий

Термин	Определение
RockITNet	Платформа для управления сетевой инфраструктурой на базе Netbox с кастомными модулями
Endpoint	Запись, содержащая IP-MAC связь и данные о подключении сетевого узла
Hardening	Процесс приведения конфигураций устройств в соответствие с политиками
Advanced_scan	Метка для устройств, с которых собирается расширенная информация
Hardening Group	Логическая группа устройств для объединения политик по различным признакам
Hardening Policy	Конкретное правило проверки конфигурации с ожидаемым значением
Hardening Severity	Уровень важности нарушения (High/Medium/Low)
Basic_scan	Метка для подсетей, включенных в процедуру автоматического сканирования
CDP Neighbors	Информация о смежных устройствах, полученная по протоколам CDP (Cisco Discovery Protocol)/LLDP (Link Layer Discovery Protocol)
Config Backup	Версионная копия конфигурации сетевого устройства
Apply Policy	Запуск проверки соответствия устройств политикам безопасности
Update Endpoints	Принудительное обновление данных о сетевых конечных точках

Термин	Определение
Prefix	IP-подсеть с маской (например, 192.168.1.0/24)
Site	Физическая локация размещения оборудования (дата-центр, офис)

2. Введение

RockITNet - система управления сетевой инфраструктурой, позволяющая выполнять автоматическое сканирование и сбор данных о сетевом оборудовании в мультивендорной сети, сбор конфигурации оборудования и отслеживание истории изменения, проверку конфигурации на соответствие необходимым настройкам и требованиям ИБ, определение точек подключения конечных устройств и историю их состояния, а также анализ состояния сетевых протоколов.

Ключевые функции RockITNet:

Инвентаризация оборудования: Система позволяет вести учет всех сетевых устройств, фиксируя их характеристики, местоположение и статус. Это обеспечивает полную прозрачность и контроль над используемым оборудованием.

Сбор конфигураций устройств: RockITNet автоматически собирает и сохраняет конфигурационные файлы сетевых устройств, позволяя отслеживать изменения, анализировать настройки и восстанавливать предыдущие конфигурации при необходимости.

Целевая аудитория:

Данная инструкция предназначена пользователей и инженеров первого и второго уровня технической поддержки сетевой инфраструктуры. Предполагается, что пользователи обладают базовыми знаниями в области сетевых технологий.

3. Управление сетевыми объектами

3.1 Описание раздела Site (Локации) в RockITNet

3.1.1 Назначение

Локация (Site) в RockITNet представляет собой физическое или логическое местоположение, такое как дата-центр, офис или площадка. Добавление локации позволяет структурировать сетевую инфраструктуру и упрощает управление оборудованием.

Основные функции:

- Организация оборудования по географическому или структурному признаку
- Фильтрация устройств и префиксов
- Группировка данных для отчетов

3.1.2 Описание атрибутов раздела Site

- Раздел Site
    - Name - уникальное название локации (например, "Центральный офис")
    - Slug - автоматически генерируемый идентификатор (можно редактировать)
    - Status:
        - Active (активная)
        - Planned (запланированная)
        - Retired (неактивная)
    - Region - географический регион (например, "Центральный")
    - Group - группа для логической группировки (например, "Офисы")

    - Facility - конкретное помещение (например, "Серверная 2")
    - ASNs - номера автономных систем через запятую
    - Timezone - часовой пояс локации
    - Description - дополнительное описание
    - Tags - метки для категоризации
- Раздел Tenancy
    - Tenant Group - группа арендаторов (например, "Франшизы")
    - Tenant - конкретный арендатор (например, "ООО Луг")
- Раздел Contact Info
    - Physical address - фактический адрес расположения
    - Shipping address - адрес для доставки (если отличается)
    - Latitude/Longitude - географические координаты
- Раздел Custom Fields
    - Произвольные дополнительные поля (зависит от настроек системы)

3.1.3 Пример

Поле	**Пример**
Name	ЦОД-Москва
Slug	dc-moscow
Status	Active
Region	CFO
Group	ЦОД

Поле	Пример
Facility	Зал 23
ASNs	12345, 54321
Timezone	Europe/Moscow
Description	Основной ЦОД
Tags	critical, tier-3
Tenant Group	Корпоративные клиенты
Tenant	ООО Луга
Physical address	г.Москва, ул. Ленина д.1
Shipping address	г.Москва, ул. Ленина д.1
Latitude	55.7558
Longitude	37.6176
Custom Fields	Уровень: High

3.2 Описание раздела Prefix (IP-подсети) в RockITNet

3.2.1 Назначение

Префикс (Prefix) в RockITNet представляет собой диапазон IP-адресов, определяемый в формате CIDR (например, 192.168.1.0/24). Добавление подсети позволяет структурировать IP-адресное пространство, управлять распределением адресов, а также связывать подсети с определенными локациями, арендаторами, VLAN и виртуальными маршрутизируемыми экземплярами (VRF).

3.2.2 Описание атрибутов раздела Prefix

- Раздел Prefix
    - Prefix: IP-подсеть с маской (например, "192.168.1.0/24")
    - Status:
        - Active - активная подсеть
        - Reserved - зарезервированная
        - Deprecated – неиспользуемая
    - Tags: Метки для фильтрации – заполнить basic_scan
    - VRF: Виртуальная маршрутизация (если используется)
    - Role: Назначение подсети (Client/Server/Infrastructure)
    - Is a pool: Отметьте для пулов адресов (Да/Нет)
    - Mark utilized: Автоматическое отслеживание использованных IP
    - Description: Описание

- Раздел Site/VLAN Assignment
    - Site: Привязка к локации, созданной на предыдущем шаге.
    - VLAN: Связанный VLAN (по имени или ID)
- Раздел Tenancy
    - Tenant Group: Группа арендаторов
    - Tenant: Конкретный арендатор

3.2.3 Пример

Поле	**Значение**
Prefix	192.168.10.0/24

Поле	Значение
Status	Active
VRF	MPLS-BACKBONE
Role	Infrastructure
Is a pool	Нет
Mark utilized	Да
Site	ЦОД-Москва
VLAN	Servers-VLAN (ID: 200)
Tenant Group	Providers
Tenant	DataLine
Description	Ядро сети
Tags	basic_scan
Comments	Сеть управления

3.3 Сканирование подсетей

Функция Basic Scan в системе RockITNet позволяет автоматически обнаруживать сетевые устройства в пределах IP-подсетей, помеченных тегом basic_scan. Процесс сканирования осуществляется автоматически после прохождения авторизации.

3.3.1 Предварительные требования.

- Убедитесь, что префиксы, которые необходимо

просканировать, помечены тегом basic_scan.

- Сервер RockITNet должен иметь сетевой доступ к IP-адресам в пределах указанных префиксов для успешного выполнения сканирования.
- Настроены учетные данные для доступа к устройствам: необходимо обеспечить возможность подключения к устройствам по протоколам управления, таким как Telnet, SSH, SNMP

3.3.2 Шаги выполнения Basic Scan для всех Prefix

Шаг 1: Переход к разделу устройств

- В главном меню выберите Devices - Devices.
- Нажмите кнопку "Basic Scan" в верхней части страницы.

Шаг 2: Подтверждение запуска

- После нажатия кнопки откроется окно подтверждения. Введите необходимые учетные данные для подтверждения прав на выполнение сканирования.
- После успешного подтверждения, повторно нажмите на кнопку "Basic Scan". Процесс сканирования начинается автоматически. Система просканирует все префиксы, помеченные тегом basic_scan.

Шаг 3: Ожидание завершения сканирования

- Процесс сканирования может занять некоторое время в зависимости от количества префиксов и их размера.

Шаг 4: Просмотр результатов

- По завершении сканирования, найденные устройства будут автоматически добавлены в систему или обновлены в соответствии с полученной информацией.

3.3.3 Шаги выполнения Basic Scan для определенного Site

Шаг 1: Переход к разделу устройств

- В главном меню выберите Organization - Sites.
- В списке выберите нужный Site.
- Нажмите кнопку "Basic Scan" в верхней части страницы.

Шаг 2: Прохождение авторизации

- После нажатия кнопки откроется окно авторизации. Введите необходимые учетные данные для подтверждения прав на выполнение сканирования.
- После успешной авторизации процесс сканирования начинается автоматически. Система просканирует все префиксы, помеченные тегом basic_scan.

Шаг 3: Ожидание завершения сканирования

- Процесс сканирования может занять некоторое время в зависимости от количества префиксов и их размера.

Шаг 4: Просмотр результатов

- По завершении сканирования найденные устройства будут автоматически добавлены в систему или обновлены в соответствии с полученной информацией.

3.4 Сбор параметров и управление конфигурациями устройств

Тег advanced_scan позволяет инициировать углубленное сканирование устройств, обнаруженных в процессе базового сканирования. Расширенное сканирование собирает дополнительную информацию, такую как конфигурационные файлы, версии программного обеспечения, настройки интерфейсов и другие параметры, что способствует более детальной инвентаризации сетевой инфраструктуры.

3.4.1 Предварительные требования

Перед выполнением расширенного сканирования убедитесь в

следующем:

- Устройства имеют тег advanced_scan: только устройства с этим тегом будут включены в процесс расширенного сканирования.
- Настроены учетные данные для доступа к устройствам: необходимо обеспечить возможность подключения к устройствам по протоколам управления, таким как SSH или SNMP.
- Сервер RockITNet имеет сетевой доступ к устройствам: для успешного сбора информации сервер должен иметь возможность установить соединение с целевыми устройствами.

3.4.2 Процесс выполнения расширенного сканирования для всех устройств

Шаг 1: Переход к разделу устройств

- Перейдите в раздел Devices.
- Выберите одно или несколько устройств, для которых необходимо выполнить расширенное сканирование.
- В разделе Tags добавьте тег advanced_scan.

Шаг 2: Запуск расширенного сканирования

- В главном меню выберите Devices.
- Нажмите кнопку "Advanced Scan" в верхней части страницы.
- Система автоматически инициирует процесс сканирования для всех устройств, помеченных тегом advanced_scan.

Ожидание завершения сканирования

- Процесс может занять некоторое время в зависимости от количества устройств и объема собираемой информации.

Шаг 3: Просмотр результатов

- По завершении сканирования результаты будут доступны в карточках соответствующих устройств.
- Дополнительная информация, такая как конфигурационные

файлы и параметры устройств, будет отображена в соответствующих разделах.

3.4.3 Процесс выполнения расширенного сканирования для Site

Шаг 1: Переход к разделу устройств

- Перейдите в раздел Devices.
- Выберите устройство, для которого необходимо выполнить расширенное сканирование.
- В разделе Tags добавьте тег advanced_scan.

Шаг 2: Запуск расширенного сканирования

- В главном меню выберите Organization - Sites.
- В списке выберите нужный Site.
- Нажмите кнопку "Advanced Scan" в верхней части страницы.
- Система автоматически инициирует процесс сканирования для всех устройств, помеченных тегом advanced_scan.

Ожидание завершения сканирования

- Процесс может занять некоторое время в зависимости от количества устройств и объема собираемой информации.

Шаг 3: Просмотр результатов

- По завершении сканирования результаты будут доступны в карточках соответствующих устройств.
- Дополнительная информация, такая как конфигурационные файлы и параметры устройств, будет отображена в соответствующих разделах.

3.4.4 Работа с файлами конфигурации

Система RockITNet предоставляет инструменты для:

- Автоматического сбора конфигураций сетевых устройств
- Хранения исторических версий конфигураций

- Анализа изменений между различными версиями конфигураций

Просмотр конфигураций устройства

Шаг 1: Работа с файлами конфигураций

- Перейти в раздел Devices главного меню и выбрать пункт Devices
- Выбрать целевое устройство из списка
- Открыть вкладку Config
- Если в системе сохранена единственная версия конфигурации, будет отображена она. В случае наличия нескольких версий необходимо выбрать требуемые для просмотра и сравнения.

Шаг 3: Сравнение версий конфигураций

- В карточке устройства перейти во вкладку Config
- Заполнить выпадающие меню Select old version и Select current version, выбрав нужные версии для сравнения.
- Различия конфигурации будут подсвечены цветом.

3.5 Просмотр информации о CDP-соседях в системе RockITNet

Система RockITNet предоставляет возможность отображения информации о соседних устройствах, обнаруженных по протоколам CDP (Cisco Discovery Protocol) и LLDP (Link Layer Discovery Protocol). Данная функция позволяет администраторам получать актуальные данные о топологии сети и взаимосвязях между устройствами.

Протоколы CDP и LLDP используется для:

- Идентификации смежных устройств
- Контроля корректности подключений
- Устранения неисправностей соединений

3.5.1 Предварительные требования

Перед просмотром информации о CDP-соседях необходимо убедиться в следующем:

- Устройства в сети поддерживают и имеют протоколы CDP/LLDP активированы.

3.5.2 Процесс просмотра информации о CDP-соседях

Для просмотра общей таблицы CDP выполните следующие шаги:

Шаг 1: Авторизация в системе

- Войдите в веб-интерфейс RockITNet с учетной записью, обладающей необходимыми правами доступа.

Шаг 2: Переход к разделу устройств

- В главном меню выберите раздел "CDP Neighbors" и откройте список всех зарегистрированных устройств.

Шаг 3: Отображается таблица информации о соседних устройствах, включая:

- Local Device
- Local port
- Neighbor name
- Neighbor port
- Neighbor ip

Для просмотра информации о CDP-соседях для определенного устройства в системе RockITNet выполните следующие шаги

Шаг 1: Авторизация в системе

- Войдите в веб-интерфейс RockITNet с учетной записью, обладающей необходимыми правами доступа.

Шаг 2: Переход к разделу устройств

- В главном меню выберите раздел "Devices" (Устройства) и откройте список всех зарегистрированных устройств.

Шаг 3: Выбор интересующего устройств

- Найдите и выберите устройство, для которого необходимо просмотреть информацию о CDP-соседях.

Шаг 4: Просмотр интерфейсов устройства

- На странице устройства перейдите к разделу "CDP Neighbors", где отображаются все соседи данного устройства.

Шаг 5: Отображается информация о соседних устройствах, включая:

- Local Device
- Local port
- Neighbor name
- Neighbor port
- Neighbor ip

3.5.3 Процесс обновления информации о CDP-соседях

Для получения актуальных данных о CDP-соседях необходимо инициировать процесс опроса. Данную операцию можно сделать вручную:

Нажмите кнопку "Update list of neighbors" на вкладке CDP Neighbors, или во вкладке CDP Neighbor определенного устройства, для которого необходимо провести обновление информации.

После нажатия система выполнит подключение к устройствам(-у), соберёт информацию с о протоколах CDP/LLDP и обновит отображаемую таблицу. Процедура может занять несколько секунд, в зависимости от отклика устройства и текущей нагрузки на систему.

3.6 Работа с оконечными устройствами (Endpoints)

3.6.1 Назначение модуля Endpoints

Модуль Endpoints выполняет сбор и анализ таблиц коммутации и

ARP-записей с сетевых устройств, для решения задач:

- Учета всех IP-MAC связей в сети
- Контроля подключенных устройств
- Обнаружения новых оконечных сетевых устройств

3.6.2 Просмотр списка Endpoints

В главном меню выбрать перейти в раздел "Endpoints". Система отобразит таблицу всех зарегистрированных конечных точек.

3.6.3 Просмотр истории подключений Endpoint по IP-адресу

Раздел IP Address → Endpoints позволяет:

- Отслеживать историю подключений устройства
- Выявлять несанкционированные перемещения

Шаг 1: Навигация по IP-адресу

- В главном меню выбрать IPAM → IP Addresses (или перейти из вкладки по IP адресу)
- В строке поиска ввести целевой IP-адрес
- Выбрать нужную запись из результатов

Шаг 2: Просмотр истории Endpoint

- В карточке IP-адреса открыть вкладку “Endpoints”
- Система отобразит таблицу с историей зафиксированных точек подключений, определенных во время сканирования

3.6.4 Обновление информации о Endpoints

Глобальное обновление информации об оконечных устройствах

Шаг 1: Переход к разделу оконечные устройства (Endpoints)

- Перейдите в главном меню системы в раздел "Endpoints".

Шаг 2: Запуск сбора данных

- Нажмите кнопку "Update endpoints info" в правой верхней части страницы.

Ожидание завершения сбора информации

- Процесс может занять некоторое время в зависимости от количества устройств и объема собираемой информации.

Шаг 3: Просмотр результатов

- По завершении сбора и анализа полученных данных, в итоговой таблице отобразятся новые данные.

Обновление информации об оконечных устройствах для Site

Шаг 1: Запуск сбора информации

- В главном меню выберите Organization - Sites.
- В списке выберите нужный Site.
- Нажмите кнопку "Update Endpoints" в верхней части страницы.
- Система автоматически инициирует процесс сбора информации и анализа данных.

Ожидание завершения сбора информации

- Процесс может занять некоторое время в зависимости от количества устройств и объема собираемой информации.

Шаг 3: Просмотр результатов

- По завершении сбора и анализа полученных данных, в итоговой таблице Endpoints отобразятся новые данные.

3.7 Управление политиками конфигураций (hardening) в RockITNet

3.7.1 Назначение модуля Hardening

Модуль Hardening обеспечивает централизованное управление стандартами конфигурации, автоматическую проверку соответствия устройств, выявление уязвимых конфигураций.

3.7.2 Hardening Group (Группы политик)

Функционал Hardening groups позволяет объединять различные политики в системе по общим признакам. Например, в группу "Password rules" входят политики проверки настроек паролей.

Для просмотра существующих групп перейдите в раздел Hardening главного меню и выберите меню Hardening Groups.

3.7.3 Hardening Severity (Уровни критичности политик)

Раздел Hardening Severity определяет уровни критичности политик, позволяя администратору и пользователям оценить степень важности и потенциальное влияние каждой политики.

Существующие уровни расположены в меню Hardening Severity раздела Hardening. В системе преднастроены следующие уровни:

Уровень	Описание
High	Нарушение политики представляет угрозу безопасности или работоспособности сети.
Medium	Нарушение политики может создать уязвимость или привести к сбоям, но не представляет прямой угрозы в текущий

Уровень	Описание
	момент.
Low	Нарушение политики незначительно влияет на безопасность или производительность сети.

3.7.4 Hardening Policies (Политики безопасности)

Данный раздел содержит перечень политик, предназначенных для верификации корректности конфигураций сетевых устройств. Каждая политика представляет собой формализованное правило, определяющее требования к настройке и эксплуатации оборудования в соответствии с утвержденными стандартами.

Каждая политика имеет следующие атрибуты:

- Group – группа, в которую входит политика
- Severity – уровень критичности
- Platform – платформа (тип устройства), к которому применяется политика
- Policy rule – правило, по которому проверяется конфигурация устройства
- Policy name – имя политики
- Description – описание политики

3.7.5 Hardening Results (Результаты проверок)

Меню 'Hardening Results' содержит сводные данные о результатах автоматизированной проверки конфигураций всех сетевых устройств установленным политикам.

Для получения информации о соответствии конфигурации конкретного сетевого устройства установленным политикам безопасности следует обратиться к вкладке 'Hardening Result' на странице данного устройства в

системе.

3.7.6 Запуск проверки

Для запуска анализа нажмите на кнопку "Apply policies" в меню "Hardening result".