Пользователи и роли

4. Управление доступом к веб-интерфейсу

Примечание

Ниже перечислены все возможные пункты меню. Наличие конкретных функций зависит от модели решения в составе **НАЙС.ОС Greenbone COMMUNITY EDITION**.

4.1 Пользователи

Веб-интерфейс поддерживает несколько пользователей с ролями и правами. На этапе первичной настройки в системном меню администрирования создаётся первый пользователь — администратор веб/скан-части. Под этой учётной записью выполняется дальнейшее управление пользователями.

Роли

Доступ реализован по ролевой модели: роль определяет, какие разделы интерфейса видны и доступны пользователю (права чтения/записи назначаются отдельно). Предустановлены несколько ролей; администратор может создавать дополнительные. Контроль прав реализован на уровне *Greenbone Management Protocol (GMP)* и распространяется на всех GMP-клиентов.

Группы

Пользователи могут объединяться в группы для логической организации и пакетного назначения прав. Для каждого пользователя задаются диапазоны IP-адресов (разрешённые/запрещённые цели сканирования); также можно ограничивать доступ к интерфейсам решения.

Управление пользователями выполняется целиком на стороне решения. Внешние каталоги как источник пользователей не поддерживаются, но для централизации аутентификации могут использоваться **LDAPS** или **RADIUS** (см. разд. 4.5). В этом случае внешний сервис проверяет пароль, а все остальные настройки ведутся в локальном управлении пользователями.

4.1.1 Создание пользователя

Требование: создавать и управлять пользователями могут только администраторы.

1. Войдите под администратором.
2. Откройте *Administration > Users*.
3. Нажмите *New* в левом верхнем углу.
4. Заполните поля (см. рис. 4.1):

Рис. 4.1 — Создание пользователя

- **Login Name** — обязательное; допустимы алфавитно-цифровые символы, `-`, `_`, `.`. При использовании центрального каталога (см. разд. 4.5) возможны ограничения по длине/символам; имя должно точно совпадать с записью в каталоге.
- **Authentication**:
  - *Password* — локальная аутентификация. Пароль без практического ограничения длины; учитывайте доступность спецсимволов на всех клиентских системах.
  - *LDAP Authentication Only* — проверка пароля через LDAPS.
  - *RADIUS Authentication Only* — проверка пароля через RADIUS.
- **Roles** — одна или несколько ролей. Без роли вход в веб-интерфейс невозможен. Для пользовательских ролей, которые должны иметь доступ к интерфейсу, минимальный набор прав: `authenticate`, `get_settings`, `help`.
- **Groups** — членство в группах.
- **Host Access** — допустимые цели сканирования. Доступны два режима:
  - *Allow all and deny* — по умолчанию разрешено, явный запрет для перечисленных;
  - *Deny all and allow* — по умолчанию запрещено, явное разрешение для перечисленных.

  Рекомендация: используйте модель разрешающих списков (allowlist).

Поддерживаются имена хостов, IPv4/IPv6, диапазоны и CIDR, например:

```
192.168.15.5
192.168.15.5-192.168.15.27
192.168.15.5-27
192.168.15.128/25
2001:db8::1
2001:db8::1-2001:db8::15
2001:db8::1-15
2001:db8::/120
```

По умолчанию маска CIDR ограничена до /20 (IPv4) и /116 (IPv6), исходя из лимита 4096 адресов на цель (для некоторых моделей, например OPENVAS SCAN 6500, лимиты могут быть выше).

Нажмите *Save* — пользователь появится на странице *Users*.

4.1.2 Управление пользователями

Administration > Users (для администратора) — список всех учётных записей.

- **Name** — имя пользователя; глобальные пользователи, созданные через системное меню, помечены значком.
- **Roles**, **Groups**, **Host Access**.
- **Authentication Type** — Local / RADIUS / LDAP.

Действия: удалить (если не super admin и не в активной сессии), редактировать, клонировать, экспортировать в XML. Под списком доступны массовые операции (удаление/экспорт выбранных).

4.1.3 Одновременный вход

Одновременный вход двух разных пользователей допускается. Повторный вход тем же пользователем из того же браузера аннулирует первую сессию; используйте другой браузер/ПК для второй сессии.

4.1.4 Гостевой доступ

Для ограниченного доступа создайте пользователя с ролью *Guest*; по паролю он увидит страницу *Dashboards*. Вариант входа гостя без пароля включается в

системном меню администрирования.

4.2 Роли

Интерфейс позволяет создавать и настраивать собственные роли.
Предустановленные роли:

- **Admin** — все права, включая управление пользователями/ролями/группами.
- **User** — все права, кроме управления пользователями/ролями/группами и синхронизации/управления фидами; раздел *Administration* недоступен.
- **Info** — только чтение VT и SCAP; можно менять личные настройки.
- **Guest** — как *Info*, но без изменения пользовательских настроек.
- **Monitor** — доступ к системным отчётам (см. разд. 16.1).
- **Observer** — чтение без возможности запускать или создавать сканы; видит назначенные ему сканы.
- **Super Admin** — доступ ко всем объектам всех пользователей; настраивается в системном меню, не редактируется из веб-интерфейса.

Только администраторы могут создавать и управлять ролями.

Изменять предустановленные роли нельзя — их можно клонировать и править копии для сохранения предсказуемого поведения при обновлениях.

4.2.1 Клонирование роли

1. Войдите под администратором и откройте *Administration > Roles*.
2. В строке роли нажмите *Clone*, затем в строке клона — *Edit*.
3. Задайте **Name** (см. рис. 4.3), при необходимости добавьте пользователей.
4. Добавьте разрешения: выберите в списке *Name* и нажмите *Create Permission*. Для «супер-разрешений» — выберите группу в *Group*.
5. Сохраните.

Рис. 4.3 — Редактирование клонированной роли

4.2.2 Создание роли

1. *Administration > Roles* *New*.
2. Опишите роль: **Name** (до 80 символов), **Comment** (опц.), **Users** (или назначьте роль из профиля пользователя).
3. Сохраните и откройте *Edit* в строке роли.
4. Добавьте разрешения. Минимум для доступа к веб-интерфейсу: `authenticate`, `get_settings`, `help`. Разрешение `write_settings` позволяет менять пароль/часовой пояс и т. п.
5. При необходимости добавьте «супер-разрешение» для группы и сохраните.

4.2.3 Управление ролями

Список ролей: *Administration > Roles*. Действия: переместить в корзину/редактировать (только собственные), клонировать, экспорт в XML. Массовые операции — под списком.

Детали роли: вкладки *Information*, *General Command Permissions* (список команд GMP), *User Tags*, *Permissions*.

4.2.4 Назначение ролей пользователю

Ролей может быть несколько; права суммируются. Назначение при создании пользователя (см. рис. 4.4) или при редактировании.

Рис. 4.4 — Создание пользователя с несколькими ролями

4.2.5 Создание супер-администратора

Роль **Super Admin** — наивысший уровень доступа, снимает ограничения прав и позволяет просматривать/редактировать любые объекты. Создаётся в системном меню администрирования. Изменять её может только супер-администратор.

4.3 Группы

Группы служат для логического объединения пользователей. Число групп не ограничено. Права могут назначаться на группу (см. разд. 4.4). По умолчанию группы не заданы.

4.3.1 Создание группы

Требование: создавать и управлять группами могут только администраторы.

1. *Administration > Groups* *New*.
2. Заполните (см. рис. 4.5): **Name** (до 80 символов), **Comment** (опц.), **Users** (члены), **Special Groups** (общий rw-доступ ко всем ресурсам группы).
3. *Save*.

Рис. 4.5 — Создание группы

4.3.2 Управление группами

Administration > Groups — список и действия: корзина, редактирование, клонирование, экспорт XML; массовые — под списком. Детали: *Information*, *User Tags*, *Permissions*.

4.4 Разрешения (Permissions)

Administration > Permissions — полный перечень назначенных разрешений. Разрешение относится к одному субъекту: *User*, *Role* или *Group*.

Типы разрешений

- **Command permissions** — привязаны к командам GMP:
  - *Command level* — без указания ресурса; позволяет выполнять команду в целом;
  - *Resource level* — с указанием ресурса; позволяет выполнять команду над конкретным объектом.

- **Super permissions** — см. разд. 4.4.2.

4.4.1 Создание и управление разрешениями

Обычно права назначаются через роли (см. разд. 4.2). Прямое управление на странице *Permissions* — для опытных администраторов.

4.4.1.1 Создание разрешения

1. *Administration > Permissions* *New*.
2. Опишите разрешение (см. рис. 4.6): **Name**, **Comment**, **Subject** (user/role/group).
3. Для «Super (Has super access)» укажите **Resource Type** и ID субъекта.
4. *Save*.

Рис. 4.6 — Создание разрешения

4.4.1.2 Создание с страницы объекта

1. Откройте детали ресурса (например, *Scans > Tasks* имя задачи *Details*).
2. Вкладка *Permissions* *New* (см. рис. 4.7) задайте право и сохраните.

Рис. 4.7 — Права с страницы объекта

Доступные типы: **read** (просмотр), **write** (просмотр+изменение без удаления). Для некоторых ресурсов *write* добавляет сопутствующие права автоматически (например, `start_task/stop_task/resume_task` для задач; `test_alert` для оповещений; `verify_*` для форматов отчётов и сканеров). Можно распространить права на связанные ресурсы (targets credentials/port list и т. п.).

4.4.1.3 Просмотр и массовые операции

Список разрешений показывает: *Name*, *Description*, *Resource Type*, *Resource*, *Subject Type*, *Subject*. Действия: корзина/редактирование/клонирование/экспорт (для собственных). Массовые — под списком.

4.4.2 Супер-разрешения

Любой объект (пользователь, задача, цель и т. д.) либо глобальный, либо принадлежит пользователю. Чтобы не раздавать множество отдельных прав, можно назначать «супер-разрешения», открывающие доступ ко всем объектам выбранного пользователя/роли/группы или (для супер-администратора) — ко всем объектам.

«Any» недоступно для явной установки и применяется только к супер-администратору.

1. Откройте нужный субъект (*Users/Roles/Groups*) и его *Details* — в правом верхнем углу указан ID (см. рис. 4.8).

Рис*. 4.8 — ID* ресурса

2. *Administration > Permissions* *New* **Name**: *Super (Has super access)* (см. рис. 4.9).
3. Выберите субъект, тип ресурса и введите ID. Сохраните.

Рис. 4.9 — Создание супер-разрешения

Супер-разрешения удобно назначать на группы — все участники получают доступ к объектам, созданным другими участниками группы.

4.4.3 Предоставление прав чтения другим пользователям

4.4.3.1 Требования

Пользователь может делиться собственными ресурсами, если у него есть глобальное право `get_users` и «конкретное» `get_users` на того пользователя, кому предоставляется доступ.

Для администраторов

Глобальное `get_users` у администратора есть по умолчанию. Конкретное право он получает, если:

- сам создал нужную учётную запись; или
- получил его от супер-администратора через вкладку *Permissions* в деталях целевой учётной записи (см. рис. 4.10–4.11).

Рис. 4.10 — Конкретное `get_users` для администратора

Рис. 4.11 — Пример назначенного права

Для обычных пользователей

1. Администратор создаёт роль, например *GrantReadPriv*, добавляет ей право `get_users` (см. рис. 4.12) и назначает роль пользователю.

Рис. 4.12 — Добавление `get_users` роли

2. Супер-администратор выдаёт этому пользователю «конкретное» `get_users` на целевую учётную запись через вкладку *Permissions* (см. рис. 4.13–4.14).

Рис. 4.13 — Конкретное право пользователю

Рис. 4.14 — Просмотр назначенного права

4.4.3.2 Предоставление доступа на чтение

1. Откройте страницу нужного объекта и перейдите в его *Details* — скопируйте ID (см. рис. 4.15).

Рис. *4.15 — ID* объекта

2. *Administration > Permissions* *New* в **Name** выберите право для типа объекта:

```
Filters — get_filters
Scan configuration — get_configs
Alert — get_alerts
Note — get_notes
Override — get_overrides
Tag — get_tags
Target — get_targets
Task (с отчётом) — get_tasks
Schedule — get_schedules
```

3. Выберите *User*, укажите пользователя и вставьте ID. Сохраните (см. рис. 4.16).

Рис. 4.16 — Предоставление доступа к объекту

По аналогии можно делиться объектами с ролями или группами — потребуется глобальное и «конкретное» `get_roles`/`get_groups`. Исключение: предустановленные роли уже имеют «конкретное» `get_roles`.

4.5 Центральная аутентификация пользователей

Для синхронизации паролей и снижения нагрузки на сервис-деск решение поддерживает аутентификацию через **LDAPS** или **RADIUS**. Внешний сервис используется только для проверки пароля; учётные записи должны существовать локально и иметь те же имена, что и в каталоге/на RADIUS-сервере.

4.5.1 LDAPS

Поддерживаются STARTTLS (порт 389) и LDAPS (порт 636). Необходима работа по SSL/TLS и доверие к сертификату сервера.

4.5.1.1 Загрузка сертификата удостоверяющего центра

Для проверки сервера загрузите сертификат выпускавшего ЦС в формате Base64 (обычно `.pem`, начинается с `-----BEGIN CERTIFICATE-----`). Для промежуточных ЦС импортируйте цепочку (Issuing CA + Root CA). Примеры расположений:

- **UCS**: `/etc/univention/ssl/ucsCA/CAcert.pem`.
- **Active Directory**: экспортируйте сертификат ЦС через консоль ЦС (см. документацию Microsoft) и загрузите его при настройке LDAPS.

4.5.1.2 Подключение к дереву LDAPS

1. *Administration > LDAP* *Edit* включить *Enable* (см. рис. 4.17).

Рис. 4.17 — Настройка *LDAPS*

2. Указать **LDAP Host** (имя/IP) и загрузить доверенный сертификат сервера.
3. Задать **Auth. DN** — DN с подстановкой `%s` для имени пользователя. Примеры:

```
cn=%s,ou=people,dc=domain,dc=de
uid=%s,ou=people,dc=domain,dc=de
%s@domain.de
domain.de\%s
```

4. Опционально включить **Use LDAPS only** (запрет STARTTLS и plain-LDAP).
5. *OK* — при включённом LDAPS становится доступен режим *LDAP Authentication Only* для пользователей (см. рис. 4.18–4.19).

Рис*. 4.18 — LDAPS* включён

Рис. 4.19 — Аутентификация через *LDAPS*

Учетная запись должна существовать в LDAPS под тем же именем. Если CN в сертификате сервера не совпадает с указанным *LDAP Host*, подключение будет отклонено.

4.5.2 RADIUS

1. *Administration > Radius* *Edit* включить *Enable*.
2. Указать **RADIUS Host** и общий секрет (**Secret Key**) (см. рис. 4.20).

3. *OK* — становится доступен режим *RADIUS Authentication Only* для пользователей (см. рис. 4.21).

Рис. 4.20 — Конфигурация *RADIUS*

Рис. 4.21 — Аутентификация через *RADIUS*