Документ 2. Инструкция по установке и развертыванию программного комплекса ESLS (On-premise)

Настоящее руководство содержит описание процедуры развертывания, первоначальной настройки и проверки работоспособности серверных компонентов программного комплекса ESLS в инфраструктуре Заказчика с использованием готовых образов виртуальных машин.

1. Минимальные системные требования и предварительные условия

1.1. Аппаратные требования

Развертывание компонентов программного комплекса осуществляется на базе виртуальных или физических серверов со следующими минимальными аппаратными характеристиками в зависимости от роли сервера. Для всех типов серверов крайне рекомендуется использование твердотельных накопителей (SSD) для обеспечения стабильной производительности систем хранения и баз данных.

Роль сервера	Процессор	Оперативная память (RAM)	Дисковое пространство
Центральный сервер ядра (ESLS Core)	4 ядра (архитектура x86_64)	8 ГБ	50 ГБ (желательно SSD)
Сервер магазина (ESLS Shop)	4 ядра (архитектура x86_64)	4 ГБ	50 ГБ (желательно SSD)

1.2. Требования к среде виртуализации

Развертывание осуществляется в корпоративных средах виртуализации (KVM, VMware vSphere, Microsoft Hyper-V, Proxmox VE и др.). Архитектура предоставляемых образов оптимизирована под целевую платформу виртуализации Заказчика.

1.3. Сетевые требования

- **Сетевой адрес:** Статический IP-адрес (рекомендуется) или резервирование адреса на DHCP-сервере.
- **Служба DNS:** Обязательно наличие функционирующего DNS-сервера в локальной сети. Доступ к компонентам системы осуществляется исключительно по доменным именам (FQDN). IP-адреса для прямой адресации панели управления не используются.
- **Требования к DNS-зоне:** В целевой DNS-зоне организации (например, corp.domain.tld) необходимо настроить wildcard-запись типа A для корректной

маршрутизации запросов к ядру:
*.core.corp.domain.tld. IN A <IP-адрес_виртуальной_машины_Core>
(Где <IP-адрес_виртуальной_машины_Core> — фактический адрес развернутого сервера).

2. Получение дистрибутива

Дистрибутив программного комплекса поставляется в виде подготовленных образов дисков виртуальных машин под соответствующие роли (ESLS Core Image и ESLS Shop Image).

1. 1. Учетные данные (логин и пароль) для доступа к официальному сертифицированному репозиторию необходимо запросить у нас.
2. 2. Авторизуйтесь на портале: https://repo.esls.ru
3. 3. Выберите и загрузите файлы образов (Core и/или Shop), соответствующие используемому в вашей организации гипервизору.

3. Порядок развертывания и базовая настройка

3.1. Импорт образа

Выполните импорт загруженного файла образа виртуального диска (Core или Shop) в среду виртуализации согласно внутренним регламентам администрирования вашей ИТ-инфраструктуры. Запустите виртуальную машину.

3.2. Первичный доступ к консоли

Для первоначального подключения к серверу можно использовать локальную консоль гипервизора, протокол SSH или встроенную веб-панель управления Cockpit.

- **Порт Cockpit (Web-UI):** 9090/tcp
- **Учетные данные по умолчанию (OS):** логин и пароль необходимо запросить у нас.

3.3. Настройка сетевых параметров

По умолчанию сетевой интерфейс виртуальной машины инициализируется в режиме получения адреса по DHCP. Если требуется назначить статические параметры сети вручную, используйте штатные утилиты диспетчера сети (NetworkManager):

```
# Запуск интерактивного интерфейса настройки сети
nmtui
```

Или воспользуйтесь интерфейсом командной строки nmcli для привязки статического IP-адреса, маски подсети, шлюза и локального DNS-сервера.

3.4. Инициализация серверных компонентов

После завершения настройки сети и проверки разрешения доменных имен, выполните подключение к серверу по SSH и запустите специализированный интерактивный скрипт конфигурации:

```
# Переход в режим суперпользователя (root) с загрузкой
окружения
sudo su -l

# Запуск мастера первоначальной настройки системы
esls-server-setup
```

Следуйте указаниям мастера для инициализации системных служб и привязки сервера к вашему внутреннему доменному имени.

4. Проверка работоспособности и первый вход (для сервера Core)

Программный комплекс по умолчанию использует защищенное соединение HTTPS с самоподписанными сертификатами безопасности. Для первичного сопряжения, скачивания корневого сертификата и авторизации в веб-панели управления ценниками строго соблюдайте следующую последовательность действий:

4. **Подтверждение доверия к API:** Откройте веб-браузер и перейдите по адресу: https://api.core.<имя_вашего_домена>. Браузер отобразит предупреждение о недоверенном сертификате. Добавьте данный сертификат в исключения безопасности (подтвердите доверие), чтобы разрешить фоновые запросы к API-серверу.
5. **Скачивание корневого сертификата:** Для настройки доверия на конечных устройствах пользователей или интеграционных шлюзах, корневой сертификат доступен для скачивания после завершения настройки по адресу: https://ca.core.<имя_вашего_домена>/roots.pem
6. **Вход в панель управления:** Перейдите по основному адресу интерфейса управления: https://core.<имя_вашего_домена>
7. **Авторизация в системе:** Для входа используйте встроенную административную учетную запись. Учетные данные (логин и пароль) необходимо запросить у нас.

Важно: Сразу после успешного входа в панель управления рекомендуется изменить пароль учетной записи в разделе настроек профиля безопасности.

5. Подключение периферийных модулей (Серверы магазинов)

При развертывании зависимых серверов магазинов (ESLS Shop) и подключении базовых станций (ESLAP):

- Идентификатор магазина (shop_id) должен строго соответствовать локальному имени хоста (Hostname) целевого сервера магазина. Это необходимо для корректной маршрутизации очередей данных и синхронизации с ERP-системой.
- Порядок авторизации и привязки аппаратных точек доступа регламентируется отдельным эксплуатационным документом «Инструкция по настройке и эксплуатации базовых станций ESLAP».