11. ПОДГОТОВКА АГЕНТА ДЛЯ АВТОМАТИЧЕСКОГО СКАНИРОВАНИЯ СЕТИ

Сканирование сети выполняется для получения списка устройств с их IP-адресами для топологии сети, чтобы не создавать устройства вручную. Агентом для сканирования сети может быть любой сервер, виртуальная машина, зонд или иное устройство, работающее под управлением Unix-совместимой операционной системы, на которое можно установить пакеты, которые обеспечат сканирование. Устройство должно иметь возможность приёма команд с удалённого сервера по протоколу SSH.

Для работы функции сканирования требуется обеспечить запуск следующих утилит:

- zmap (https://github.com/zmap/zmap, требует отдельной загрузки и установки, на Red Hat-подобных ОС входит в состав EPEL – epel-release). Получает список IP-адресов;
- arp (в составе пакета net-tools, обычно входит в состав дистрибутива ОС). Позволяет сопоставить списку IP-адресов MAC-адреса;
- nmblookup (в составе пакета samba4-client, обычно входит в состав дистрибутива ОС). Получает сетевые идентификаторы NetBIOS.

Установка проводится в соответствии с руководством администратора соответствующей операционной системы.

Задания на сканирование подсетей поступают с сервера приложений wiSLA на агент в виде команд по протоколу SSH, выполняются с sudo и требуют привилегий администратора. Пользователь, под которым будет происходить подключение для запуска сканирования, должен входить в sudoers и иметь возможность выполнения команд с повышенными привилегиями без ввода пароля.

После установки требуется настроить утилиту zmap. Обычно по умолчанию в ней отключено сканирование локальных подсетей. Для включения достаточно найти файл настроек zmap (как правило, это /etc/zmap/blacklist.conf), закомментировать строки, по которым планируется сканирование или добавить собственные правила. В случае проблем с установкой или настройкой zmap обратитесь в
службу технической поддержки.

В сети может работать несколько таких агентов. Администратор может проводить сканирование, последовательно меняя настройки сканирования на портале оператора в разделе «Топология сети».