

Программный комплекс по защите
системно-технической инфраструктуры
«Efros Defence Operations»

Руководство администратора

Аннотация

Данный документ представляет собой руководство администратора для работы с программным комплексом по защите системно-технической инфраструктуры «Efros Defence Operations» (далее – ПК «Efros DO» или комплекс). Руководство содержит сведения, необходимые пользователям для установки и настройки работы комплекса.

Администратор должен знать стандартные программные средства (операционные системы, утилиты, офисные пакеты, антивирусные пакеты), а также обладать общими знаниями по администрированию сетевых устройств.

Содержание

1 Сведения о комплексе, технические и программные средства, обеспечивающие выполнение функций программы	5
1.1 Общие сведения о комплексе	5
1.2 Используемые программные и технические средства	11
2 Общие указания по установке комплекса	22
3 Состав и содержание дистрибутива	23
4 Предварительные настройки	27
4.1 Настройка СУБД	27
4.2 Настройка политик безопасности ОС	29
5 Установка, обновление и удаление комплекса на базе Docker-контейнера	43
5.1 Установка комплекса	43
5.2 Перенастройка сети	48
5.3 Обновление комплекса на базе Docker-контейнера	48
5.4 Удаление изделия	52
6 Установка, обновление и удаление комплекса на базе Kubernetes	56
6.1 Отказоустойчивость и катастрофоустойчивость кластера	56
6.2 Варианты обеспечения отказоустойчивости кластера	57
6.3 Предварительные настройки	59
6.4 Установка комплекса на базе Kubernetes	63
6.5 Обновление сертификатов	71
6.6 Работа с узлами кластера	75
6.7 Размещение гостевого портала в ДМЗ	78
6.8 Остановка и запуск кластера ПК «Efros DO»	79
6.9 Возможные ошибки при работе с кластером и способы их устранения	81
6.10 Дополнительные функциональные возможности кластера	89
6.11 Обновление комплекса на базе Kubernetes	89
6.12 Удаление кластера	97
7 Работа с ПК «Efros DO»	99
7.1 Аутентификация пользователя	99
7.2 Лицензирование	100
7.3 Online активация комплекса	101
7.4 Offline активация комплекса	103
7.5 Реактивация лицензии комплекса	106

7.6	Обновление лицензии комплекса	108
7.7	Удаление лицензии	108
8	Windows-агент ПК «Efros DO»	110
8.1	Установка windows-агента	110
8.2	Настройка параметров службы windows-агента	112
9	Агент ПК «Efros DO»	116
9.1	Установка и удаление агента ПК «Efros DO» (ОС MS Windows)	116
9.2	Установка и удаление агента ПК «Efros DO» (ОС Linux).....	123
9.3	Установка и удаление агента ПК «Efros DO» (ОС macOS)	125
9.4	Модуль «Контроль целостности до загрузки ОС» (ICM).....	126
9.5	Изменение адреса сервера ПК «Efros DO»	128
9.6	Службы и процессы модулей агента	129
9.7	Обновление агента ПК «Efros DO»	132
9.8	Графический интерфейс агента	132
10	Сообщения администратору	133
	Перечень сокращений	134

1 Сведения о комплексе, технические и программные средства, обеспечивающие выполнение функций программы

1.1 Общие сведения о комплексе

ПК «Efros DO» является высокопроизводительным комплексом по защите системно-технической инфраструктуры. Конфигурация ПК «Efros DO» зависит от наличия лицензий на следующие функциональные модули:

- «Efros Network Assurance» («Efros NA»);
- «Efros Firewall Assurance» («Efros FA»);
- «Efros Network Access Control» («Efros NAC»);
- «Efros Integrity Check Compliance» («Efros ICC»);
- «Efros Vulnerability Control» («Efros VC»);
- «Efros Network Flow Analysis» («Efros «NFA»);
- «Efros Change Manager» («Efros CM»);
- «Efros Secure DNS» («Efros SDNS»).

Архитектура комплекса построена на основе микросервисов и модулей платформы «Efros DO» на базе платформы контейнеризации Docker (далее – на базе Docker-контейнера) или на базе инфраструктуры оркестровки контейнеризированных приложений Kubernetes (далее – на базе Kubernetes):

- платформа интеграции – единый интерактивный интерфейс, представляющий полный контроль над автоматизацией процессов информационной безопасности (ИБ);
- подсистема хранения данных (системы управления базами данных (СУБД));
- модуль обмена данными Apache Kafka;
- модуль хранения данных OpenSearch;
- модуль распределенного хранения объектов MinIO;
- функциональные модули – «Efros NA», «Efros FA», «Efros NAC», «Efros ICC», «Efros VC», «Efros «NFA»», «Efros CM», «Efros SDNS»;
- микросервис лицензирования;
- микросервис аутентификации и авторизации;
- микросервис уведомлений и событий;
- микросервис объектов защиты;
- микросервис сбора метрик ИБ;
- микросервис маршрутизации запросов;
- микросервис генерации отчетов;

- микросервис базы знаний;
- микросервис драйверов сканеров уязвимостей;
- микросервис системы заявок;
- микросервис отправки сообщений;
- микросервис расписаний;
- микросервис гостевых порталов;
- микросервис службы DNS;
- микросервис управления службами DNS;
- микросервис обработки событий DNS;
- микросервис поддержки иерархии;
- микросервис управления агентами ПК «Efros DO»;
- микросервис поиска маршрутов для моделирования трафика на карте сети;
- микросервис управления контейнеризацией и кластеризацией;
- микросервис резервного копирования и восстановления;
- микросервис загрузки данных из базы правил межсетевых экранов;
- микросервис миграции данных;
- микросервис интеграции с внешними системами заявок.

Внешние модули, которые предназначены для взаимодействия с оборудованием и программным обеспечением различных производителей, входят в состав комплекса. Модули могут быть установлены автоматически одновременно с установкой сервера ПК «Efros DO» или дополнительно установлены в процессе работы комплекса. Кроме того, пользователи с соответствующими правами имеют возможность добавить пользовательские модули для подключения отдельных типов устройств.

Дополнительно в состав комплекса входят агенты, для установки на контролируемых устройствах:

- 1) Windows-агент – предназначен для обеспечения операций контроля целостности файловых объектов. Устанавливается на электронно-вычислительной машине (ЭВМ) с операционной системой (ОС) MS Windows, подключается к комплексу по сети.
- 2) Агент ПК «Efros DO» – совместно с ПК «Efros DO» позволяет управлять доступом пользователей к корпоративным ресурсам при проводном и беспроводном подключении с учетом состояния защищенности рабочих мест и соответствия принятым в организации требованиям по информационной безопасности.

Необходимым условием работы комплекса является возможность подключения к системам хранения данных. Допускается работа комплекса со встроенной СУБД (поставляется в дистрибутиве) или с подключением к внешней СУБД.

В работе комплекса используются 2 категории систем хранения данных: SQL (встроенная либо внешняя СУБД) и NoSQL (внутренние хранилища данных – OpenSearch, MinIO). СУБД SQL применяется для хранения всех данных, используемых и получаемых комплексом. СУБД NoSQL применяется сервисами аудита для хранения записей аудита, а также хранения данных сетевых потоков, таких как NetFlow.

Упрощенная архитектурная схема сервисов и потоков данных представлена на рис. 1.

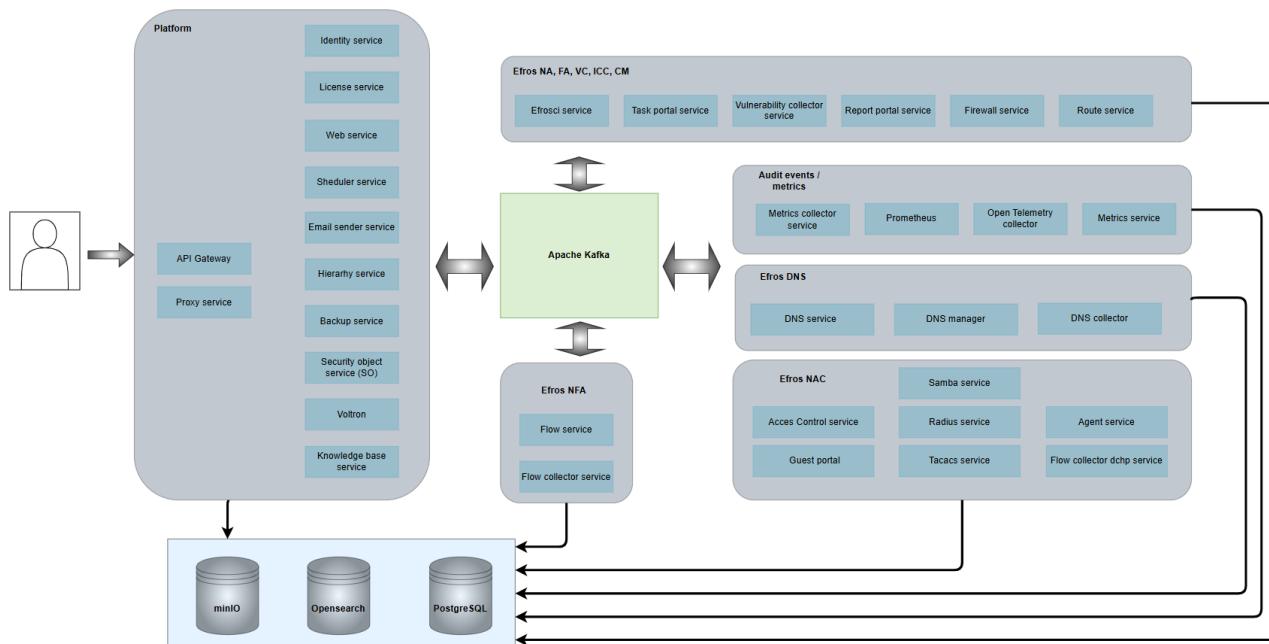


Рисунок 1 – Схема сервисов и потоков данных

Взаимосвязь сервисов в ПК «Efros DO» приведена в таблице 1.

Таблица 1 – Взаимосвязь сервисов в комплексе

Имя сервиса	Описание	Связь с другими сервисами
edo-voltron-service	Микросервис, обеспечивающий проксирование API CI	<ul style="list-style-type: none"> edo-ci-service: 20000/TCP; edo-co-service: 8080/TCP; Postgres DB: 5432/TCP; Apache Kafka service: 9092/TCP; edo-gateway-service: 8080/TCP; edo-identity-service: 8080/TCP
edo-web-service	Микросервис, отвечающий за пользовательский веб-интерфейс	<ul style="list-style-type: none"> edo-gateway-service: 8080/TCP
nginx-controller*	Сервер Nginx, выполняющий шифрование трафика и обратное проксирование на сервис иерархии и агенты	
edo-gateway-service	Микросервис маршрутизации запросов	<ul style="list-style-type: none"> edo-license-service: 8080/TCP; edo-identity-service: 8080/TCP; edo-co-service: 8080/TCP; edo-metrics-service: 8080/TCP;

Имя сервиса	Описание	Связь с другими сервисами
edo-identity-service	Микросервис аутентификации и авторизации пользователей и служб комплекса, а также парольной политики	<ul style="list-style-type: none">• Edo web service: 8080/TCP• Apache Kafka service: 9092/TCP;• edo-gateway-service: 8080/TCP;• Opensearch DB: 9200/TCP
edo-license-service	Микросервис, контролирующий работу выданных лицензий. Связывается с сервером лицензирования для активации и обновления лицензионных	<ul style="list-style-type: none">• edo-identity-service: 8080/TCP;• Postgres DB: 5432/TCP;• edo-gateway-service: 8080/TCP;• Apache Kafka service: 9092/TCP
edo-so-service	Микросервис по работе с объектами защиты (ОЗ)	<ul style="list-style-type: none">• edo-identity-service: 8080/TCP;• Postgres DB: 5432/TCP;• edo-gateway-service: 8080/TCP;• Apache Kafka service: 9092/TCP
edo-acsservice	Микросервис контроля доступа в сеть и к сетевому оборудованию	<ul style="list-style-type: none">• Postgres DB: 5432/TCP;• edo-gateway-service: 8080/TCP;• efros-otel-collector: 4317/TCP;• Apache Kafka service: 9092/TCP
edo-radius	RADIUS-сервер	<ul style="list-style-type: none">• edo-gateway-service: 8080/TCP;• edo-acsservice: 5000/TCP
edo-tacacs	TACACS+ сервер	<ul style="list-style-type: none">• edo-gateway-service: 8080/TCP;• edo-acsservice: 5000/TCP
edo-guest-portal-service	Микросервис, обеспечивающий работу гостевых порталов	<ul style="list-style-type: none">• edo-gateway-service: 8080/TCP;• Postgres DB: 5432/TCP
domain-service- <суффикс домена>	SMB-сервер	<ul style="list-style-type: none">• edo-acsservice: 5000/TCP
edo-ci-service	Микросервис управления и загрузки конфигураций, контроля сетевых устройств и других объектов сетевой инфраструктуры	<ul style="list-style-type: none">• Postgres DB: 5432/TCP;• efros-otel-collector: 4317/TCP;• Opensearch DB: 9200,9300/TCP
edo-email-sender- service	Микросервис по отправке почтовых уведомлений	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• Postgres DB: 5432/TCP
edo-vulnerability- collector	Микросервис драйверов сканеров уязвимостей	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• edo-gateway-service: 8080/TCP;• Postgres DB: 5432/TCP
edo-knowledge-base- service	Микросервис базы знаний	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• Postgres DB: 5432/TCP
edo-agent-service	Микросервис, обеспечивающий управление и взаимодействие с агентами ПК «Efros DO»	<ul style="list-style-type: none">• edo-gateway-service: 8080/TCP;• Apache Kafka service: 9092/TCP
edo-flow-collector	Микросервис сбора данных сетевой активности с сетевых устройств по протоколу NetFlow	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• edo-flow-service: 8080/TCP;• edo-gateway-service: 8080/TCP;

Имя сервиса	Описание	Связь с другими сервисами
edo-flow-collector-dhcp	Микросервис, обеспечивающий профилирование конечных точек по протоколу DHCP	<ul style="list-style-type: none">• Opensearch DB: 9200,9300/TCP• Apache Kafka service: 9092/TCP;• edo-flow-service: 8080/TCP;• Opensearch DB: 9200,9300/TCP
edo-flow-collector-sflow	Микросервис сбора данных сетевой активности с сетевых устройств по протоколу SFlow	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• edo-flow-service: 8080/TCP;• Opensearch DB: 9200,9300/TCP
edo-flow-service	Микросервис сбора отчетов по сетевой активности	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• Opensearch DB: 9200,9300/TCP
edo-guest-portal-service	Микросервис гостевых порталов для доступа в сеть	<ul style="list-style-type: none">• edo-gateway-service: 8080/TCP;• Postgres DB: 5432/TCP
edo-metrics-collector	Микросервис централизованного сбора событий системы	<ul style="list-style-type: none">• Apache Kafka Service: 9092/TCP;• OpenSearch: 9200/TCP
edo-metrics-service	Микросервис отчетов событий системы	<ul style="list-style-type: none">• edo-identity-service: 8080/TCP;• edo-gateway-service: 8080/TCP;• Opensearch DB: 9200,9300/TCP;• Postgres DB: 5432/TCP;• Apache Kafka service: 9092/TCP
edo-schedule-service	Микросервис расписаний	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• edo-gateway-service: 8080/TCP;• Opensearch DB: 9200,9300/TCP
edo-report-portal-service	Микросервис генерации отчетов	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• Postgres DB: 5432/TCP
edo-task-portal-service	Микросервис по работе с заявками и управления изменениями	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• edo-gateway-service: 8080/TCP;• Postgres DB: 5432/TCP;• edo-license-service: 8080/TCP
edo-dns-service	Микросервис службы защищенного DNS	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• edo-dns-manager: 8081/TCP
edo-dns-manager	Микросервис управления службами защищенного DNS	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• efros-otel-collector: 4317/TCP;• edo-dns-service: 9153/TCP;• edo-dns-collector: 9153/TCP;• Postgres DB: 5432/TCP
edo-dns-collector	Микросервис обработки событий DNS (микросервиса edo-dns-service)	<ul style="list-style-type: none">• Apache Kafka service: 9092/TCP;• edo-dns-service: 9153/TCP;• edo-dns-manager: 8081/TCP
edo-backup-service	Микросервис резервного копирования и восстановления	<ul style="list-style-type: none">• edo-gateway-service: 8080/TCP;• Postgres DB: 5432
edo-kafka-cluster-controller****	Микросервис распределенного обмена сообщениями между серверными приложениями в режиме реального времени	

Имя сервиса	Описание	Связь с другими сервисами
	Apache Kafka	
edo-kafka-cluster-entity-operator**	Компонент Apache Kafka	<ul style="list-style-type: none">Apache Kafka: 9091/TCP
edo-kafka-cluster-kafka-exporter**	Микросервис, обеспечивающий трансляцию метрик и статистики Kafka	<ul style="list-style-type: none">Apache Kafka: 9091/TCP
strimzi-cluster-operator**	Микросервис управления Apache Kafka	<ul style="list-style-type: none">Apache Kafka: 9091/TCP
prometheus-efros-kube-prometheus-stac-prometheus**	Микросервис сбора и агрегации метрик и событий и его компоненты	<ul style="list-style-type: none">edo-metrics-collector: 8080/TCP;efros-efros-otel-collector: 8889/TCP;kube-dns: 9153/TCP;edo-radius: 9812/TCP;alertmanager: 8080/TCP, 9093/TCP;kube-state-metrics: 8080/TCP
efros-kube-prometheus-stac-operator**		
efros-kube-state-metrics**		
alertmanager-efros-kube-prometheus-stac-alertmanager**		
efros-efros-otel-collector**	Микросервис сбора и агрегации метрик и событий	<ul style="list-style-type: none">prometheus-efros-kube-prometheus-stac-prometheus: 9090/TCP
efros-local-path-provisioner**	Микросервис аллокации дискового пространства	
edo-ci-firewall-service	Микросервис, обеспечивающий отображение правил межсетевых экранов	<ul style="list-style-type: none">Postgres DB: 5432/TCP;edo-co-service: 80,443/TCP
edo-hierarchy-service	Микросервис, обеспечивающий построение иерархии между комплексами	<ul style="list-style-type: none">Postgres DB: 5432/TCP;Apache Kafka service: 9092/TCP
edo-ci-route-service	Микросервис, обеспечивающий построение векторов атак и путей на карте сети	<ul style="list-style-type: none">edo-ci-service: 20000/TCP
edo-sd-connector	Микросервис, обеспечивающий возможность интеграции с внешними системами заявок	<ul style="list-style-type: none">edo-identity-service: 8080/TCP;Postgres DB: 5432/TCP;Apache Kafka service: 9092/TCP;edo-gateway-service: 8080/TCP
edo-k8s-operator-service	Микросервис управления контейнеризацией и кластеризацией	

Имя сервиса	Описание	Связь с другими сервисами
opensearch-cluster-master***	Микросервис, обеспечивающий хранение событий	
edo-store-minio	Внутреннее S3-хранилище	
edo-store-postgres****	Микросервис встроенной БД	
migration-service	Микросервис миграции данных	• Postgres DB: 5432/TCP

* В комплексе на базе Docker-контейнера используется сервис «edo-proxy-service».

** Отсутствуют в комплексе на базе Docker-контейнера.

*** В комплексе на базе Docker-контейнера имеет имя «edo-store-opensearch».

**** В комплексе на базе Docker-контейнера имеет имя «edo-infr-kafka» и дополняется сервисом «edo-infr-zookeeper».

***** Отсутствует в комплексе на базе Kubernetes

 В случае возникновения каких-либо ошибок при разворачивании сервисов необходимо посмотреть логи сервиса.

Команда просмотра логов сервиса для комплекса на базе Docker-контейнера:

```
docker logs -t <имя контейнера>
```

Команда просмотра логов пода для комплекса на базе Kubernetes:

```
kubectl logs -nedo <имя пода>
```

1.2 Используемые программные и технические средства

Для эксплуатации и эффективного применения ПК «Efros DO» необходимо использование на ЭВМ лицензионного системного программного обеспечения.

Установка серверной части и внешних модулей ПК «Efros DO» может быть выполнена на базе Docker-контейнера или на базе Kubernetes (геораспределенный кластер). Минимальный состав технических средств ЭВМ для установки компонентов комплекса в разных исполнениях приведены в пунктах ниже.

1.2.1 Требования к среде функционирования комплекса на базе Docker-контейнера

Минимальный состав технических средств ЭВМ¹ для установки серверной части и внешних модулей ПК «Efros DO» на базе платформы контейнеризации Docker рассчитывается на основе данных, приведенных в таблице 2.

¹ Под ЭВМ понимается электронно-вычислительная машина, совместимая с архитектурой Intel x86 (x86_64).

Таблица 2 – Технические требования к среде функционирования ПК «Efros DO» и прикладному программному обеспечению на базе Docker-контейнера

Элемент	Параметр		
Количество объектов защиты	До 500	До 1000	До 2000*
Требования к программному обеспечению			
Операционная система	Astra Linux Special Edition (v.1.7, v.1.8) с ядром Linux 5.10.176-1-generic и выше, сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.); РЕД ОС (v. 7.3), сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)		
Поддерживаемые внешние СУБД**	СУБД «Jatoba», сертификат соответствия № 4327 (выдан ФСТЭК России 19.11.2020 г.) – кластерная версия и standalone-дистрибутив; СУБД PostgreSQL 14 и выше – standalone-дистрибутив		
Прикладное ПО	Система контейнерной изоляции приложений Docker v. 25.0.5 и выше (docker.io из состава ОС Astra Linux Special Edition (v.1.7)); Система контейнерной изоляции приложений Docker v. 25.0.7 и выше (docker-ce из состава РЕД ОС (v.7.3)); Система сборки, запуска и управления множеством контейнеров Docker-compose v. 2.4.0; Распределенная платформа потоковой обработки Confluent Kafka v. 5.5.15; Служба поиска OpenSearch v. 1.3.19; Система хранения MinIO v. 220218; Nginx v. 1.27.4		
Требования к аппаратному обеспечению			
Процессор	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)	16 ядер (от 2 ГГц)
Оперативная память	от 32 Гб	от 48 Гб	от 64 Гб
Жесткий диск (комплекс + СУБД)	от 600 Гб	от 1200 Гб	от 2400 Гб
Сервер комплекса	от 200 Гб	от 200 Гб	от 200 Гб
Сервер СУБД	от 400 Гб	от 1000 Гб	от 2200 Гб
Сетевая карта	от 1 Гбит/с	от 1 Гбит/с	от 1 Гбит/с
* От 2000 ОЗ – параметры рассчитываются индивидуально. Необходимо обращение в техподдержку			
** В состав ПК «Efros DO» входит встроенная СУБД «PostgreSQL», которую допускается использовать при пилотной эксплуатации комплекса. При этом необходимо учитывать, что при больших нагрузках работоспособность комплекса не гарантирована. Для штатной эксплуатации требуется внешняя СУБД, которая не входит в комплект поставки комплекса.			
При установке встроенной или внешней СУБД на сервер комплекса объем жесткого диска должен обеспечивать корректную работу комплекса			

Дополнительные требования приведены в пунктах 1.2.3 – 1.2.8.

1.2.2 Требования к среде функционирования комплекса на базе Kubernetes

ПК «Efros DO» может работать в режиме геораспределенного отказоустойчивого кластера, то есть на распределенной инфраструктуре из нескольких территориально удаленных данных центров (ЦОД).

Это позволяет сохранять работоспособность в случае выхода из строя одного из ЦОД, а также балансировать нагрузку и обеспечивать выделение из комплекса модулей для внешнего доступа.

Если один сервер выходит из строя, остальные серверы автоматически перенимают его функции, обеспечивая надежный и бесперебойный доступ к ресурсам и данным.

При восстановлении работоспособности узла происходит согласование узлов кластера, службы ПК «Efros DO» и кластер продолжают работать в штатном режиме.

При использовании 1 данных центра (ЦОД) рекомендуется устанавливать комплекс на 3 и более серверах (узлах). Для 3 и более ЦОД возможна установка любого нечетного равномерного количества узлов (3+3+1, 2+2+1, 1+1+1). Рекомендуется устанавливать комплекс на 5 и более узлах.

Технические требования к среде функционирования и прикладному программному обеспечению для ПК «Efros DO» на базе Kubernetes приведены в таблице 3.

Таблица 3 – Технические требования к среде функционирования и прикладному программному обеспечению для ПК «Efros DO» на базе Kubernetes

Элемент	Параметр
Требования к программному обеспечению	
Операционная система	Astra Linux Special Edition (v. 1.7, v. 1.8) с ядром Linux 5.10.176-1-generic и выше, сертификат соответствия № 2557 (выдан ФСТЭК России 27.01.2012 г.); РЕД ОС (v. 7.3), сертификат соответствия № 4060 (выдан ФСТЭК России 12.01.2019 г.)
Поддерживаемые внешние СУБД*	СУБД «Jatoba», сертификат соответствия № 4327 (выдан ФСТЭК России 19.11.2020 г.) – кластерная версия и standalone-дистрибутив**; СУБД PostgreSQL 14 и выше – standalone-дистрибутив
Прикладное ПО	Strimzi kafka (v3.7.0\0.44.0); Служба поиска OpenSearch (v. 2.18.0); Kubernetes (v. 1.29.6); NGINX Ingress Controller – nginx 1.25; Система хранения MinIO v. 220218; External DNS v.1.15.2
Требования для кластера Kubernetes	
SSH (администрирование)	порт 22/TCP
Kubernetes API (связь с API-сервером)	порт 6443/TCP

Элемент	Параметр
ClusterIP (виртуальный IP-адрес)	порт 9443/TCP
Плагин Cilium (сеть между узлами)	порт 4240/TCP порт 8472/UDP
etcd (хранилище состояния кластера)	порт 2379-2380/TCP
Kubelet API (связь с рабочими узлами)	порт 10250,10256/TCP
kube-scheduler (планировщик кластера)	порт 10259/TCP
kube-controller-manager (контроллеры управления)	порт 10257/TCP
NodePort Services (подключение к сервисам через узлы кластера)	порт 30000-30050/TCP
EDO DNS (поддержка геораспределенных систем)***	порт 53/UDP
Требования к аппаратному обеспечению для одного узла	
Процессор	8 ядер (рекомендуемое – 16 ядер) (от 2 ГГц); архитектура процессора – не ниже x86-64-v3
Оперативная память	32 Гб (рекомендуемое – 64 Гб)
Жесткий диск	Под корневой раздел: 100 Гб SSD для внешней базы; 300 Гб SSD для встроенной базы
Сетевая карта	от 1 Гбит/с
Требования к аппаратному обеспечению для Nexus-хоста	
Процессор	4 ядра (от 2 ГГц)
Оперативная память	8 Гб
Жесткий диск	100 Гб для хранения docker-образов
Порты	22,5000,8081/TCP
Доступ	SSH
Требования к аппаратному обеспечению для одного узла СУБД в data-центре****	
Процессор	16 ядер (от 2 ГГц)
Оперативная память	32 Гб (рекомендуемое – 64 Гб)
Жесткий диск	Под корневой раздел: 100 Гб SSD для внешней базы; 300 Гб SSD для встроенной базы

* Внешние СУБД не входят в поставку комплекса.

** Для обеспечения отказоустойчивости ПК «Efros DO» необходимо использовать внешнюю СУБД «Jatoba».

*** При установке геораспределенной конфигурации ПК «Efros DO» на базе GSLB или в разных подсетях.

**** Информация о зависимости смежной связанной системы приведена для справки

При установке комплекса на базе инфраструктуры Kubernetes следует учитывать:

- 1) Отказоустойчивость в схеме установки по умолчанию, обеспечивается приложением ***keepalived*** (на базе протокола VRRP 112) с обязательным доступом с узлов 1 и 3 до зарезервированного IP-адреса 224.0.0.18 (multicast передача пакетов).
- 2) В системе требуется отключить SWAP-файл.
- 3) При установке ограничений на потребление ресурсов модулями для сервиса «edo-dns-service» необходимо выделить не менее 2 Гб памяти и 2 ядер процессора на каждый контейнер. При меньшем объеме ресурсов возможны превышения лимитов по памяти и отключение контейнера.
- 4) Точные требования к аппаратному обеспечению для узла определяются проектным решением и инфраструктурой заказчика.

Дополнительные требования приведены в пунктах 1.2.3 – 1.2.8.

1.2.3 Требования к портам подключения для модулей ПК «Efros DO»

Общие требования к портам комплекса для подключения модулей ПК «Efros DO» приведены в таблице 4.

Таблица 4 – Требования к портам комплекса для подключения модулей ПК «Efros DO»

Элемент	Параметр
Требования для функционирования модуля «Efros NAC»	
TACACS+	порт 49/TCP (порт сервера)
DHCP	порт 67/UDP (порт сервера)
RADIUS	порт 1812,1813/UDP (порт сервера)
RADIUS CoA	порт 1700,3799/UDP (порт сервера)
Гостевые порталы	порт 5802/TCP (порт сервера)
Требования для функционирования модуля «Efros NFA»	
Netflow v9+, IPFIX	порт 2056/UDP (порт сервера)
sFlow	порт 6343/UDP (порт сервера)
Требования для функционирования модулей «Efros NA», «Efros FA», «Efros ICC», «Efros VC», «Efros CM»	
SNMP Trap / Inform	порт 162/UDP (порт сервера)
Syslog сервер UDP	порт 514/UDP (порт сервера)
Syslog сервер TCP	порт 1468/TCP (порт сервера)
Требования для функционирования модуля «Efros SDNS»	
DNS	порт 53/UDP (порт сервера)
Требования при использовании комплексом внешней СУБД	
СУБД «Jatoba»	порт 5432/TCP (порт назначения)
Требования по подключению к серверам синхронизации времени	
NTP	порт 123/UDP (порт назначения)

Элемент	Параметр
Требования для функционирования сканеров уязвимостей	
MaxPatrol 8	порт 22,445/TCP (порт назначения)
MaxPatrol VM	порт 80,443/TCP (порт назначения)
RedCheck	порт 80,443/TCP (порт назначения)
SafeERP	порт 80,443/TCP (порт назначения)
Требования по подключению почтовых серверов	
Microsoft Exchange Web Services Managed API	порт 443/TCP (порт назначения)
SMTP	порт 25,587,465/TCP (порт назначения)
Требования по подключению к сетевым папкам	
SMB	порт 445/TCP (порт назначения)
SFTP	порт 22/TCP (порт назначения)

Для ввода комплекса в домен при использовании модуля «Efros NAC» необходима доступность портов, приведенных в таблице 5.

Таблица 5 – Протоколы и порты, используемые для ввода в домен

Сервис	Порт
RPC Endpoint Mapper	135/TCP
NetBIOS	137,138/TCP/UDP
LDAP	389/TCP/UDP
LDAP SSL	636/TCP
LDAP GC	3268/TCP
LDAP GC SSL	3269/TCP
DNS	53/TCP/UDP
Kerberos	88/TCP/UDP
SMB	445/TCP

1.2.4 Требования к браузерам

Единый интерактивный веб-интерфейс обеспечивает доступ пользователей к функциональности ПК «Efros DO» с использованием следующих минимальных версий браузера:

- Google Chrome (130 и выше);
- Microsoft Edge (130 и выше);
- Яндекс.Браузер (24.10 и выше).

1.2.5 Требования к Windows-агенту ПК «Efros DO»

Технические требования к Windows-агенту ПК «Efros DO» приведены в таблице 6.

Таблица 6 – Технические требования к Windows-агенту ПК «Efros DO»

Элемент	Параметр
Windows-агент	
Операционная система	MS Windows (64-разрядные): <ul style="list-style-type: none">— Windows Server 2008R2 Foundation Edition SP1;— Windows Server 2008R2 Standard Edition SP1;— Windows Server 2008R2 Enterprise Edition SP1;— Windows Server 2008R2 Datacenter Edition SP1;— Windows Server 2012/2012R2 Foundation;— Windows Server 2012/2012R2 Essentials;— Windows Server 2012/2012R2 Standard;— Windows Server 2012/2012R2 Datacenter;— Windows Server 2016 Standard;— Windows Server 2016 Datacenter;— Windows Server 2016 Essentials;— Windows Server 2019 Standard;— Windows Server 2019 Datacenter;— Windows Server 2019 Essentials;— Windows 7 Professional SP1;— Windows 7 Enterprise SP1;— Windows 7 Ultimate SP1;— Windows 8.1 Core;— Windows 8.1 Professional;— Windows 8.1 Enterprise;— Windows 10 Home;— Windows 10 Pro;— Windows 10 Enterprise;— Windows 11 Home;— Windows 11 Pro;— Windows 11 Enterprise
Процессор	1,6 ГГц
Оперативная память	1 Гб
Жесткий диск	100 Мб
Требования к открытым портам для подключения Windows-агента	
Сбор данных с Windows-агента	20001/TCP (порт устройства с установленным Windows-агентом)
Отправка событий о запуске Windows-агента	20002/TCP (порт сервера ПК «Efros DO»)

1.2.6 Требования к агенту ПК «Efros DO»

Технические требования к агенту ПК «Efros DO» приведены в таблице 7.

Таблица 7 – Технические требования к агенту ПК «Efros DO»

Элемент	Параметр
Агент ПК «Efros DO» (версия 1.5)	
Операционная система	Astra Linux Special Edition (v.1.7, v.1.8) x86_64; РЕД ОС (рабочая станция) (v.7.3) x86_64; Ubuntu 22.04 x86_64; macOS Monterey (v.12.6) x86_64; MS Windows (64-разрядные): <ul style="list-style-type: none">— Windows Server 2016 Standard;— Windows Server 2016 Datacenter;— Windows Server 2016 Essentials;— Windows Server 2019 Standard;— Windows Server 2019 Datacenter;— Windows Server 2019 Essentials;— Windows 10 Home;— Windows 10 Pro;— Windows 10 Enterprise;— Windows 11 Home;— Windows 11 Pro;— Windows 11 Enterprise
Требования к портам подключения агента ПК «Efros DO»	
Взаимодействие с устройством	9123/TCP (порт ЭВМ с установленным агентом)
Взаимодействие с ПК «Efros DO»	8443/TCP (порт сервера ПК «Efros DO»)
Встроенный модуль «Суппликант»	
Операционная система	Поддерживаемые операционные системы: <ul style="list-style-type: none">— Astra Linux Special Edition (v.1.7, v.1.8) x86_64;— РЕД ОС (рабочая станция) (v.7.3) x86_64;— Ubuntu 22.04 x86_64;— MS Windows (поддерживаются версии ОС, аналогичные приведенным для агента ПК «Efros DO», указанные в данной таблице выше)
Прикладное ПО	Прикладное ПО для работы с сетевыми интерфейсами в ОС MS Windows: <ul style="list-style-type: none">— WinPcap v. 3.0 и выше*;— Npcap v. 1.82 (не входит в комплект поставки комплекса)

Элемент	Параметр
Токены	Поддерживаемые токены: — JaCarta PKI; — JaCarta PKI/Flash
Встроенный модуль «Сбор событий»	
Операционная система	MS Windows (поддерживаются версии ОС, аналогичные приведенным для агента ПК «Efros DO», указанные в данной таблице выше)
Встроенный модуль «Взаимодействие с VPN клиентами»	
NGate	VPN-клиент NGate 1.0.30-6 и 1.0.30-18. Поддерживаемые операционные системы: — Astra Linux Special Edition (v.1.7, v.1.8) x86_64; — РЕД ОС (рабочая станция) (v.7.3) x86_64; — Ubuntu 22.04 x86_64; — MS Windows (поддерживаются версии ОС, аналогичные приведенным для агента ПК «Efros DO», указанные в данной таблице выше)
S-Terra	C-Terra Клиент 5.0. Поддерживаемые операционные системы: — MS Windows (поддерживаются версии ОС, аналогичные приведенным для агента ПК «Efros DO», указанные в данной таблице выше)
Модуль «Контроль целостности до загрузки ОС»**	
Процессор	Материнская плата целевого устройства должна иметь процессор архитектуры Intel x86-64 класса Pentium и выше
BIOS	Соответствие спецификации UEFI BIOS версии не ниже 2.0
Устройство хранения	Требования к устройству хранения: — не менее 200 Мб; — наличие раздела «EFI System Partition» с разметкой GPT; — наличие раздела FAT32 при установке с разметкой MBR
Операционная система	Поддерживаемые операционные системы: — Astra Linux Special Edition (v.1.7, v.1.8) x86_64; — РЕД ОС (рабочая станция) (v.7.3) x86_64; — MS Windows (поддерживаются версии ОС, аналогичные приведенным для агента ПК «Efros DO», указанные в данной таблице выше). ! Параметр «Secure Boot» должен быть отключен в настройках EFI/UEFI BIOS целевого устройства для корректной работы модуля и компьютера
* Установка WinPcap v. 4.1.3 доступна при установке агента.	
** Установка модуля «Контроль целостности до загрузки ОС» должна осуществляться на физическую ЭВМ	

1.2.7 Используемые протоколы и порты устройств

Активный аудит контролируемого оборудования осуществляется с использованием протоколов и входящих портов устройств, указанных в таблице 8.

Таблица 8 – Протоколы и входящие порты устройств, используемые ПК «Efros DO» для аудита оборудования

Протокол	Назначение	Функции	Входящий порт устройства, TCP
SSH	Получение конфигурации сетевых устройства, систем виртуализации, операционных систем семейства UNIX	Модули из категории: Сетевые, Виртуализация, Модуль Linux	22*
SSH	Получение конфигурации WatchGuard	Модуль WatchGuard	4118*
Telnet	Получение конфигурации сетевых устройств	Модули из категории: Сетевые	23*
REST API (HTTPS)	Получение конфигурации сетевых устройства, систем виртуализации, UiPath RPA	Модули из категории: Сетевые, Виртуализация, Модуль UiPath RPA	443*
REST API (HTTPS)	Получение конфигурации Континент 4	Модуль Код Безопасности	444*
REST API (HTTPS)	Получение конфигурации Primo RPA	Модуль Primo RPA	50001*
REST API (HTTPS)	Получение конфигурации Tionix	Модуль Tionix	5000*, 8774*, 9696*
REST API (HTTPS)	Получение конфигурации Kubernetes	Модуль Kubernetes	6443*
REST API (HTTPS)	Получение конфигурации Proxmox	Модуль Альт Сервер Виртуализации	8006*
vSphere Web Services API (SOAP over HTTPS)	Получение конфигурации VMware ESXi, VMware vCenter	Модуль vCenter	443
LDAP	Получение конфигурации Microsoft Active Directory	Модуль Active Directory Domain	389
LDAPS			636
SMB			445
LEA	Получение конфигурации Check Point SmartCenter R77	Модуль Check Point	18184
CPMI			18190
XML-RPC	Получение конфигурации UserGate	Модуль UserGate	4040*
Microsoft TDS	Получение конфигурации СУБД Microsoft SQL	Модуль Microsoft SQL	1433*

Протокол	Назначение	Функции	Входящий порт устройства, TCP
Oracle Net	Получение конфигурации СУБД Oracle	Модуль Oracle	1521*
PostgreSQL Protocol	Получение конфигурации СУБД PostgreSQL, Jatoba	Модуль PostgreSQL, модуль Jatoba	5432*
Firebird Wire Protocol	Получение конфигурации СУБД Firebird	Модуль Firebird	3050*
MySQL Client/Server Protocol	Получение конфигурации СУБД MySQL	Модуль MySQL	3306*
SCP	Копирование на устройство с Docker скрипта для выполнения «Проверок безопасности Docker»	Модуль Docker	22*
SFTP	Копирование файлов конфигурации устройств Cisco ASA, Dionis и Континент 3 для контроля конфигурации устройств	Модуль Cisco, модуль Фактор-TC, модуль Код Безопасности	22*
SCP, SFTP	Копирование файлов конфигурации на устройство для восстановления конфигурации	Восстановление конфигурации оборудования	22*
SNMP	Сканирование сети для последующего добавления найденных устройств в список устройств	Сканирование сети (SNMP сканер)	161*
Проприетарный на базе HTTPS	Сбор данных с Windows-агента о операционной системе Windows	Модуль Windows	20001*

* Номер порта по умолчанию, можно установить произвольный номер порта

1.2.8 Используемые порты внешних систем

Для управления списком внешних сервисов отправки сообщений/совершения звонков для валидации номера телефона, задаваемого пользователем при самостоятельной регистрации на гостевом портале необходимо настроить взаимодействие с SMS-провайдерами согласно таблице 9.

Таблица 9 – SMS-провайдеры

SMS-provайдеры	Порт
SMS.RU	443/TCP
OZEKI	9508/TCP Примечание: см. документацию вендора

2 Общие указания по установке комплекса

Перед началом эксплуатации ПК «Efros DO» необходимо ознакомиться с сопроводительными документами.

-  Установка изделия должна осуществляться под руководством специально подготовленного персонала

При установке изделия на ЭВМ рекомендуется консультироваться с технической поддержкой ООО «Газинформсервис».

Телефон технической поддержки: 8 (800) 700-09-87.

Официальный сайт: <https://www.gaz-is.ru/>.

Email: support@gaz-is.ru.

Электронный адрес для обращения в техническую поддержку:

<https://www.gaz-is.ru/poddergka/zajavka.html>.

Пользователи изделия могут обратиться в техническую поддержку по указанному телефону в рабочие дни с 09:00 до 18:00 (в пятницу до 17:00), круглосуточно на сайте разработчика или по адресу электронной почты разработчика (производителя).

3 Состав и содержание дистрибутива

Комплект установочных файлов предоставляется производителем в виде ссылки для скачивания. Также комплект может быть поставлен заказчику на установочном компакт-диске. Состав дистрибутива для ПК «Efros DO» на базе Docker-контейнера указан в таблице 10, на базе Kubernetes – в таблице 11.

Дистрибутив агента ПК «Efros DO» для установки агента на конечную точку под управлением различных ОС поставляется совместно с дистрибутивом ПК «Efros DO» и приведен в таблице 12.

Таблица 10 – Состав дистрибутива для установки ПК «Efros DO» на базе Docker-контейнера

Файл	Назначение
efros-do-<номер релиза>.tar.gz	Дистрибутив, содержащий все компоненты программы, образы и зависимости
deploy.sh	Скрипт для установки ПК «Efros DO» на ОС
Описание модулей.zip	Описание подключаемых внешних модулей для работы с устройствами
Efros Config Inspector Agent <версия>.Remote_Install.msi	Файл для массовой удаленной установки windows-агента на конечную точку
Efros Config Inspector Agent <версия>.msi	Файл для установки windows-агента на конечную точку
README.md	Инструкция по установке

Таблица 11 – Состав дистрибутива для установки ПК «Efros DO» на базе Kubernetes

Файл	Назначение
docker-compose.yml	Декларативное описание контейнера с Nexus
deploy.sh	Скрипт для установки и запуска Nexus
Efros Config Inspector Agent <версия>.Remote_Install.msi	Файл для установки windows-агента на конечную точку для массовой удаленной установки
Efros Config Inspector Agent <версия>.msi	Файл для установки windows-агента на конечную точку
INSTALL.md	Инструкция по установке Nexus
nexus3.tar.gz	Образ Nexus
nexus_data.tar.gz	Образы и зависимости кластерной версии ПК «Efros DO»
nexus_dependencies.tar.gz	Зависимости для разворачивания Nexus в контейнере
start.sh	Скрипт для запуска Nexus
stop.sh	Скрипт для остановки Nexus
nexus_env	Переменные среды для разворачивания Nexus
checksum.sha256	Контрольные суммы файлов дистрибутива
download_distr.py	Скрипт для выгрузки инсталлятора из Nexus
custom_registry	Каталог со скриптами настройки удаленного репозитория образов

Файл	Назначение
custom_registry/load_image.sh	Скрипт для загрузки образа на удаленный репозиторий образов
custom_registry/main.py	Скрипт для переноса образов ПК «Efros DO» с локального репозитория образов на удаленный

Таблица 12 – Состав дистрибутива для установки агента ПК «Efros DO»

Файл	Назначение
Astra 1.7 x86_64.zip	Дистрибутив агента ПК «Efros DO» для установки агента на конечную точку под управлением ОС Astra Linux Special Edition
RedOS 7.3 x86_64.zip	Дистрибутив агента ПК «Efros DO» для установки агента на конечную точку под управлением РЕД ОС
Windows x86_64.zip	Дистрибутив агента ПК «Efros DO» для установки агента на конечную точку под управлением ОС MS Windows
MacOS x86_64.zip	Дистрибутив агента ПК «Efros DO» для установки агента на конечную точку под управлением macOS
Ubuntu 22.04 x86_64.zip	Дистрибутив агента ПК «Efros DO» для установки агента на конечную точку под управлением ОС Ubuntu 22.04

Состав образов функциональных модулей и микросервисов ПК «Efros DO» на базе Docker-контейнера, поставляемых пользователю, приведен в таблице 13. Состав образов функциональных модулей и микросервисов ПК «Efros DO» на базе Kubernetes аналогичен составу, приведенному в таблице 13 и дополнительно содержит образы, перечень которых приведен в таблице 14.

Таблица 13 – Состав образов для ПК «Efros DO» на базе Docker-контейнера

Файл	Назначение
edo-acs-service.tar.gz	Функциональный модуль централизованного управления контролем доступа к сетевым устройствам
edo-efrosci.tar.gz	Функциональный модуль управления конфигурациями, анализа защищенности, анализа сетевой безопасности и оценки рисков
edo-agent-service.tar.gz	Микросервис управления агентами ПК «Efros DO»
edo-backup-service_latest.tar.gz	Микросервис резервного копирования и восстановления
edo-ci-firewall-service.tar.gz	Микросервис загрузки данных из базы правил межсетевых экранов
edo-ci-route-service.tar.gz	Микросервис поиска маршрутов для моделирования трафика на карте сети
edo-dns-manager.tar.gz	Микросервис управления службами DNS
edo-dns-service.tar.gz	Микросервис службы DNS

Файл	Назначение
edo-dns-collector.tar.gz	Микросервис обработки событий DNS
edo-email-sender-service.tar.gz	Микросервис отправки сообщений
edo-flow-collector.tar.gz	Модуль сбора статистики
edo-flow-service.tar.gz	Модуль Flow Service
edo-gateway-service.tar.gz	Микросервис маршрутизации запросов
edo-hierarchy-service.tar.gz	Микросервис поддержки иерархии
edo-identity-service.tar.gz	Микросервис аутентификации и авторизации
edo-k8s-operator.tar.gz	Микросервис управления контейнеризацией и кластеризацией
edo-knowledge-base-service.tar.gz	Микросервис базы знаний
edo-license-service.tar.gz	Микросервис лицензирования
edo-metrics-collector.tar.gz	Микросервис уведомлений и событий
edo-metrics-service.tar.gz	Микросервис сбора метрик ИБ
edo-portal-api.tar.gz	Микросервис гостевых порталов
edo-proxy-service_1.23.1.tar.gz	Микросервис сервера Nginx, выполняющий шифрование трафика и обратное проксирование
edo-radius_3.0.21-latest.tar.gz	Модуль протокола RADIUS
edo-report-portal-service.tar.gz	Микросервис генерации отчетов
edo-samba-service_4.9.5.tar.gz	Функциональный модуль централизованного управления контролем доступа к сетевым устройствам
edo-schedule-service.tar.gz	Микросервис расписаний
edo-so-service.tar.gz	Микросервис объектов защиты
edo-tacacs_4.0.65535-latest.tar.gz	Модуль протокола TACACS+
edo-task-portal-service.tar.gz	Микросервис системы заявок
edo-vulnerability-collector.tar.gz	Микросервис драйверов сканеров уязвимостей
edo-web-service.tar.gz	Платформа интеграции
edo-infr-kafka_5.5.15-1-ubi8.tar.gz	Микросервис распределенного обмена сообщениями между серверными приложениями в режиме реального времени
edo-infr-zookeeper_5.5.15-1-ubi8.tar.gz	Микросервис синхронизации хранилищ
edo-migration-service.tar.gz	Микросервис миграции данных
edo-sd-connector_latest.tar.gz	Микросервис, обеспечивающий возможность интеграции с внешними системами заявок
edo-store-minio_220218.tar.gz	Внутреннее S3-хранилище
edo-store-opensearch_1.3.19-s3.tar.gz	Микросервис, обеспечивающий хранение событий
edo-store-postgres_15.tar.gz	Модуль встроенного хранилища
edo-voltron-service_latest.tar.gz	Микросервис проксирования API CI

Таблица 14 – Состав дополнительных образов для ПК «Efros DO» на базе Kubernetes

Файл	Назначение
edo-kafka-cluster-entity-operator	Компонент Apache Kafka
edo-kafka-cluster-kafka-exporter	Микросервис, обеспечивающий трансляцию метрик и статистики Kafka
strimzi-cluster-operator	Микросервис управления Apache Kafka
prometheus-efros-kube-prometheus-stac-prometheus	Микросервис сбора и агрегации метрик и событий и его компоненты
efros-kube-prometheus-stac-operator	
efros-kube-state-metrics	
alertmanager-efros-kube-prometheus-stac-alertmanager	
efros-efros-otel-collector	Микросервис сбора и агрегации метрик и событий
efros-local-path-provisioner	Микросервис аллокации дискового пространства
opensearch-cluster-master	Аналог edo-store-opensearch для кластера
nginx-controller	Аналог edo-proxy-service для кластера

4 Предварительные настройки

4.1 Настройка СУБД

- (i) При использовании встроенной СУБД на базе Docker-контейнера дополнительные настройки не требуются. СУБД разворачивается в отдельном контейнере в ходе установки комплекса (см. раздел 5).
- ! Работа комплекса со встроенной СУБД поддерживается только для исполнения ПК «Efros DO» на базе Docker-контейнера. На базе Kubernetes использование встроенной СУБД не допускается.

При использовании внешней СУБД необходимо предварительно выполнить установку СУБД в соответствии с документацией на используемую версию СУБД.

Для настройки работы внешней СУБД PostgreSQL\СУБД «Jatoba» с ПК «Efros DO» необходимо произвести следующие действия:

- 1) Создать во внешней СУБД служебного пользователя для ПК «Efros DO», который будет владельцем БД для программного комплекса.
- 2) Разрешить служебному пользователю подключаться к БД комплекса с IP-адреса сервера, на котором будет установлен непосредственно комплекс. Для этого необходимо в файле ***pg_hba.conf*** для ***IPv4 local connections*** прописать значения, в зависимости от установки СУБД и комплекса:
 - если СУБД установлена отдельно от сервера комплекса при работе с ПК «Efros DO» на базе Docker-контейнера:

```
host {имя_базы_данных} {имя_служебного_пользователя_edo} x.x.x.x/32
md5

host {имя_базы_данных}-ci {имя_служебного_пользователя_edo}
x.x.x.x/32 md5

host {имя_базы_данных}-cifw {имя_служебного_пользователя_edo}
x.x.x.x/32 md5

host postgres {имя_служебного_пользователя_edo} x.x.x.x/32 md5
```

где x.x.x.x – IP-адрес сервера комплекса.

- в случае установки СУБД и ПК на один сервер при работе с ПК «Efros DO» на базе Docker-контейнера:

```
host {имя_базы_данных} {имя_служебного_пользователя_edo} x.x.x.x/32
md5

host {имя_базы_данных}-ci {имя_служебного_пользователя_edo}
x.x.x.x/32 md5
```

```
host {имя_базы_данных}-cifw {имя_служебного_пользователя_edo}  
x.x.x.x/32 md5  
  
host postgres {имя_служебного_пользователя_edo} x.x.x.x/32 md5
```

где x.x.x.x – IP-адрес сервера, на который установлен комплекс и СУБД.

```
host {имя_базы_данных} {имя_служебного_пользователя_edo}  
172.16.128.0/17 md5  
  
host {имя_базы_данных}-ci {имя_служебного_пользователя_edo}  
172.16.128.0/17 md5  
  
host {имя_базы_данных}-cifw {имя_служебного_пользователя_edo}  
172.16.128.0/17 md5  
  
host postgres {имя_служебного_пользователя_edo} 172.16.128.0/17 md5
```

где 172.16.128.0 – IP-адрес сети Docker-контейнера по умолчанию.

- если СУБД установлена отдельно от сервера комплекса при работе с ПК «Efros DO» на базе Kubernetes:

```
host {имя_базы_данных} {имя_служебного_пользователя_edo}  
ip_address_host1/32 md5  
  
host {имя_базы_данных} {имя_служебного_пользователя_edo}  
ip_address_host2/32 md5  
  
host {имя_базы_данных} {имя_служебного_пользователя_edo}  
ip_address_host3/32 md5  
  
host {имя_базы_данных}-ci {имя_служебного_пользователя_edo}  
ip_address_host1/32 md5  
  
host {имя_базы_данных}-ci {имя_служебного_пользователя_edo}  
ip_address_host2/32 md5  
  
host {имя_базы_данных}-ci {имя_служебного_пользователя_edo}  
ip_address_host3/32 md5  
  
host {имя_базы_данных}-cifw {имя_служебного_пользователя_edo}  
ip_address_host1/32 md5  
  
host {имя_базы_данных}-cifw {имя_служебного_пользователя_edo}  
ip_address_host2/32 md5  
  
host {имя_базы_данных}-cifw {имя_служебного_пользователя_edo}  
ip_address_host3/32 md5  
  
host postgres {имя_служебного_пользователя_edo} ip_address_host1/32  
md5  
  
host postgres {имя_служебного_пользователя_edo} ip_address_host2/32  
md5  
  
host postgres {имя_служебного_пользователя_edo} ip_address_host3/32  
md5
```

где команда «host postgres...» – предназначена для запуска проверки корректности пароля подключения к СУБД при работе с ПК «Efros DO» на базе Kubernetes.

! Для обеспечения отказоустойчивости ПК «Efros DO» на базе Kubernetes необходимо использовать внешнюю СУБД «Jatoba».

- 3) В конфигурационном файле ***postgresql.conf*** разрешить прослушивать другие адреса. По умолчанию, СУБД прослушивает только ***localhost***. Необходимо раскомментировать строку ***listen_addresses = 'localhost'*** и указать или IP-адрес сервера (рекомендуется), на котором установлен комплекс, или разрешить прослушивание запросов на всех IP-адресах (*):

```
listen_addresses = '*'
```

! При создании базы данных необходимо, чтобы были указаны следующие параметры:

- тип кодировки – Encoding UTF8;
- порядок сортировки строк – LC_COLLATE en-US;
- классификация символов – LC_CTYPE en-US.

4.2 Настройка политик безопасности ОС

- !** Процесс установки дистрибутива одинаков для различных поддерживаемых операционных систем: Astra Linux Special Edition (Astra Linux SE), РЕД ОС. При установке на целевую ОС необходимо скопировать архив дистрибутива, действия со скриптом аналогичны.
- !** При установке комплекса на ОС Astra Linux SE обязательно выполнить действия, описанные в пунктах 4.2.1 – 4.2.3. Для других ОС эти пункты пропускаются.
- !** При установке комплекса на ОС РЕД ОС (v. 7.3) автоматически выключается система контроля доступа Security-Enhanced Linux. Допускается включение функции системы контроля доступа только в режиме «Permissive». В этом случае информация о всех действиях, которые нарушают текущую политику безопасности, будут зафиксированы в журнале, но сами действия не будут заблокированы

Ниже приведен порядок установки ПК «Efros DO». В качестве примера взята ОС Astra Linux SE. Для ПК «Efros DO» на этапе завершения установки ОС Astra Linux SE, необходимо добавить наборы программного обеспечения, приведенные на рис. 2.

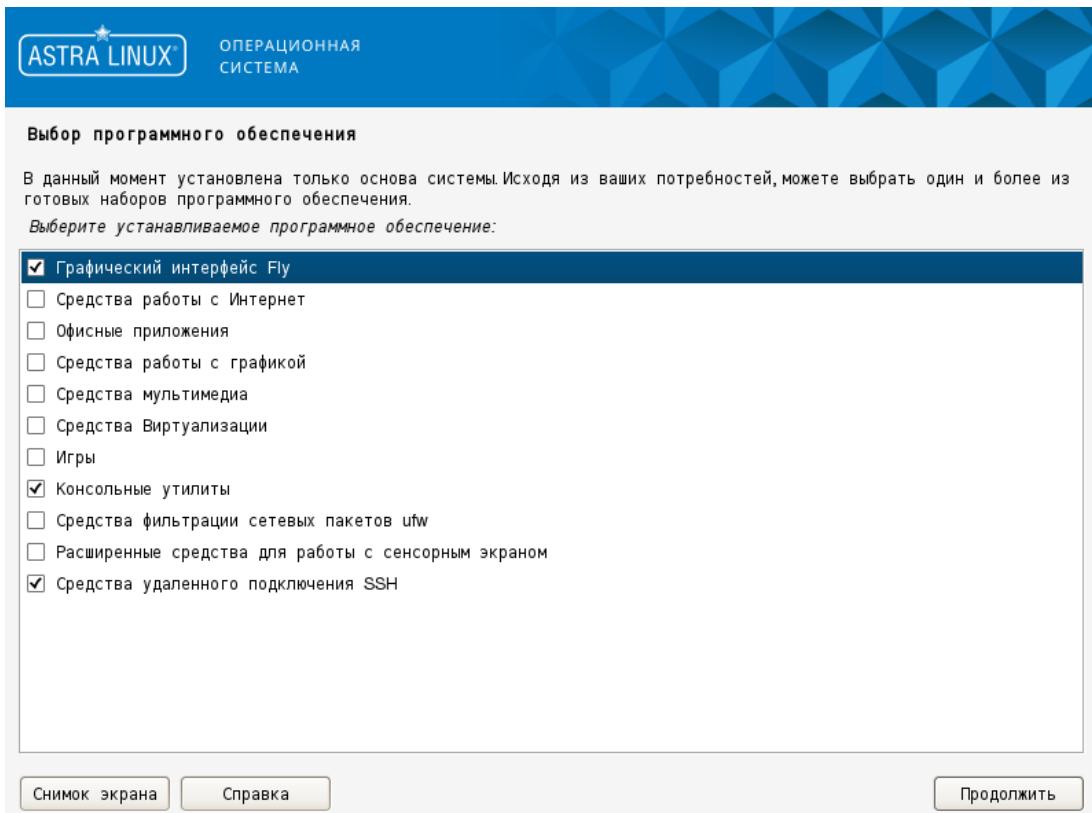


Рисунок 2 – Завершение установки ОС Astra Linux SE

4.2.1 Настройка политик безопасности ОС для типа защиты «Максимальный» («Смоленск»)

Перед установкой ПК «Efros DO» необходимо выполнить следующие настройки ОС Astra Linux SE для типа защиты «Максимальный» («Смоленск»):

- 1) После ввода логина и пароля, при выборе атрибутов безопасности для учетной записи из раскрывающегося списка необходимо выбрать уровень целостности «Высокий» (рис. 3).

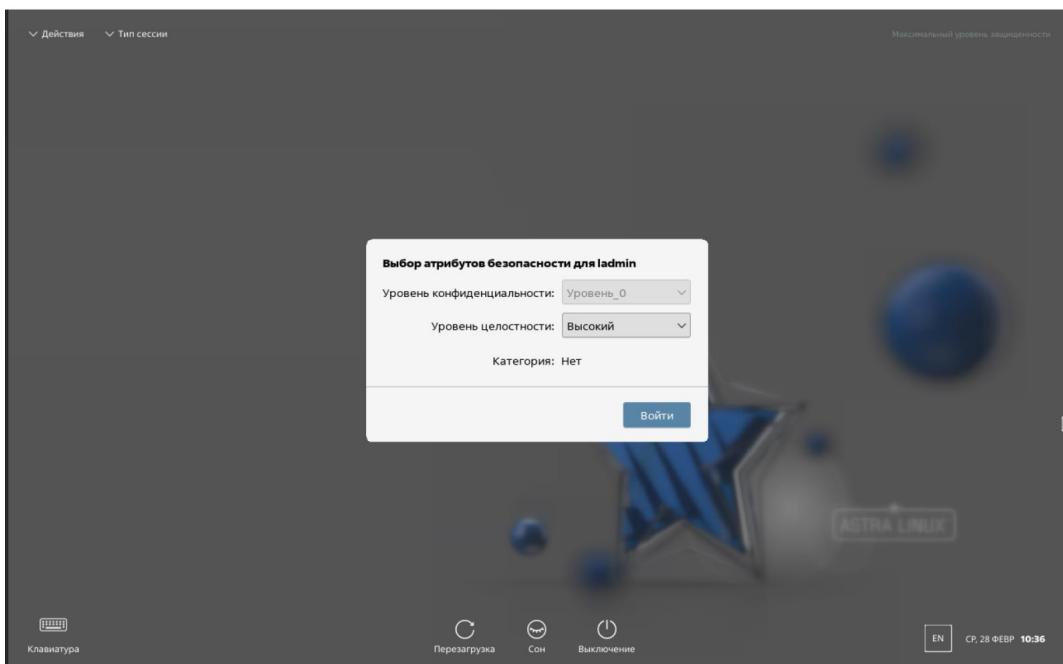


Рисунок 3 – Выбор атрибутов безопасности

- 2) Перейти в меню «Пуск» → «Системные» → «Политика безопасности» (рис. 4).

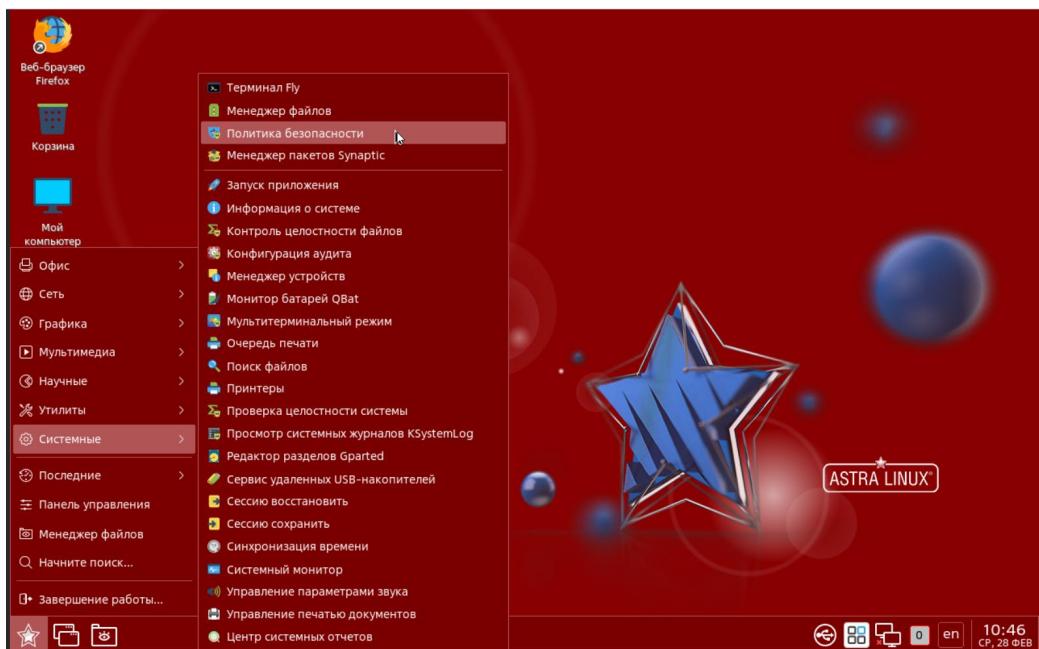


Рисунок 4 – Вкладка «Политики безопасности»

- 3) Ввести пароль администратора ОС (рис. 5).

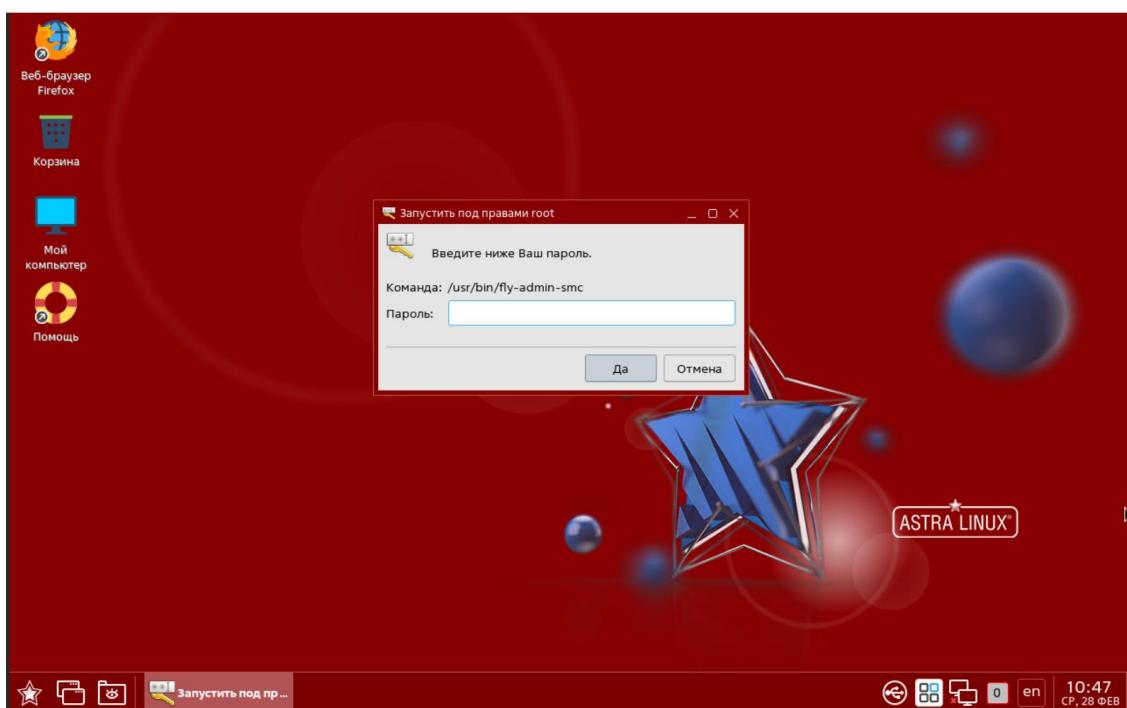


Рисунок 5 – Ввод пароля администратора ОС

- 4) Откроется окно «Управление политикой безопасности – Локальная политика» (рис. 6).

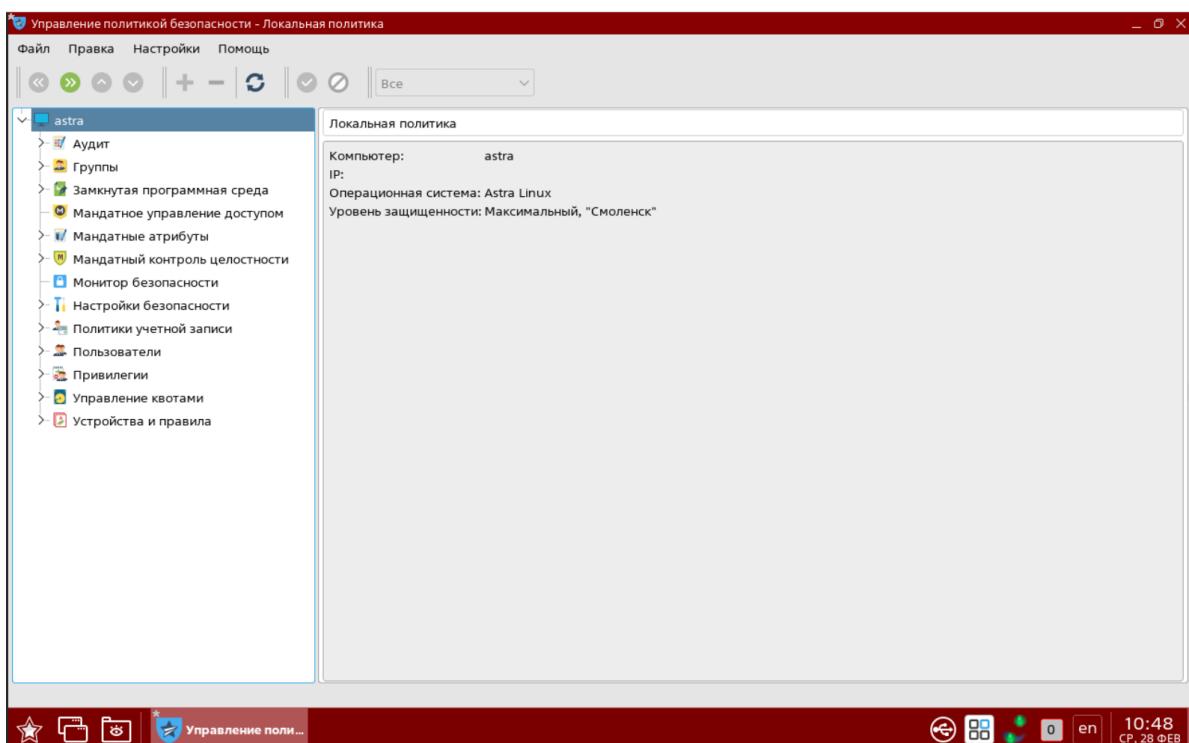


Рисунок 6 – Окно «Управление политикой безопасности – Локальная политика»

- 5) Перейти в раздел «Замкнутая программная среда» (рис. 7).

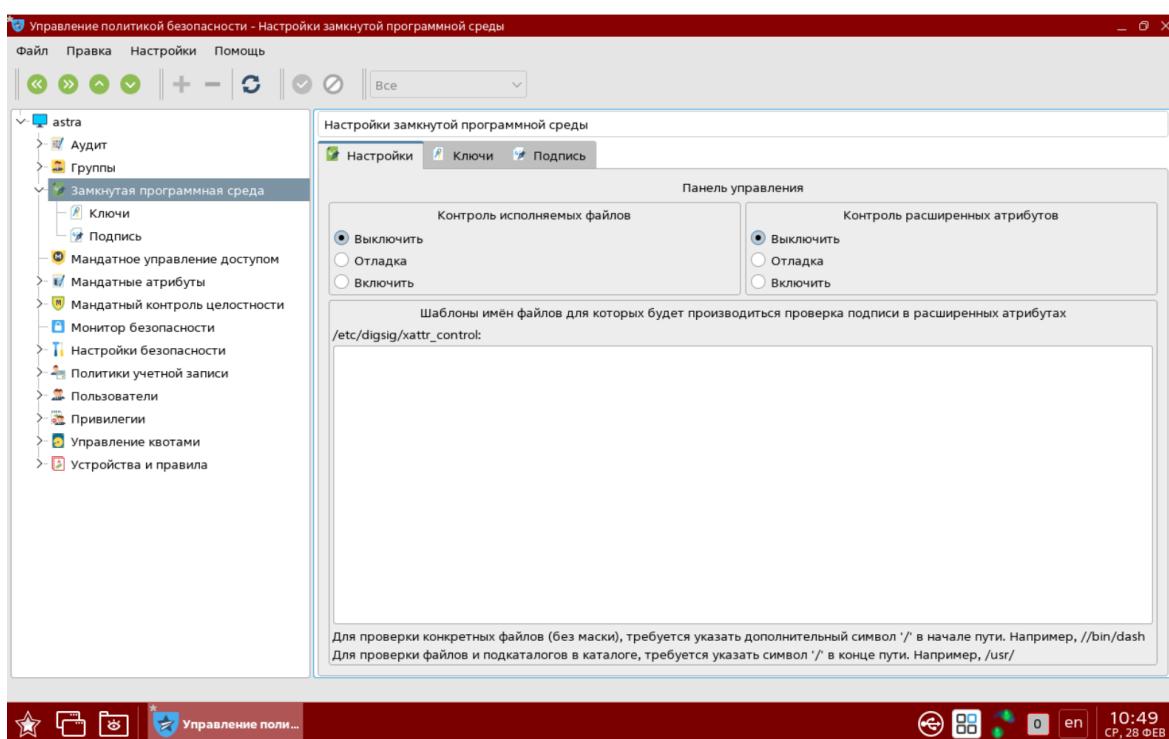


Рисунок 7 – Раздел «Замкнутая программная среда»

По умолчанию функции контроля исполняемых файлов и контроля расширенных атрибутов выключены. Необходимо оставить режим «Выключить» либо выбрать режим «Отладка». При использовании режима «Отладка» система будет выводить предупреждения о неподписанных файлах, но запуск их будет разрешен.

Аналогичную настройку можно произвести редактированием конфигурационного файла **/etc/digsig/digsig_initramfs.conf** – для использования отладочного режима для тестирования специального ПО параметру **DIGSIG_ELF_MODE** необходимо установить значение «2»: **DIGSIG_ELF_MODE=2**.

- 6) Перейти в раздел «Мандатное управление доступом» (рис. 8). Убедиться, что в поле «Подсистема Мандатного Управления Доступом» проставлен флаг.
- 7) Перейти в раздел «Мандатный контроль целостности» (рис. 9). Убедиться, что в поле «Подсистема Мандатного Контроля Целостности» проставлен флаг.

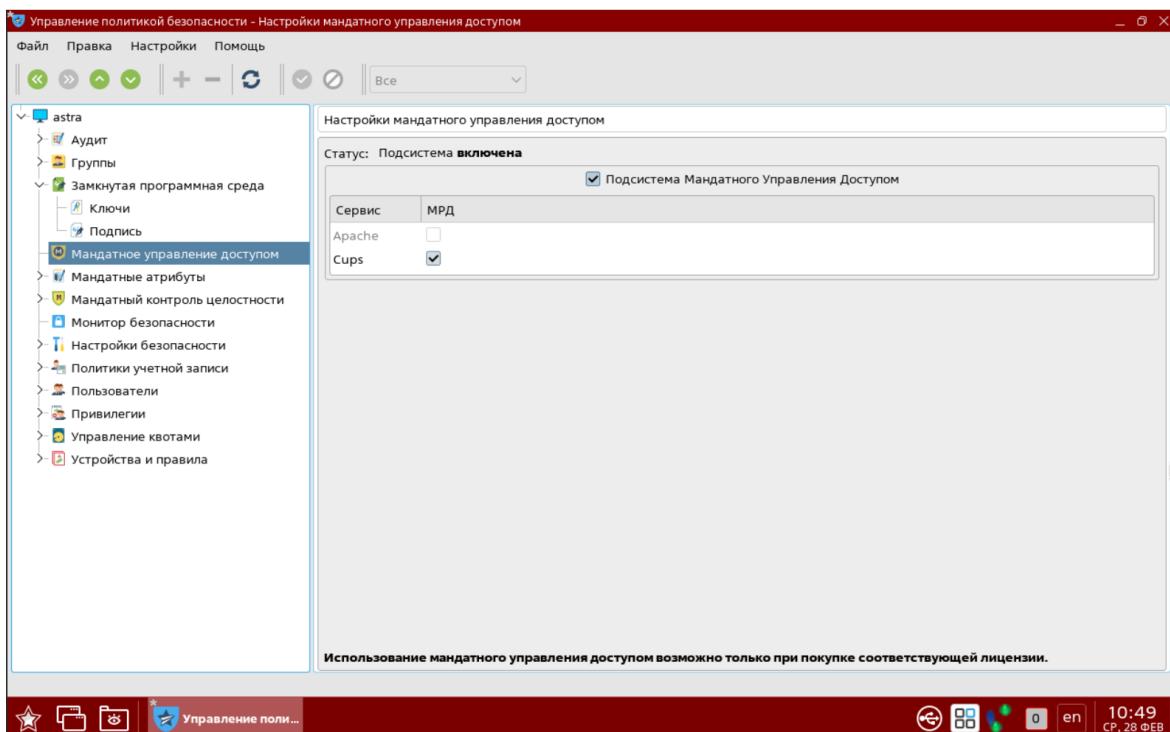


Рисунок 8 – Раздел «Мандатное управление доступом»

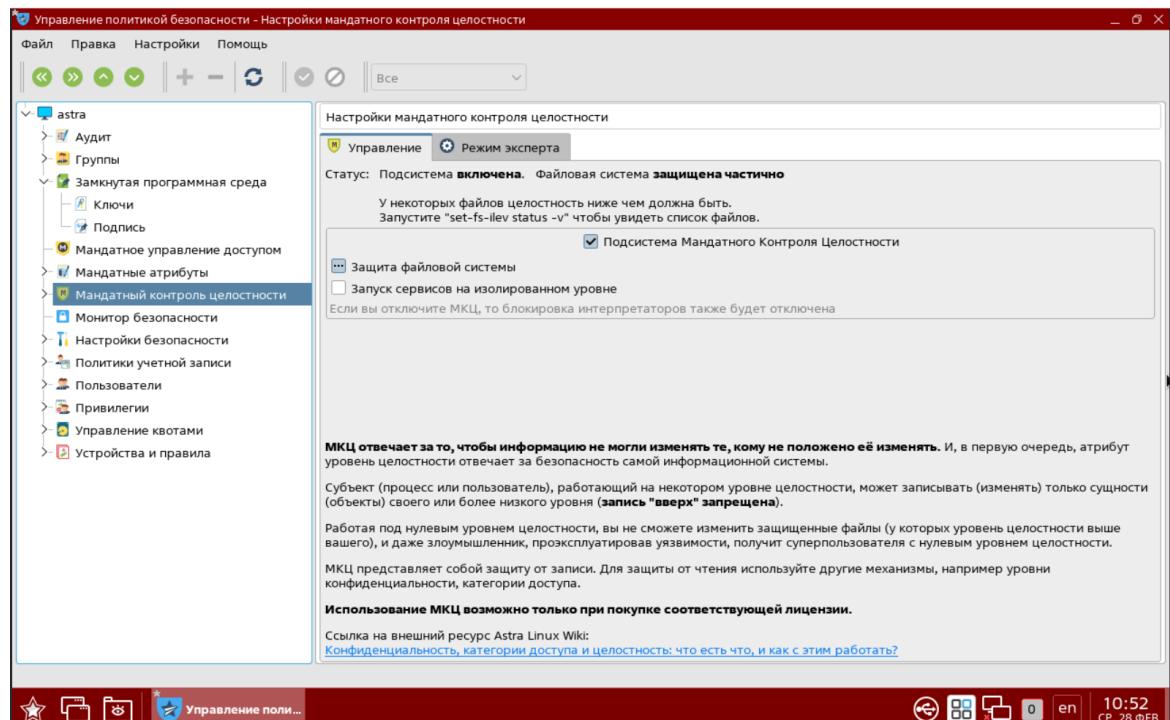


Рисунок 9 – Раздел «Мандатный контроль целостности»

- 8) Перейти в подраздел «Политика очистки памяти». Флаг в поле «Очистка разделов подкачки» должен отсутствовать (рис. 10).

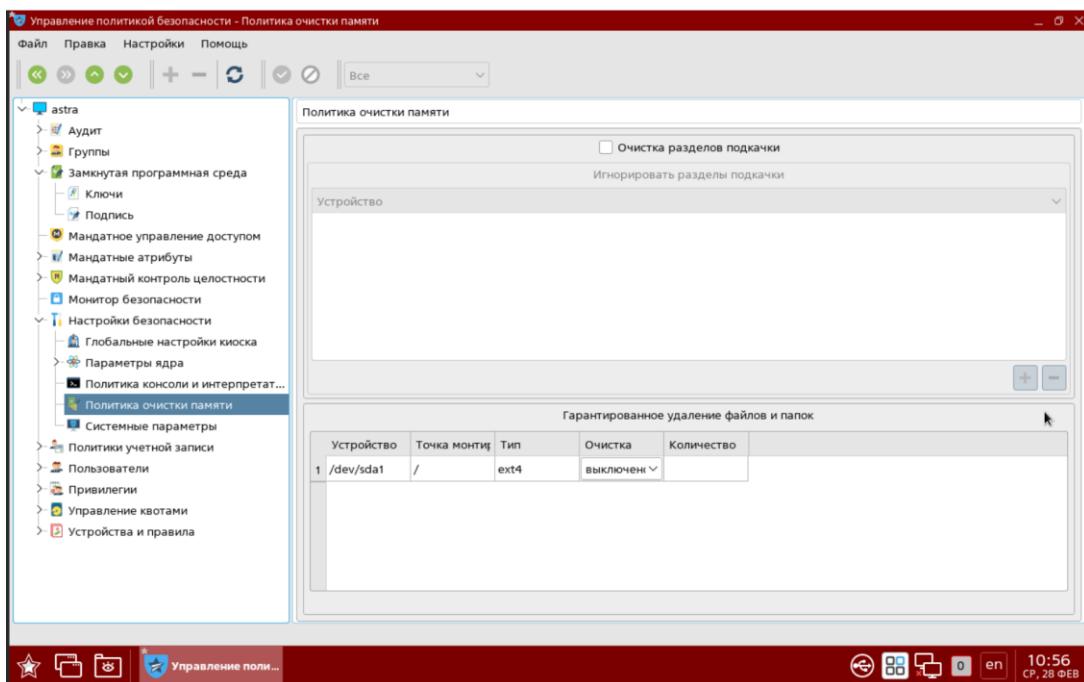


Рисунок 10 – Подраздел «Политика очистки памяти»

- 9) Перейти в подраздел «Системные параметры» (рис. 11). Установить флаги в следующих полях:
- «Включить аудит parsec»;
 - «Блокировка клавиш SysRq для всех пользователей, включая администраторов».

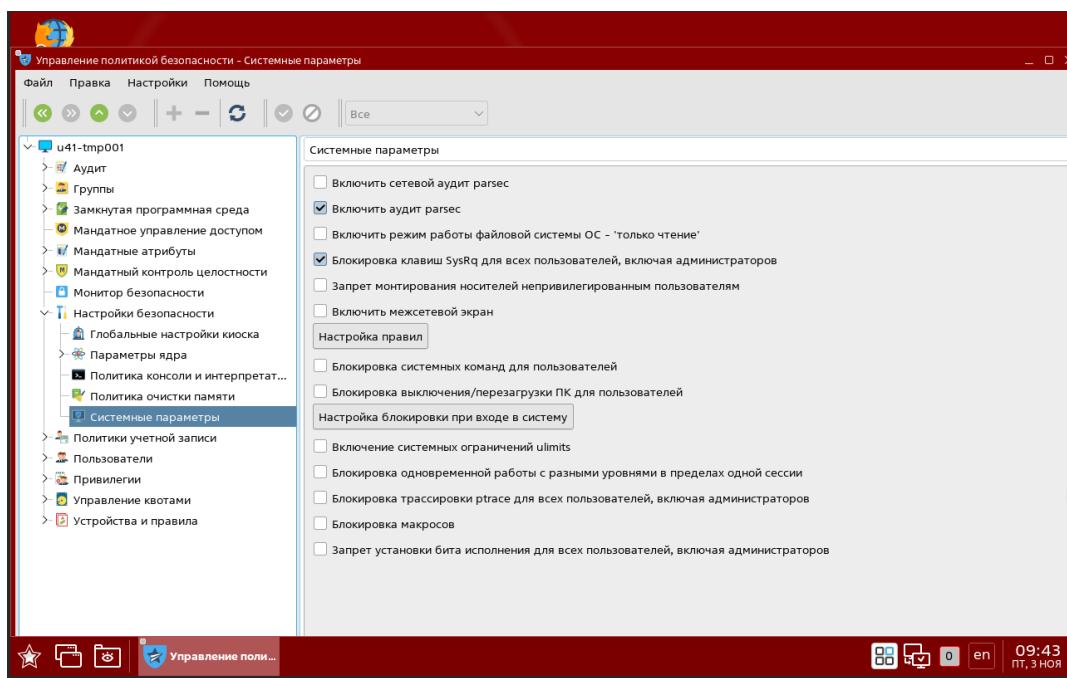


Рисунок 11 – Подраздел «Системные параметры»

- 10) Перейти в подраздел «Политика консоли и интерпретаторов» (рис. 12). Установить флаг в поле «Включить ввод пароля для sudo».

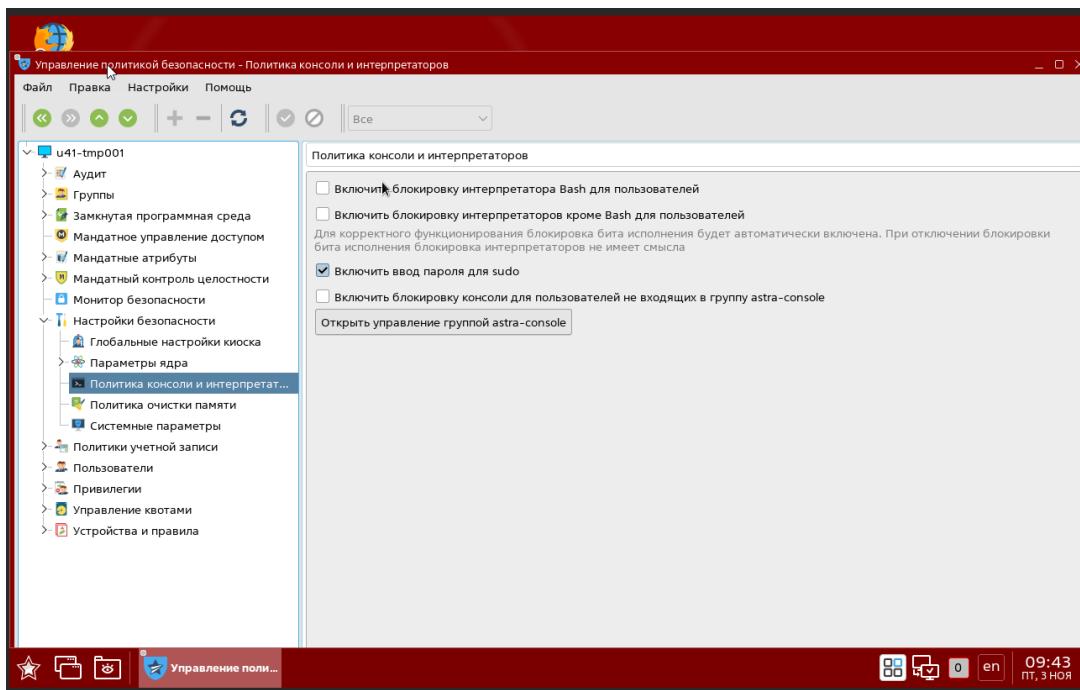


Рисунок 12 – Подраздел «Политика консоли и интерпретаторов»

- 11) Настройка политик безопасности для ОС Astra Linux SE тип защиты «Максимальный» («Смоленск») завершена.

4.2.2 Настройка политик безопасности ОС для типа защиты «Усиленный» («Воронеж»)

Перед установкой ПК «Efros DO» необходимо выполнить следующие настройки ОС Astra Linux SE для типа защиты «Усиленный» («Воронеж»):

- 1) После ввода логина и пароля, при выборе атрибутов безопасности для учетной записи из раскрывающегося списка необходимо выбрать уровень целостности «Высокий» (рис. 13).
- 2) Перейти в меню «Пуск» → «Системные» → «Политика безопасности» (рис. 14).

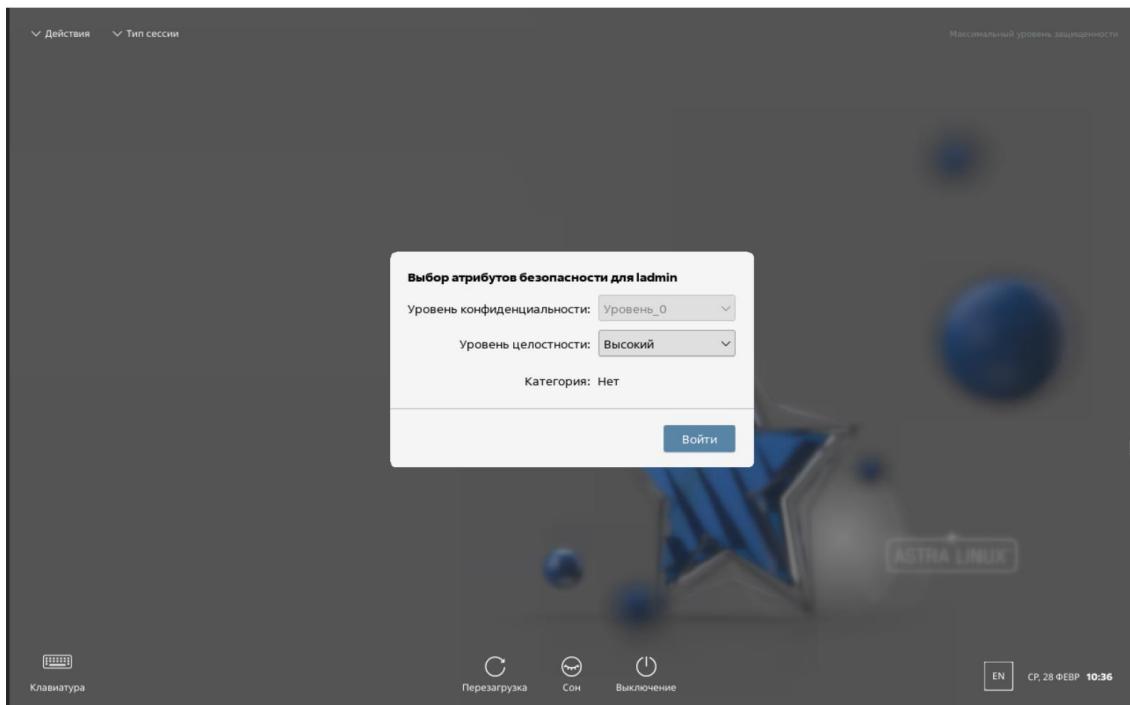


Рисунок 13 – Выбор атрибутов безопасности

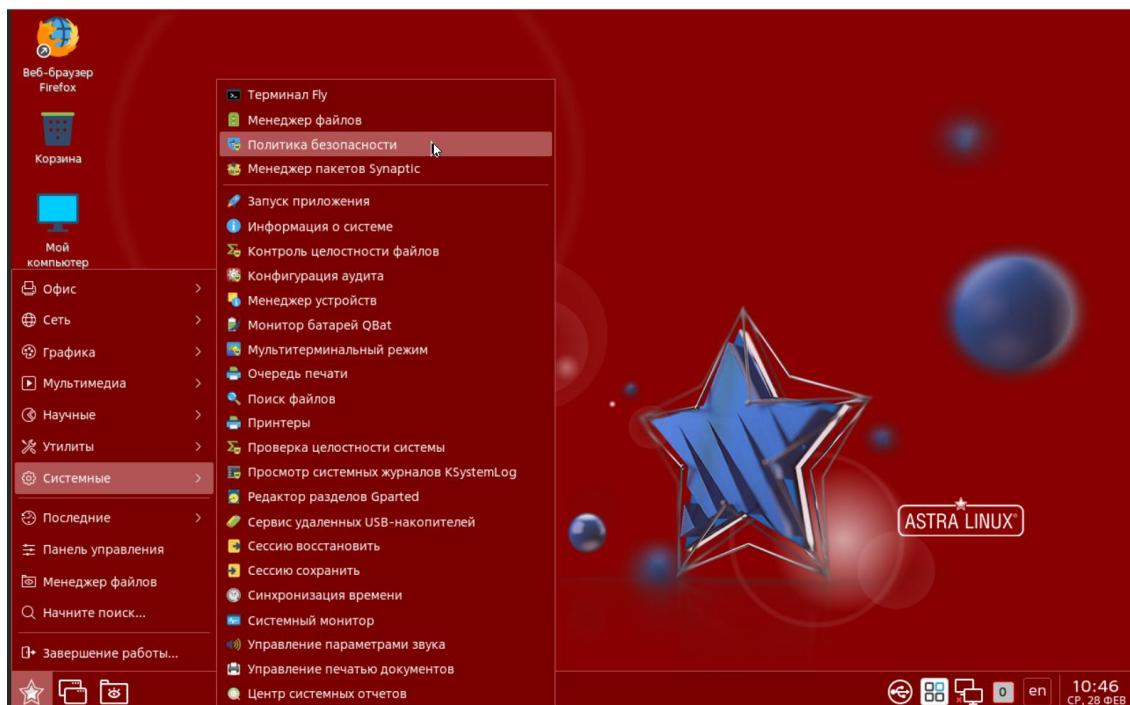


Рисунок 14 – Вкладка «Политики безопасности»

- 3) Ввести пароль администратора ОС (рис. 15).

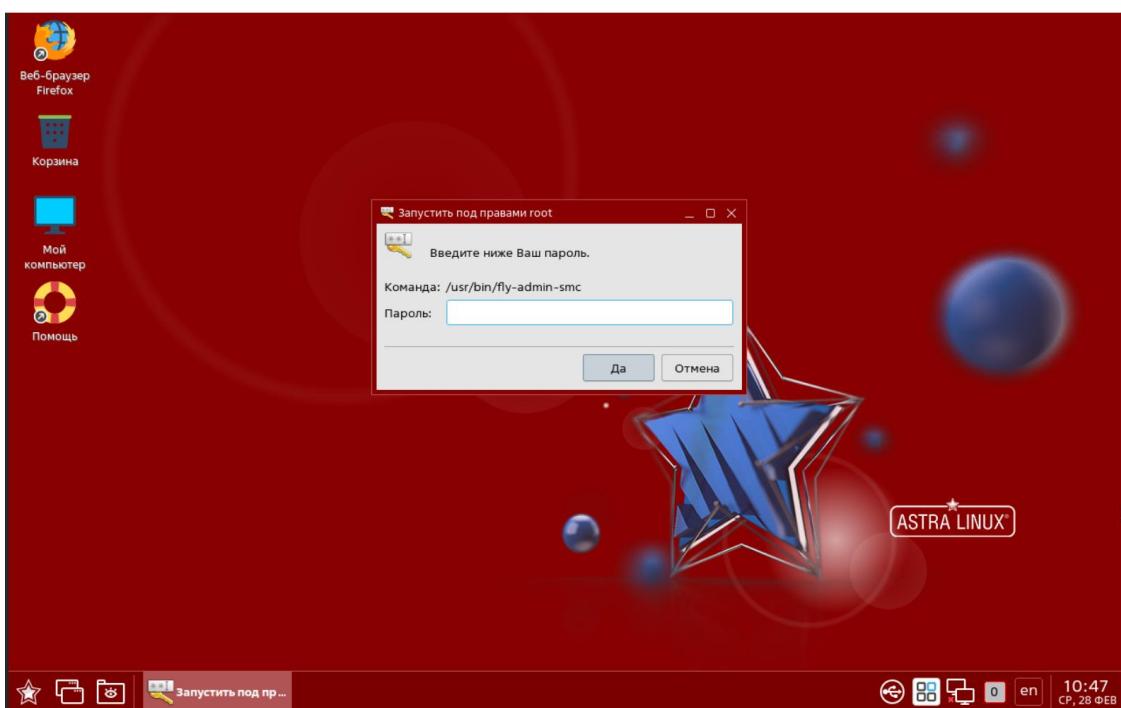


Рисунок 15 – Ввод пароля администратора ОС

- 4) Откроется окно «Управление политикой безопасности – Локальная политика» (рис. 16).

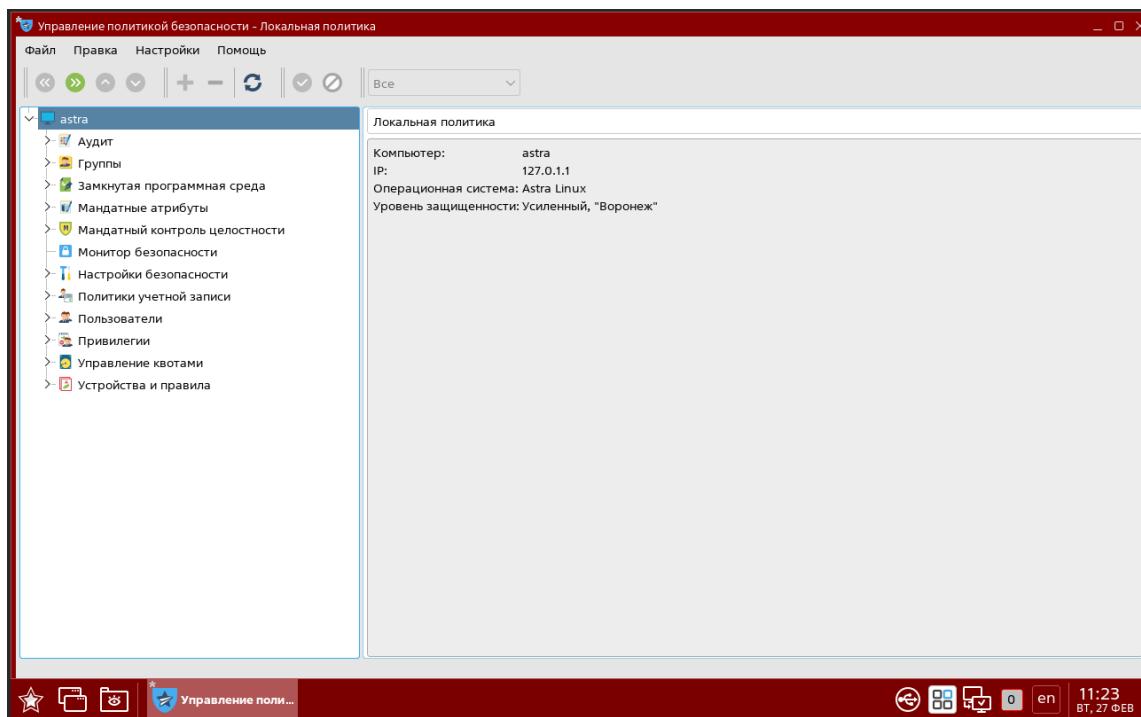


Рисунок 16 – Окно «Управление политикой безопасности – Локальная политика»

- 5) Перейти в раздел «Замкнутая программная среда» (рис. 17).

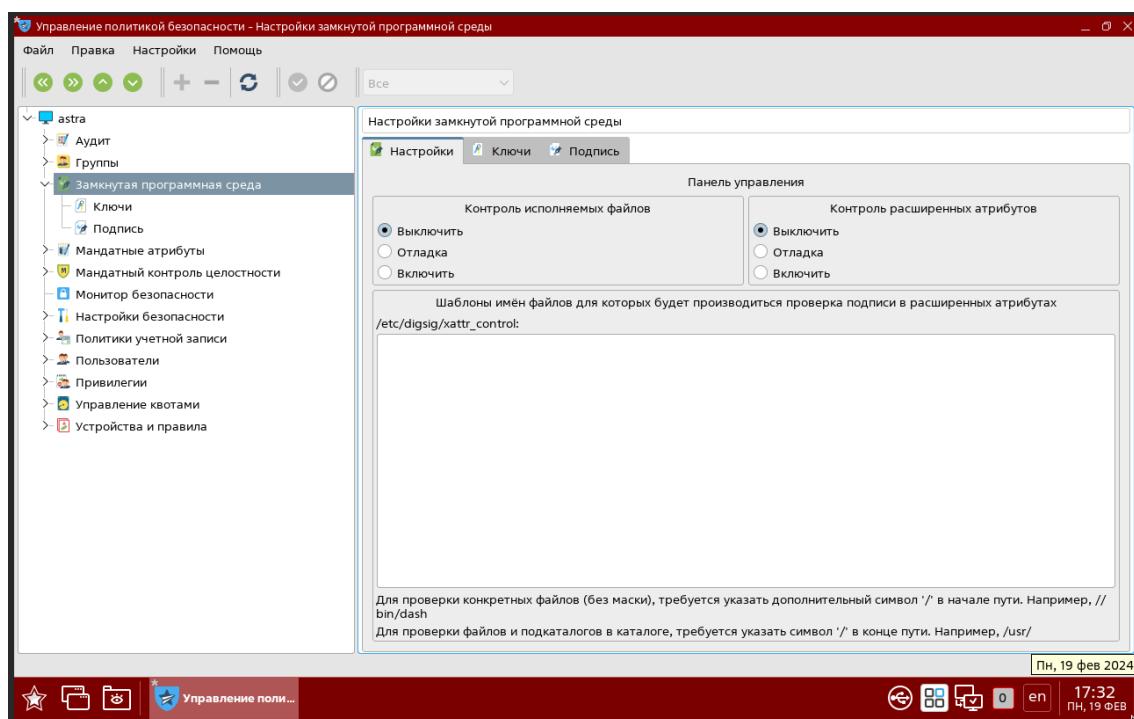


Рисунок 17 – Раздел «Замкнутая программная среда»

По умолчанию функции контроля исполняемых файлов и контроля расширенных атрибутов выключены. Необходимо либо оставить режим «Выключить», либо выбрать режим «Отладка». При использовании режима «Отладка» система будет выводить предупреждения о неподписанных файлах, но запуск их будет разрешен.

Аналогичную настройку можно произвести редактированием конфигурационного файла **/etc/digsig/digsig_initramfs.conf** – для использования отладочного режима для тестирования специального ПО параметру **DIGSIG_ELF_MODE** необходимо установить значение «2»: **DIGSIG_ELF_MODE=2**.

- 6) В разделе «Мандатные атрибуты» изменять настройки не требуется.
- 7) Перейти в раздел «Мандатный контроль целостности» (рис. 18). Убедиться, что в поле «Подсистема Мандатного Контроля Целостности» проставлен флаг.
- 8) Перейти в подраздел «Политика очистки памяти». Флаг в поле «Очистка разделов подкачки» должен отсутствовать (рис. 19).

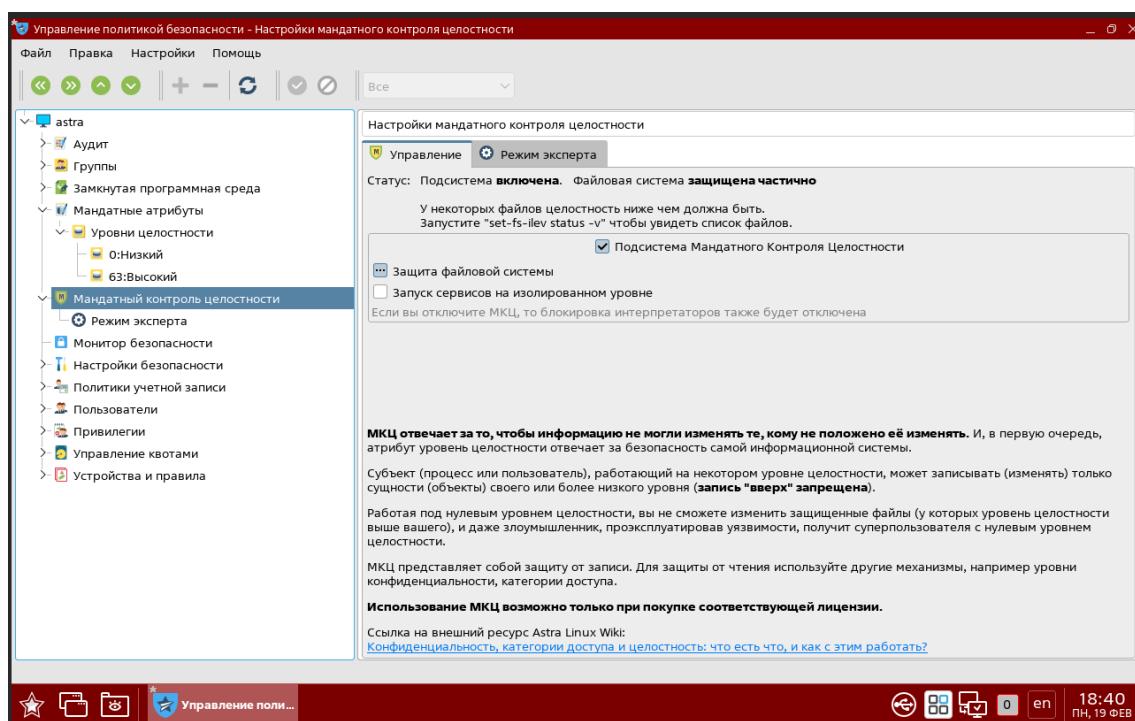


Рисунок 18 – Раздел «Мандатный контроль целостности»

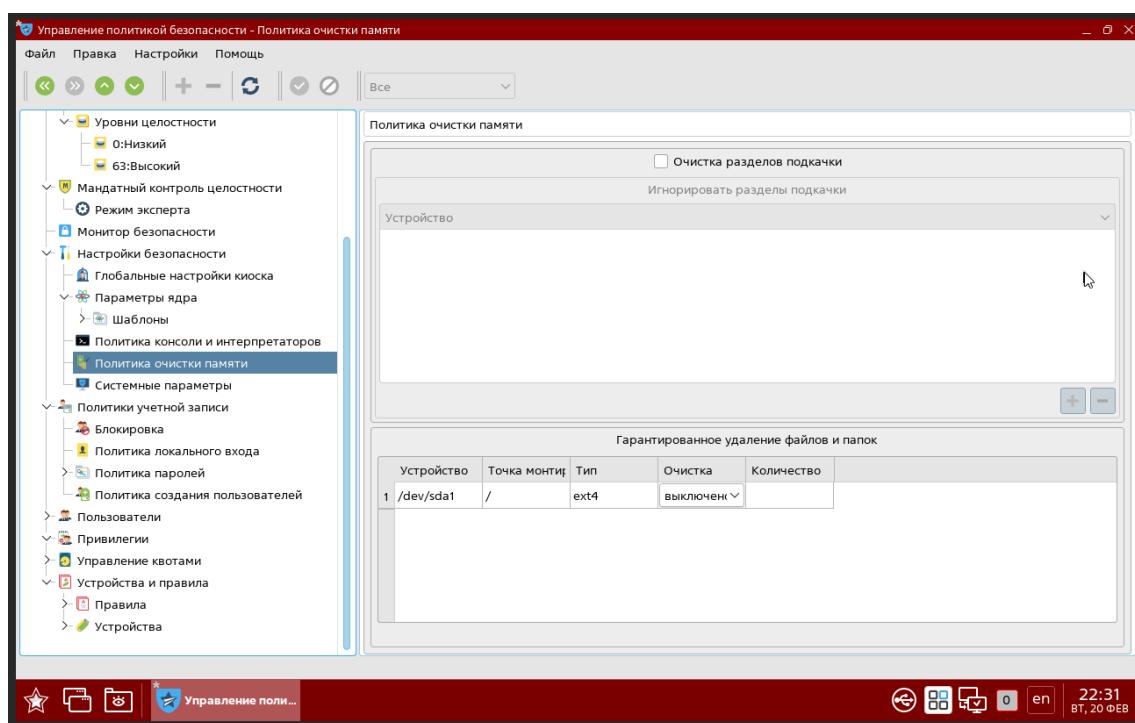


Рисунок 19 – Подраздел «Политика очистки памяти»

- 9) Перейти в подраздел «Системные параметры» (рис. 20). Установить флаги в следующих полях:
- «Блокировка клавиш SysRq для всех пользователей, включая администраторов»;

- «Блокировка трассировки ptrace для всех пользователей, включая администраторов».

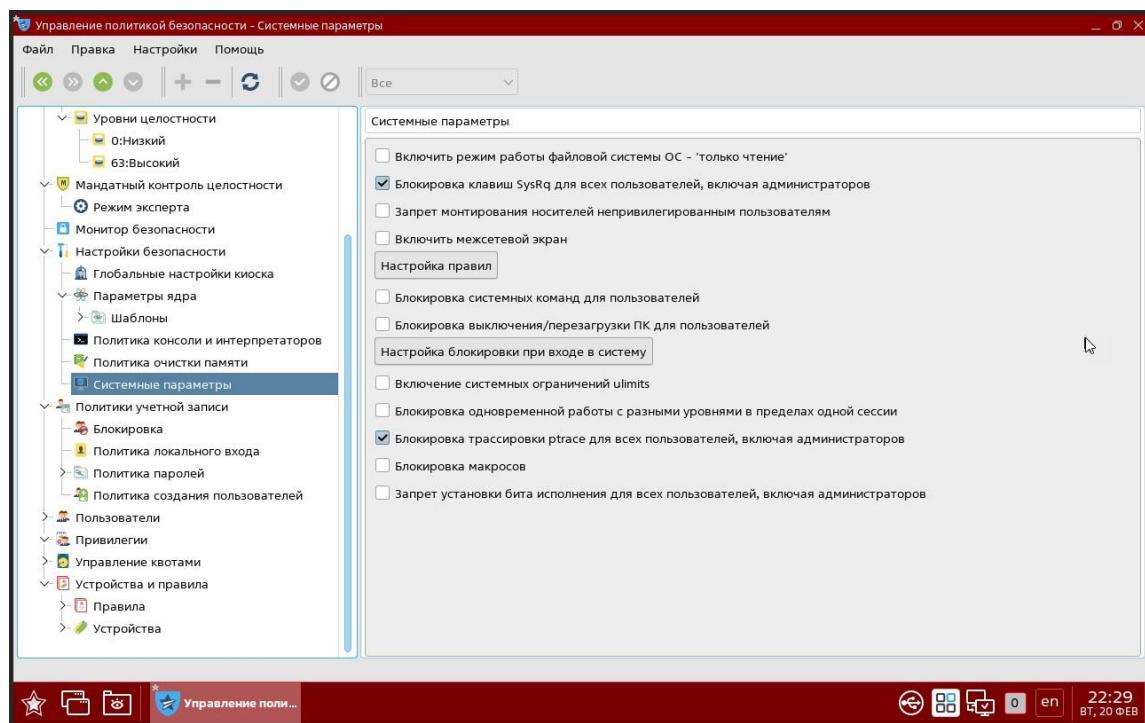


Рисунок 20 – Подраздел «Системные параметры»

- 10) Перейти в подраздел «Политика консоли и интерпретаторов» (рис. 21). Установить флаг в поле «Включить ввод пароля для sudo».

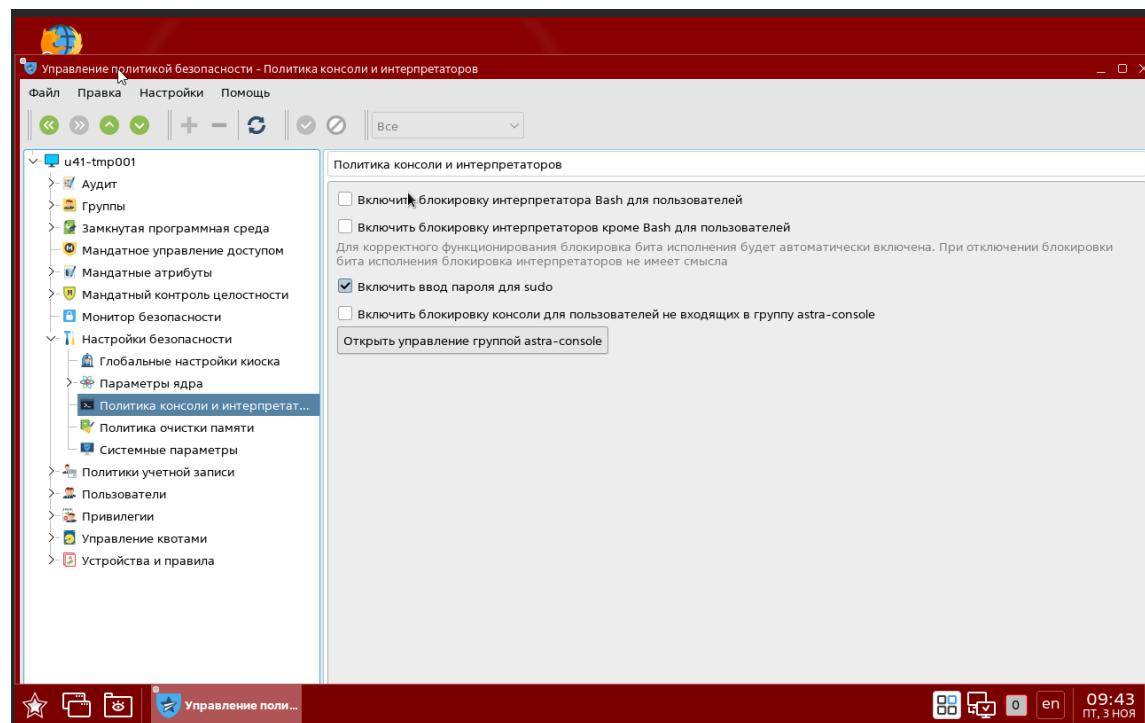


Рисунок 21 – Подраздел «Политика консоли и интерпретаторов»

- 11) Настройка политик безопасности для ОС Astra Linux SE тип защиты «Усиленный» («Воронеж») завершена.

4.2.3 Настройка политик безопасности ОС для типа защиты «Базовый» («Орел»)

Для ОС Astra Linux SE тип защиты «Базовый» («Орел») дополнительные настройки не требуются.

5 Установка, обновление и удаление комплекса на базе Docker-контейнера

5.1 Установка комплекса

Для установки ПК «Efros DO» на базе платформы контейнеризации Docker необходимо скопировать на ЭВМ в домашнюю директорию (например, в */tmp/distrib*) архивы и скрипт с диска, входящие в комплект поставки в соответствии с таблицей 10.

Существует два способа установки комплекса – с использованием встроенной СУБД (по умолчанию) или с подключением к внешней СУБД.

-  В процессе установки команды необходимо вводить от имени суперпользователя *root* либо, используя команду *sudo*.

Для установки комплекса необходимо выполнить следующие действия:

- 1) Запустить скрипт *deploy.sh*:

- при установке со встроенной СУБД «PostgreSQL» – скрипт без дополнительных аргументов, с правами администратора (рис. 22);

```
[root@u41ft79 edo-distr]# sudo ./deploy.sh
```

Рисунок 22 – Запуск скрипта *deploy.sh* без дополнительных аргументов

- с подключением к внешней СУБД (например, СУБД «Jatoba») – скрипт с аргументом *--dbfree* (рис. 23).

```
[root@u41ft79 edo-distr]# sudo ./deploy.sh --dbfree
```

Рисунок 23 – Запуск скрипта *deploy.sh* с аргументом *--dbfree*

Запуск скрипта инициирует следующие процессы:

1. проверка на наличие старых версий ПК «Efros DO» (при наличии, производится их удаление);
 2. распаковка файлов;
 3. запуск процесса установки и запуска ПК «Efros DO».
-
- 2) Если выбран вариант установки с подключением к внешней СУБД, то в процессе установки пользователю необходимо указать следующие параметры (рис. 24):
 - IP-адрес сервера СУБД (в формате 192.168.1.1);

- порт для подключения к серверу СУБД (в формате 5432);
- учетная запись для подключения к БД;
- пароль для подключения к БД;
- имя БД (рекомендуется использовать предложенное по умолчанию имя «edodb»).

! В момент установки комплекса, внешний сервер СУБД должен быть уже доступен по указанным параметрам.

В результате выполнения шага 2 будут созданы три БД ПК «Efros DO»:

1. С указанным именем БД – основная БД комплекса.
2. С указанным именем БД и постфиксом «-сі» – используется микросервисом объектов защиты.
3. С указанным именем БД и постфиксом «-cifw» – используется микросервисом загрузки данных из базы правил межсетевых экранов.

```
[INFO] Необходимо настроить параметры для подключения к внешней СУБД
[INFO] Введите параметры для подключения к внешней СУБД
Введите IP адрес сервера СУБД: 10.116.41.150
[WARNING]: Введен корректный IP адрес сервера СУБД
Введите порт: 5801
Введите логин для доступа к СУБД: postgres
Введите пароль: .
[INFO] Подключение к внешней СУБД успешно!
Введите имя базы данных EDO (по умолчанию - edodb):
[INFO] Настройка подключения к СУБД завершена.
[INFO] EDO будет использовать БД с именами:
edodb, edodb-сі, edodb-cifw
```

Рисунок 24 – Процесс установки. Параметры внешней СУБД

- 3) Если на сервере есть несколько сетевых интерфейсов, необходимо ввести IP-адрес, по которому будет доступен веб-интерфейс (рис. 25).

```
[INFO] Обнаружено несколько сетевых адаптеров.
[MESSAGE] При наличии на хосте нескольких сетевых интерфейсов есть возможность настроить работу EDO только на одном.
[MESSAGE] Введите адрес из приведенного списка или оставьте пустую строку для настроек по умолчанию.
10.116.41.65/24
10.4.0.1/24
Введите адрес в формате X.X.X.X:
[INFO] EDO будет доступен на всех адресах.
[INFO] Проверка конфигурации Docker daemon ...
[INFO] Docker Daemon работает normally.
Введите адрес для интерфейса docker0, в формате <адрес>/<маска>, по умолчанию 172.16.0.1/16: ■
```

Рисунок 25 – Процесс установки. IP-адрес веб-интерфейса при наличии нескольких сетевых интерфейсов

- 4) В процессе установки скрипт запросит адрес сервера, на который производится установка комплекса, в формате <IP-адрес>. При нажатии на клавишу «Enter»

будет выбрано автоматически предложенное значение (рис. 26). При необходимости указать отличный от предложенного адрес, осуществить ввод вручную.

**Ведите адрес сервера ED0, по умолчанию 10.116.41.64:
[INFO] Используются стандартные настройки - 10.116.41.64**

Рисунок 26 – Процесс установки. Данные адреса для установки

- ⓘ В случае если требуется изменить адрес сервера комплекса после установки, необходимо выполнить команду для обновления данных в конфигурационном файле:

```
sudo edoctl --rewrite-host-ip
```

- 5) Затем скрипт запросит данные для настройки внутренней сети docker, в формате <адрес>/<маска>. При нажатии на клавишу «Enter» автоматически выбирается следующая сеть: 172.16.0.1/16 (рис. 27). Если данная сеть занята, то необходимо ввести пользовательские параметры сети.

**[INFO] Первый запуск Efros Defence Operations
Введите сеть для docker, по умолчанию "172.16.0.1/16": 10.20.0.0/16**

Рисунок 27 – Процесс установки. Данные для настройки внутренней сети docker

- 6) Установка программного комплекса завершена, при успешном завершении проверки отобразится сообщение в соответствии с рис. 28.

```
[+] Running 32/32
# Network edo_default                                created
# Volume "edo_data-raddb4"                            created
# Volume "edo_data-dict"                             Created
# Volume "edo_data-raddb"                            Created
# Volume "edo_data-kafka"                           Created
# Volume "edo_data-dict4"                           Created
# Container edo-infr-zookeeper                      Started
# Container edo-store-opensearch                     Started
# Container edo-proxy-service                       Started
# Container edo-ci-service                          Started
# Container edo-infr-kafka                          Started
# Container edo-email-sender-service                Started
# Container edo-schedule-service                   Started
# Container edo-flow-collector-dhcp                Started
# Container edo-guest-portal-service               Started
# Container edo-identity-service                  Started
# Container edo-vulnerability-collector           Started
# Container edo-acs-service                         Started
# Container edo-flow-collector-sflow              Started
# Container edo-report-portal-service             Started
# Container edo-knowledge-base-service            Started
# Container edo-flow-service                        Started
# Container edo-task-portal-service                Started
# Container edo-metrics-collector                 Started
# Container edo-flow-collector                     Started
# Container edo-tacacs                           Started
# Container edo-radius                            Started
# Container edo-license-service                  Started
# Container edo-metrics-service                 Started
# Container edo-so-service                        Started
# Container edo-web-service                      Started
# Container edo-gateway-service                 Started
[INFO] Инициализация завершена. Docker Daemon настроен. Efros-DO запущен.
[INFO] Первый запуск Efros Defence Operations завершен.
```

Рисунок 28 – Установка завершена

Для различных действий с приложением используется shell-скрипт */opt/efros-do/edoctl*. Он запускается с аргументами командной строки (если запуск производится не с правами *root*, то необходима команда *sudo*):

- *./edoctl --ps* – просмотр запущенных сервисов (рис. 29);
- *./edoctl --stop* – остановка всех сервисов (рис. 30);
- *./edoctl --start* – запуск всех сервисов;
- *./edoctl --restart* – перезапуск сервисов (рис. 31);
- *./edoctl --down* – остановка служб приложения, удаление контейнеров;
- *./edoctl --logs <имя-службы>* – просмотр логов docker одной службы (если задано имя службы) либо всего приложения.

```
root@u41ft63:/opt/efros-do# ./edoctl --ps
NAME           COMMAND          SERVICE          STATUS        PORTS
edo-acs-service "/docker-entrypoint..." edo-acs-service  running (unhealthy)  5000:5001/tcp
edo-ci-service  "/bin/bash -c 'efros_'" edo-ci-service   running (starting)  0.0.0.0:162→162/udp, 0.0.0.0:514→514/udp, 0.0.0.0:1468→1468/tcp, 0.0.0.0:20002→20002/tcp
edo-email-sender-service ".SC.EmailSenderSer..." edo-email-sender-service running (healthy)  80/tcp
edo-flow-collector-dhcp "/app/efros/edo-flow..." edo-flow-collector-dhcp running
edo-flow-collector-sflow "/docker-entrypoint..." edo-flow-collector-sflow running
edo-flow-service    "/bin/bash -c 'while..." edo-flow-service   running (unhealthy)  80/tcp
edo-gateway-service "/Voltron.Gateway.W..." edo-gateway-service running (healthy)  80/tcp
edo-guest-portal-service "/dockr-entrypoint..." edo-guest-portal-service running
edo-identity-service ".SC.Identity.Api" edo-identity-service running (healthy)  80/tcp
edo-infr-kafka     "/etc/confluent/dockr..." edo-infr-kafka    running (healthy)  9992/tcp
edo-license-updater "/etc/confluent/dockr..." edo-license-updater running (healthy)  8888/tcp
edo-knowledge-base-service ".SC.KnowledgeBase..." edo-knowledge-base-service running (healthy)  80/tcp
edo-license-service ".SC.License.Api" edo-license-service running (healthy)  80/tcp
edo-metrics-collector ".SC.EventsCollecto..." edo-metrics-collector running
edo-metrics-service ".SC.AnalizedMetrics" edo-metrics-service running
edo-proxy-service   "/dockr-entrypoint..." edo-proxy-service  running (healthy)  0.0.0.0:443→443/tcp, 0.0.0.0:5802→5802/tcp
edo-radius         "/lib/systemd/system..." edo-radius       running (unhealthy)  0.0.0.0:1812→1813→1812-1813/udp
edo-report-portal-service ".Reporting.WebAp..." edo-report-portal-service running (healthy)  80/tcp
edo-schedule-service "/Voltron.Schedule..." edo-schedule-service running (healthy)  80/tcp
edo-so-service      ".SC.SecurityObject..." edo-so-service    running (healthy)  80/tcp
edo-store-opensearch "/opensearch-docker..." edo-store-opensearch running (healthy)  127.0.0.1:5805→9200/tcp
edo-tacacs          "/lib/systemd/system..." edo-tacacs       running
edo-task-portal-service ".TaskPortal.WebApi" edo-task-portal-service running (unhealthy)  80/tcp
edo-vulnerability-collector ".SC.Vulnerabilit..." edo-vulnerability-collector running (healthy)  80/tcp
edo-web-service     "./Voltron.WebApi" edo-web-service   running (healthy)  80/tcp
root@u41ft63:/opt/efros-do#
```

Рисунок 29 – Просмотр запущенных сервисов

```
root@u41ft63:/opt/efros-do# ./edoctl --stop
[+] Running 3/16
  " Container edo-tacacs           Stopping            3.2s
  # Container edo-flow-collector-dhcp  Stopped             2.7s
  " Container edo-email-sender-service Stopping            3.2s
  " Container edo-vulnerability-collector Stopping            3.2s
  " Container edo-ci-service          Stopping            3.2s
  " Container edo-gateway-service    Stopping            3.2s
  " Container edo-knowledge-base-service Stopping            3.1s
  " Container edo-guest-portal-service Stopping            3.1s
  " Container edo-report-portal-service Stopping            3.1s
  " Container edo-task-portal-service  Stopping            3.1s
  # Container edo-flow-collector-sflow  Stopped             1.4s
  " Container edo-metrics-collector  Stopping            3.1s
  " Container edo-schedule-service   Stopping            3.1s
  " Container edo-radius             Stopping            3.1s
  # Container edo-flow-collector     Stopped             1.4s
  " Container edo-proxy-service      Stopping            3.1s
root@u41ft63:/opt/efros-do#
```

Рисунок 30 – Остановка всех сервисов

```
root@u41ft63:/opt/efros-do# ./edoctl --restart
[+] Running 9/22
  # Container edo-proxy-service      Started            0.7s
  # Container edo-store-opensearch  Started            0.9s
  # Container edo-infr-zookeeper   Started            1.0s
  # Container edo-ci-service        Started            0.6s
  # Container edo-infr-kafka       Started            0.5s
  # Container edo-flow-collector-dhcp Started            1.4s
  # Container edo-task-portal-service Restarting        2.5s
  # Container edo-acs-service      Restarting        2.5s
  # Container edo-identity-service Started            1.3s
  # Container edo-report-portal-service Restarting        2.5s
  # Container edo-flow-service     Restarting        2.5s
  # Container edo-metrics-collector Restarting        2.5s
  # Container edo-vulnerability-collector Restarting        2.5s
  # Container edo-knowledge-base-service Restarting        2.5s
  # Container edo-schedule-service  Restarting        2.5s
  # Container edo-guest-portal-service Restarting        2.5s
  # Container edo-flow-collector-sflow Started            0.4s
  # Container edo-email-sender-service Started            2.3s
  # Container edo-license-service   Restarting        1.3s
  # Container edo-web-service      Restarting        1.3s
  # Container edo-so-service       Restarting        1.3s
  # Container edo-metrics-service  Restarting        1.3s
root@u41ft63:/opt/efros-do#
```

Рисунок 31 – Перезапуск всех сервисов

- 7) После установки доступен просмотр списка запущенных сервисов, их состояния и параметров.

! В случае отображения неверного состояния сервисов необходимо перезагрузить комплекс. Для этого выполнить следующие шаги:

1. Остановить комплекс, выполнив команду:

```
sudo /opt/efros-do/edoctl --down
```

2. Перезагрузить docker, выполнив команду:

```
sudo systemctl restart docker
```

3. Запустить комплекс, выполнив команду:

```
sudo /opt/efros-do/edoctl --start
```

5.2 Перенастройка сети

Для настройки сетевого интерфейса docker0 и подсети, в которой работают контейнеры комплекса, необходимо выполнить следующие действия:

- 1) Перейти **cd /opt/efros-do**.
- 2) Выполнить остановку контейнеров **./edoctl --down**.
- 3) Удалить неиспользуемые сети **docker network prune -f**.
- 4) Изменить сеть в конфигурации **./edoctl --init**.
- 5) Ввести пользовательские параметры сети в формате «10.0.0.0/16» или оставить по умолчанию.

5.3 Обновление комплекса на базе Docker-контейнера

5.3.1 Требования при обновлении комплекса

Для корректного обновления комплекса на базе Docker-контейнера необходимо выполнение следующих требований:

- 1) Перед обновлением комплекса рекомендуется сделать резервную копию БД системы через раздел «Настройки» → «Резервные копии» (подробнее см. документ «Руководство пользователя. Часть 1. Настройка и администрирование»).
- 2) При использовании внешней СУБД PostgreSQL версии 13 необходимо

выполнить обновление до версии 14 или выше.

- 3) Перед обновлением необходимо вывести комплекс из домена. После завершения обновления при необходимости ввести комплекс в домен.

-  При обновлении комплекса следует учитывать, что время запуска сервиса `edo-ci-service` увеличено (до часа). Время зависит от количества шифруемых данных БД (паролей, ключей).

5.3.2 Обновление комплекса

Обновление ПК «Efros DO» осуществляется после предоставления нового дистрибутива разработчиком. Процесс обновления аналогичен процессу установки программного комплекса:

- 1) Скопировать файлы `efros-do_<номер релиза>.tar.gz` и `deploy.sh` в одну директорию.
- 2) Для обновления комплекса со встроенной БД – запустить скрипт `deploy.sh` без дополнительных аргументов, с правами администратора.
- 3) Для обновления комплекса с подключенной внешней БД запустить скрипт `deploy.sh` с аргументом `--dbfree`. В процессе обновления пользователю необходимо будет повторно указать следующие параметры:
 - IP-адрес сервера СУБД (в формате 192.168.1.1);
 - порт для подключения к серверу СУБД (в формате 5432);
 - учетную запись для подключения к БД;
 - пароль для подключения к БД;
 - имя используемой БД.

-  В процессе обновления ПК «Efros DO» выполняется шифрование чувствительных данных в базе данных.

Рекомендуется предварительно выполнить резервное копирование базы данных.

После обновления для сохранения ключа шифрования рекомендуется сделать резервную копию значения переменной `host_machine_id` из `/opt/efros-do/.env`.

Для этого можно использовать команду:

```
grep host_machine_id /opt/efros-do/.env | cut -d '=' -f 2 > $HOME/host_machine_id
```

Для отмены обновления комплекса необходимо ввести «N» или «п».

Для продолжения обновления комплекса необходимо ввести «Y» или «у».

- 4) Проверить версию базы платформы контейнеризации Docker. При необходимости произвести обновление Docker до v.25 или выше (для ОС Astra Linux SE – docker.io, для РЕД ОС – docker-ce).
- 5) Произвести установку новой версии комплекса аналогично подразделу 5.1 данного документа.

! В момент обновления комплекса, должны отсутствовать другие внешние подключения к обновляемой БД (выбранной на шаге 3).

- 6) При обновлении комплекса производится автоматическая миграция данных. Перечень данных миграции приведен в пункте 5.3.3.
- 7) После завершения миграции необходимо перезапустить комплекс, выполнив следующие команды:

```
sudo /opt/efros-do/edoctl --down
sudo /opt/efros-do/edoctl --start
```

5.3.3 Миграция данных при обновлении комплекса

Миграция данных при обновлении комплекса до актуальной версии производится автоматически.

Перечень элементов миграции и описание миграции приведены в таблице 15. Также указана версия комплекса, с которой производится обновление.

Таблица 15 – Элементы миграции при обновлении комплекса

Элементы миграции	Описание миграции	Предыдущая версия ПК «Efros DO»
Сетевые пользователи и метки	Для сетевых пользователей и меток будут применены следующие изменения: <ul style="list-style-type: none">• к названиям групп сетевых пользователей и их меток добавится префикс «group_», при наличии дубликатов меток, к названиям меток будет добавлен постфикс с порядковым номером;• сетевым пользователям типа «локальный» присваиваются метки, созданные для групп, в которые он входил ранее	2.12 или ниже
Словари	Для словарей будут применены следующие изменения: <ul style="list-style-type: none">• в виртуальный словарь «NetUsers» добавится новый атрибут «Tag» – метка сетевого пользователя;• словарь «NetUserGroups» будет удален;	2.12 или ниже

Элементы миграции	Описание миграции	Предыдущая версия ПК «Efros DO»
	<ul style="list-style-type: none">из словаря «NetUsers» будут удалены сетевые пользователи типа «LDAP группа»	
Наборы политик (сетевые пользователи)	<p>В условиях созданных политик/шаблонах будут применены следующие изменения по сетевым пользователям:</p> <ul style="list-style-type: none">в условиях политик название словаря/атрибута «NetUserGroups/Name» заменено на «NetUsers/Tag»;в условиях политик/шаблонов «NetUserGroups/Name {оператор: «равно» или «не равно»} <группа сетевых пользователей>» будут заменены название словаря/атрибута (см. выше) и значение <группа сетевых пользователей> на <название метки группы, созданной при миграции>;условия политик доступа «NetUserGroups/Name {оператор отличный от «равно» или «не равно»} <группа сетевых пользователей>» и условия, в которых в качестве значения атрибута выбран атрибут «NetUserGroups/Name», будут удалены из правила/условий срабатывания политики. Статус политики или правила аутентификации/ авторизации – «Выключено»;в условиях политик названия словаря и атрибута «AdDomainGroups/Name» будут изменены на изменено на «<Название AD>/Group»;в условиях политик названия словаря и атрибута «NetUsers/Name» будут изменены на изменено на «<Название LDAP>/Group»	2.12 или ниже
Наборы политик (источники данных)	В условиях созданных политик будут применены следующие изменения в названиях словарей и атрибутов: <ul style="list-style-type: none">«AdDomainGroups/Name» изменено на «<Название AD>/Group»;«NetUsers/Name» изменено на «<Название LDAP>/Group»	2.12 или ниже
Наборы политик (правила аутентификации)	<p>В политиках изменен порядок обхода правил аутентификации.</p> <p>В правилах аутентификации удалена возможность перехода к проверке следующего правила. Теперь выполняется либо отклонение запроса устройства на аутентификацию, либо переход к авторизации</p>	2.12 или ниже
Источники данных: Active Directory и LDAP	В источниках данных к названиям соединений Active Directory и LDAP добавляются префиксы «ad_» и «ldap_»	2.12 или ниже

Элементы миграции	Описание миграции	Предыдущая версия ПК «Efros DO»
Имя БД микросервиса объектов защиты	Изменение имени БД микросервиса объектов защиты на имя: <имя используемой БД>-ci	2.12 или ниже
Заявки раздела «Центр задач»	Для маршрутов активных заявок, в котором присутствует объект «Уведомление», будет выводиться уведомление об ошибке. Для устранения ошибки необходимо удалить маршрут и создать заново	2.12
Заявки раздела «Центр задач»	Статусы активных заявок будут переведены в статус «Закрыта»	2.12
Данные раздела «Центр задач» (в том числе события)	Очищение БД раздела «Центр задач» (в том числе события)	2.11 или ниже
SNMP профили	Перемещение SNMP профилей из БД контроля устройств в БД сервиса объектов защиты	2.10 или ниже

При обнаружении проблем автоматической миграции доступна команда ручного запуска миграции:

```
sudo /opt/efros-do/edoctl --2_13-migration
```

После завершения миграции необходимо перезапустить комплекс.

5.4 Удаление изделия

Для удаления приложения необходимо выполнить одну из следующих команд:

- команду ***edoctl --uninstall*** для частичного удаления комплекса (без потери БД) (рис. 32);
- команду ***edoctl --purge-all*** для полного удаления комплекса (рис. 33).

```
root@u41ft66:/opt/efros-do# edoctl --uninstall
```

Рисунок 32 – Запуск команды для частичного удаления

```
root@u41ft66:/opt/efros-do# edoctl --purge-all
```

Рисунок 33 – Запуск команды для полного удаления

! При полном удалении ПК «Efros DO» также будет удален ключ шифрования базы данных.

Это означает, что данный экземпляр БД невозможно будет использовать при новой установке комплекса, данные будут утеряны.

Если при новой установке необходимо будет использовать текущий экземпляр БД, то до удаления необходимо сохранить значение переменной *host_machine_id* из */opt/efros-do/.env*.

Для этого можно использовать команду:

```
grep host_machine_id /opt/efros-do/.env | cut -d '=' -f 2 > $HOME/host_machine_id
```

Также для корректной работы сервиса иерархии необходимо сохранить значение переменной *hierarchy_guid* из */opt/efros-do/.env*.

Для этого можно использовать команду:

```
grep hierarchy_guid /opt/efros-do/.env | cut -d '=' -f 2 > $HOME/hierarchy_guid
```

Затем необходимо вставить значения *host_machine_id* и *hierarchy_guid* в */opt/efros-do/.env* при новой установке перед запуском скрипта *./deploy.sh*.

Если файл */opt/efros-do/.env* не существует, можно воспользоваться следующим списком команд:

```
mkdir -p /opt/efros-do
cat << EOF > /opt/efros-do/.env
EDO_VERSION=2.13
host_machine_id=$(cat $HOME/host_machine_id)
hierarchy_guid=$(cat $HOME/hierarchy_guid)
EOF
```

Для отмены удаления комплекса необходимо ввести «N» или «n».

Для продолжения удаления комплекса необходимо ввести «Y» или «у».

В процессе удаления на экране будет отображаться информация об удалении файлов и каталогов в соответствии с рисунками 34, 35.

```
Хотите продолжить? [Д/Н]
(Чтение базы данных ... на данный момент установлено 49290 файлов и каталогов.)
Удаляется efros-do (1.4.2) ...
Stopping edo-gateway-service    ... done
Stopping edo-license-service   ... done
Stopping edo-so-service        ... done
Stopping edo-metrics-service   ... done
Stopping edo-web-service       ... done
Stopping edo-tacacs            ... done
Stopping edo-radius             ... done
Stopping edo-acsservice         ... done
Stopping edo-identity-service  ... done
Stopping edo-ci-service        ... done
Stopping edo-flow-service      ... done
Stopping edo-flow-collector-sflow ... done
Stopping edo-flow-collector    ... done
Stopping edo-schedule-service  ... done
Stopping edo-metrics-collector ... done
Stopping edo-store-postgres    ... done
Stopping edo-infr-kafka         ... done
Stopping edo-store-elasticsearch ... done
Stopping edo-infr-zookeeper    ... done
Stopping edo-proxy-service     ... done
Going to remove edo-gateway-service, edo-license-service, edo-so-service, edo-metrics-service, edo-web-service, edo-tacacs, edo-radius, edo-acsservice, edo-identity-service, edo-ci-service, edo-flow-service, edo-flow-collector-sflow, edo-flow-collector, edo-schedule-service, edo-metrics-collector, edo-store-postgres, edo-infr-kafka, edo-store-elasticsearch, edo-infr-zookeeper, edo-proxy-service
Removing edo-gateway-service    ... done
Removing edo-license-service   ... done
Removing edo-so-service        ... done
Removing edo-metrics-service   ... done
Removing edo-web-service       ... done
Removing edo-tacacs            ... done
Removing edo-radius             ... done
Removing edo-acsservice         ... done
Removing edo-identity-service  ... done
Removing edo-ci-service        ... done
Removing edo-flow-service      ... done
Removing edo-flow-collector-sflow ... done
Removing edo-flow-collector    ... done
Removing edo-schedule-service  ... done
Removing edo-metrics-collector ... done
Removing edo-store-postgres    ... done
Removing edo-infr-kafka         ... done
Removing edo-store-elasticsearch ... done
Removing edo-infr-zookeeper    ... done
Removing edo-proxy-service     ... done
-
```

Рисунок 34 – Процесс удаления файлов и каталогов (начало)

```
Deleted: sha256:688f65ce3a33d5aae47eb089c6f608c4026364ddaba08f87f9f94b4c22b995dc
Deleted: sha256:291f6e44771a7b4399b0c6fb40ab4fe0331ddf76eda11080f052b003d96c7726
Untagged: edo-infr-kafka:5.5.0
Untagged: localhost:80/edo-infr-kafka:5.5.0
Untagged: localhost:80/edo-infr-kafka@sha256:ad865d13e75acc38a252a6641213d5b1f86cd1ce74a96c5a18ef64853f7fee2b
Deleted: sha256:7d3fff76bebeec000934e06652b732d8affe94a6770e7f603dc538da3e139472
Deleted: sha256:f642031e18cfbb570bf4d1a12665f8cea1e7601de8bf2f8335ce49bba2b5222
Deleted: sha256:91475761aec75919d22452098f684a34ee5c0244549bd85d7f343ad56833911c
Deleted: sha256:283dd1b3aa373ca8db49275d08c794ad8593809aaab4c1995df52e8bd6d1f4db
Deleted: sha256:2bf35c488a79e4d5fc62cf3b2241b7a7be7b2359aa6fb034333d1c8c1d144ed2
Untagged: edo-infr-zookeeper:5.5.0
Untagged: localhost:80/edo-infr-zookeeper:5.5.0
Untagged: localhost:80/edo-infr-zookeeper@sha256:6e33666a21ed552cf4a6b9096a2fa94c954a60c17ec470a20f0422b9cbaa6a26
Deleted: sha256:124ff6469e3d01eb72c58afa0668a5a19f7bf0318355e98847a4b4e28fcfdbea
Deleted: sha256:7c1b2a63d63d4e8a4bc26812347923d30df54e09f0d69ba09633cdc590e6fd37
Deleted: sha256:cf7c6836cab0ee5a22bf97d37d3cc5ba22658f8248de66dbe9e045bbb3ed4fcf
Deleted: sha256:5ae1074330ca9e55e23f527aa4323f440379637b6ee79c815354a09609b4e2be
Deleted: sha256:d9ad8c636ab061323a045478cbb0b0aab95ed152d6b42e4d7696f658bf1a9b1d
Deleted: sha256:6966a3782a9b048a87507999bca0503e5971f5c83164ce8ce775dfeffcc7f3d29
Deleted: sha256:a8ff4211732a595e112b39fd1c98459406ef1a3aae94b743df60d1996ca19bc75
Deleted Volumes:
edo_data-logs-secondary
edo_data-pg
edo_data-raddb-ssl
edo_data-zookeeper
edo_data-cl-modules
edo_data-dict
edo_data-docker-ssl
edo_data-kafka-secrets
edo_data-db-backup
edo_data-logs
edo_data-raddb
edo_data-www-ssl
edo_data-raddb-secondary
edo_data-zookeeper-log
edo_data-db-acs
edo_data-dict-secondary
edo_data-kafka
edo_data-license
edo_data-tac-plus-secondary
edo_data-zookeeper-secrets
edo_data-cl-configurations
edo_data-raddb-ssl-secondary
edo_data-samba
edo_data-tac-plus

Total reclaimed space: 1.305GB
administrator@efros-do:"$ _
```

Рисунок 35 – Процесс удаления файлов и каталогов (продолжение)

6 Установка, обновление и удаление комплекса на базе Kubernetes

ПК «Efros EDO» может работать в режиме геораспределенного отказоустойчивого кластера, то есть на распределенной инфраструктуре из нескольких территориально удаленных данных центров (ЦОД).

Это позволяет сохранять работоспособность в случае выхода из строя одного из ЦОД, а также балансировать нагрузку и обеспечивать выделение из комплекса модулей для внешнего доступа.

Если один сервер выходит из строя, остальные серверы автоматически перенимают его функции, обеспечивая надежный и бесперебойный доступ к ресурсам и данным.

При восстановлении работоспособности узла происходит согласование узлов кластера, службы ПК «Efros DO» и кластер продолжает работать в штатном режиме.

Отказоустойчивость кластера ПК «Efros DO» реализовывается на базе инфраструктуры Kubernetes.



Установка комплекса на базе Kubernetes может производиться на различном количестве ЦОД:

- на одном ЦОД – рекомендуется 3 и более виртуальных машин (узлов);
- на трех ЦОД – рекомендуется 5 и более виртуальных машин (узлов).



Запускать установку комплекса необходимо с Nexus-хоста (см. пункт 6.3.2).



Скрипты необходимо запускать с правами администратора.

6.1 Отказоустойчивость и катастрофоустойчивость кластера

Отказоустойчивость и катастрофоустойчивость кластера ПК «Efros DO» обеспечивается на уровне инфраструктуры и требуют развертывания продукта с рядом условий:

- наличие резервных линий связи для обеспечения связности ЦОД;
- независимые друг от друга ЦОД для обеспечения катастрофоустойчивости;
- кворум узлов продукта для обеспечения отказоустойчивости, корректной работы и восстановления функций комплекса в случае отказа.

Наличие резервных линий связи влияет на управление кластером и взаимодействие отдельных ЦОД. При отсутствии связности между всеми ЦОД комплекс продолжает работать в полном объеме, однако управление кластером, репликация и синхронизация данных невозможны. Связность может обеспечиваться в любом порядке, однако все ЦОД должны включаться в неразрывную цепь.

При восстановлении связности комплекс обеспечивает восстановление функций в

полном объеме.

Распределение узлов между ЦОД осуществляется на основе физической инфраструктуры. Если используется только два физически разделённых ЦОД без дополнительного узла в третьей зоне, существует высокий риск рассинхронизации узлов и потери управления кластером.

Отказоустойчивость и катастрофоустойчивость обеспечиваются резервированием ЦОД и узлов с учетом кворума, необходимого для платформы.

При равном количестве узлов на каждом ЦОД, кворум рассчитывается по формуле $n/m+1$, где n – общее количество узлов, m – количество ЦОД. Катастрофоустойчивость обеспечивается при сохранении работоспособности $n/2+1$ ЦОД и/или узлов на них.

Таким образом, если комплекс должен обеспечивать работу при отказе 3 узлов – рекомендуется общее количество узлов не менее 7 для 3 ЦОД.

Для гарантированного сохранения работоспособности кластера необходимо определить необходимый параметр катастрофоустойчивости с учетом возможного количества отказавших в развернутом ПК «Efros DO» узлов и на его основе вычислить необходимое число узлов и ЦОД.

6.2 Варианты обеспечения отказоустойчивости кластера

ПК «Efros DO» поддерживает два варианта обеспечения отказоустойчивости кластера:

- 1) Использование приложения **keepalived** и веб-сервера **haproxy** – по умолчанию установка для кластера, узлы которого расположены в одной подсети (L2 сети). Такое решение подходит для развертывания кластера ПК «Efros DO» в рамках одного ЦОД (где ЦОД считается единым объектом отказа, являющимся сервером в отдельной от других подсети).

При установке кластера необходимо учитывать, что рекомендуемое количество master-узлов должно составлять нечетное количество – 3, 5 и тд. Подробное описание работы с узлами кластера приведено в подразделе 6.6.

- 2) Использование GSLB решения для работы кластера в разных подсетях или реализации геораспределенного кластера в рамках нескольких ЦОД. Для выбора данного варианта отказоустойчивости необходимо установить соответствующие настройки в процессе установки кластера.

При установке комплекса следует учитывать кворум базы данных **etcd** и кворум ЦОД. Описание формул подсчета кворума приведены ниже.

6.2.1 Использование keepalived и haproxy

Приложение **keepalived** предназначено для создания виртуального IP-адреса. Балансировка трафика между компонентами Kubernetes выполняется **haproxy**.

С учетом кворума для 3 узлов кластера достаточно использовать 2 узла для установки **keepalived** и **haproxy**.

Схема отказоустойчивого кластера с горизонтальным масштабированием на 1 ЦОД приведена на рис. 36.

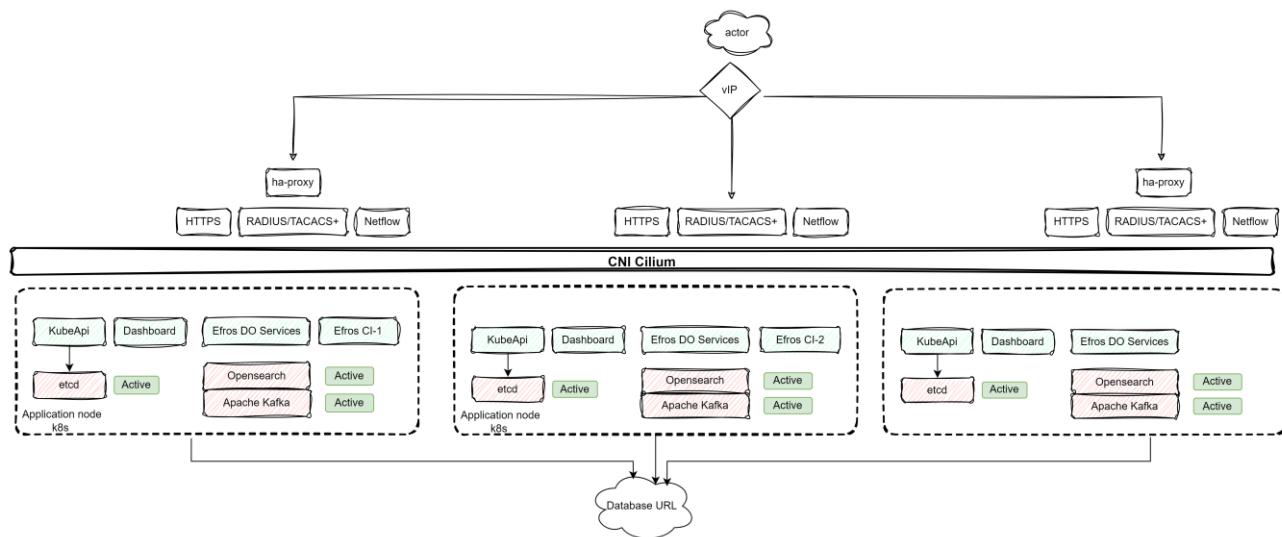


Рисунок 36 – Схема кластера с использованием keepalived и haproxy

Так как условие кворума **etcd** не выполняется при падении двух узлов, управление кластером Kubernetes становится недоступно.

При установке узлов кластера в разных подсетях узлы с **keepalived** и **haproxy** должны находиться в одной подсети. Для разных подсетей рекомендуется использовать GSLB решение.

6.2.2 Использование GSLB решения

При использовании GSLB решения с заданными параметрами в ПК «Efros DO» выполняется автоматическая проверка доступности DNS-адресов узлов кластера.

По результатам проверки выполняется исключение неработоспособных узлов из числа возможных ответов на запрос. В ответе на запрос сервисов из состава ПК «Efros DO» будет содержаться адрес работоспособного на данный момент ЦОД и/или сервиса.

В случае использования GSLB решения для 3 ЦОД (один узел для каждого ЦОД) кластера достаточно использовать 2 узла для настройки DNS серверов.

Схема отказоустойчивого кластера на 3 ЦОД приведена на рис. 37.

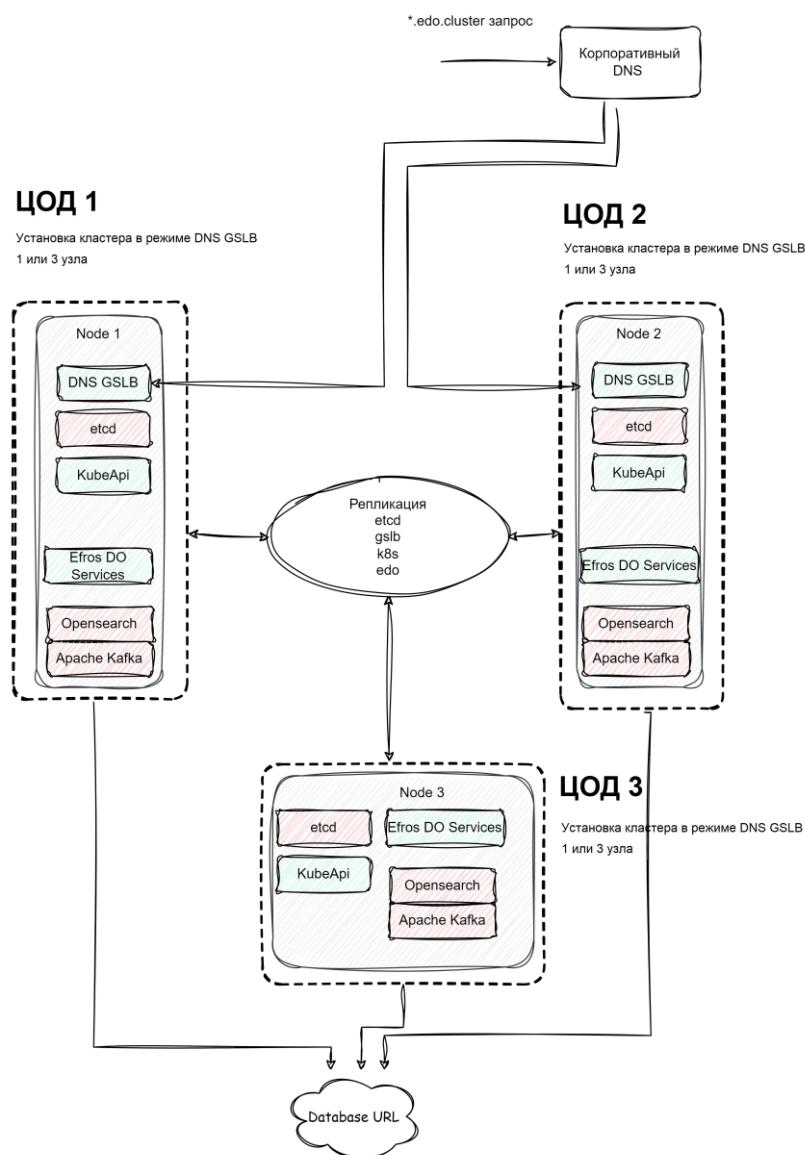


Рисунок 37 – Схема кластера с использованием GSLB решения

6.3 Предварительные настройки

6.3.1 Настройка узлов кластера

- i** Команды необходимо вводить от имени суперпользователя **root** либо, используя команду **sudo**.

Перед установкой кластера необходимо выполнить следующие шаги по настройке узлов:

- 1) Определить **hostname edo-cluster-{номер узла}**, например: edo-cluster-1, edo-cluster-2, edo-cluster-3. Пример команды приведен ниже:

```
hostnamectl set-hostname edo-cluster-1
```

 Идентификатор **hostname** должен соответствовать следующим параметрам:

- имена узлов должны соответствовать стандартам именования службы DNS;
- допустимые символы: буквы латинского алфавита нижнего регистра (строчные), цифры, «-».

2) Для каждого узла задать статический IP-адрес. Это можно сделать в файле **/etc/network/interfaces**. Пример приведен ниже:

```
auto eth0
iface eth0 inet static
    address 10.116.41.43/24
    gateway 10.116.41.1
    dns-nameservers 10.116.1.111
```

3) Далее выполнить команду перезапуска сервиса:

```
systemctl restart networking.service
```

- 4) Необходимо выделить один IP-адрес, который будет использоваться как виртуальный. Адрес не должен быть привязан к какому-либо узлу и находиться в той же подсети, что и узлы.
- 5) Должно быть однозначное сопоставление IP-адреса и **hostname**. Если узлы не добавлены в **dns**, то это можно сделать в файле **/etc/hosts**. Пример файла для узла **edo-cluster-1** с IP-адресом 10.116.41.43 приведен ниже:

```
127.0.0.1      localhost
127.0.1.1      edo-cluster-1
10.116.41.43   edo-cluster-1
10.116.41.44   edo-cluster-2
10.116.41.45   edo-cluster-3
```

6) В случае работы с GSLB решением необходимо добавить **secondary** IP-адреса на сетевые интерфейсы узлов. Для этого необходимо использовать команду:

```
sudo ip address add 10.116.48.240/24 dev ens18
```

где:

ens18 – имя сетевого интерфейса;

10.116.48.240/24 – второй IP-адрес из подсети первого IP-адреса для обеспечения сетевой доступности и корректной работы службы DNS через сетевой шлюз.

В файл **.env** необходимо добавить созданные **secondary** IP-адреса для переменной **DNS_BALANCER_HOSTS**:

```
DNS_BALANCER_HOSTS="10.100.200.101 10.100.200.102" # Второй IP  
адрес узлов кластера, где будет развернуто GSLB DNS решение (второй  
IP на интерфейсе узла)
```

- 7) Если на узле определено несколько интерфейсов, то в **/etc/hosts** необходимо указать IP-адреса из интерфейса, который будет использоваться кластером. Например, если использовать **eth1** и значение IP-адреса 10.116.48.43, то в **/etc/hosts** следует внести следующую запись: 10.116.48.43 edo-cluster-1.

6.3.2 Описание и установка Nexus

Менеджер репозиториев **Nexus** предназначен для загрузки и установки зависимостей ПК «Efros DO».

Nexus является местом хранения следующих компонентов:

- docker-образы комплекса ПК «Efros DO» (далее – образы ПК «Efros DO») и вспомогательная инфраструктура (компоненты кластера и др.);
- пакеты зависимостей, необходимые для ОС кластера;
- утилиты;
- Helm-charts.

Установка менеджера репозитория **Nexus** производится на отдельном Nexus-хосте².

6.3.2.1 Описание Nexus-хоста

Nexus-хост предназначен для централизованного хранения зависимостей комплекса (docker-образы, deb-пакеты, rpm-пакеты, helm-charts и бинарные файлы), а также для установки и обновления кластера (комплекса).

Требования к аппаратному обеспечению для Nexus-хоста приведены в пункте 1.2.2.

Образы ПК «Efros DO» по умолчанию хранятся в менеджере репозиториев Nexus. Пользователь может использовать для хранения образов также пользовательский registry (подробнее см. подпункт 6.3.2.3).

² Nexus-хост не является частью кластера

! При использовании Nexus-хоста, он должен быть доступен со всех узлов кластера.

6.3.2.2 Установка Nexus

Для установки менеджера репозиториев **Nexus** необходимо выполнить следующие действия:

- 1) Скопировать файлы **Nexus** в отдельную директорию Nexus-хоста, с которой планируется выполнять установку кластера.
- 2) Запустить скрипт **./deploy.sh**, выполнив следующую команду:

```
sudo ./deploy.sh
```

i При возникновении ошибки «`sudo: ./deploy.sh: command not found`» необходимо выполнить команду:

```
sudo chmod +x ./*.sh
```

Образы комплекса, необходимые для установки, будут автоматически скачаны и распакованы в папке **/opt/edo-distr_2_13**.

i Рекомендуется сделать резервную копию файлов **.env** и **inventory**. Файлы могут понадобиться для восстановления Nexus-хоста (см. пункт 6.9.5).

6.3.2.3 Скачивание образов комплекса из Nexus

По умолчанию образы ПК «Efros DO» хранятся в менеджере репозиториев **Nexus**.

При необходимости образы комплекса можно скачать из **Nexus** на узлы кластера и/или клиентский registry.

Установка комплекса будет производиться с Nexus-хоста.

Для скачивания образов ПК «Efros DO» на пользовательский registry необходимо поочередно ввести на Nexus-хосте следующие команды:

```
cd <директория с инсталляционными файлами>
cd ./custom_registry
sudo echo "<пароль пользовательского registry>" | sudo nerdctl --insecure-registry login -u admin --password-stdin <ip адрес пользователяского registry>:<порт пользователяского registry>
```

```
sudo ./main.py <ip адрес пользовательского registry>:<порт  
пользовательского registry>/edo/
```

Например:

```
cd /home/user/distrib  
cd ./custom_registry  
sudo echo "password" | sudo nerdctl --insecure-registry login -u  
admin --password-stdin 10.116.48.15:5000  
sudo ./main.py 10.116.48.14:5000/edo/
```

-  При возникновении ошибки при попытке скачивания данных в репозиторий пользователя «`sudo: ./main.py: command not found`» необходимо выполнить команду:

```
sudo chmod +x *.py
```

6.4 Установка комплекса на базе Kubernetes

6.4.1 Требования при установке комплекса

Для корректной установки комплекса на базе Kubernetes необходимо выполнение следующих требований:

- 1) Проводить установку комплекса необходимо с Nexus-хоста (см. пункт 6.3.2).
- 2) Команды необходимо вводить от имени суперпользователя ***root*** либо, используя команду ***sudo***.

6.4.2 Установка комплекса

Для установки комплекса на базе Kubernetes необходимо выполнить следующие шаги:

- 1) Проверить наличие архива с дистрибутивом к папке ***/opt/edo-distr_2_13***.
- 2) Перейти в каталог с распакованными файлами и отредактировать файлы ***.env*** и ***inventory***, используя образцы ***.env.example***, ***inventory.example***:

```
cd /opt/edo-distr<версия EDO>  
cp -v .env.example .env  
cp -v inventory.example inventory
```

- 3) Определить переменные, связанные с адресами узлов и именами учетных

записей для доступа к ним, с помощью редактора *nano*:

— файл *inventory*:

- отредактировать значения **ansible_host** (IP-адрес интерфейса, через который осуществляется доступ к узлам), **ansible_user**, **ansible_become_pass** не меняя структуру файла. Пример приведен на рис. 38.

```
ladmin@u542sb110:/opt/distr$ cat inventory.example
[master]
master_1  ansible_host=10.100.200.101  ansible_user=admin ansible_become_pass=MySudoPassword
master_2  ansible_host=10.100.200.102  ansible_user=admin ansible_become_pass=MySudoPassword
master_3  ansible_host=10.100.200.103  ansible_user=admin ansible_become_pass=MySudoPassword

[all:vars]
ansible_connection=ssh
ansible_private_key_file=/root/.ssh/id_rsa
```

Рисунок 38 – Редактирование файла *inventory*

ⓘ В случае установки кластера с использованием **ssh private keys**, необходимо удалить переменную **ansible_become_pass** из файла, а для переменной **ansible_private_key_file** оставить значения по умолчанию:

```
[master]
master_1  ansible_host=10.100.200.101  ansible_user=admin
master_2  ansible_host=10.100.200.102  ansible_user=admin
master_3  ansible_host=10.100.200.103  ansible_user=admin

[all:vars]
ansible_connection=ssh
ansible_private_key_file=/root/.ssh/id_rsa
```

— файл *.env*:

- в блоке «Variables for EDO Cluster Installation» обязательный параметр для заполнения **NEXUS_ADDRESS**, где указывается IP-адрес **Nexus**.

ⓘ В случае установки кластера с использованием **ssh private keys**, необходимо выключить запрос пароля для sudo на время установки, в переменной **PRIVATE_KEY_PATH** необходимо задать путь до приватного ключа на хосте с установщиком (предварительно на узлах в **authorized_keys** должны быть прописаны публичные ключи). Пример приведен ниже:

```
#=====
```

```
#-----Variables for EDO Cluster Installation-----
#=====
# пути к SSH ключам, которые используются для доступа на
# узлах кластера. Переопределить при необходимости.
PRIVATE_KEY_PATH="/root/.ssh/id_rsa"

NEXUS_REGISTRY_ADDRESS="http://10.200.200.8:5000"
# Адрес docker-registry для установки образов (указывается
# ip-адрес хоста, где развернут nexus)

NEXUS_REPOSITORY_ADDRESS="http://10.200.200.8:8081"
# Адрес репозитория для установки зависимостей (указывается
# тот ip-адрес хоста, где развернут nexus)

CUSTOM_REGISTRY_ADDRESS=""
# Адрес custom docker-registry для установки кластера EDO из
# клиентского или из облачного docker-registry
```

где:

NEXUS_REGISTRY_ADDRESS – адрес docker-registry для установки образов комплекса. Указывается IP-адрес хоста с Nexus и порт;

NEXUS_REPOSITORY_ADDRESS – адрес репозитория для установки зависимостей. Указывается IP-адрес хоста с Nexus и порт;

CUSTOM_REGISTRY_ADDRESS – адрес custom docker-registry для установки кластера из клиентского или облачного docker-registry. Параметр можно оставить пустым.

- в блоке «High Ability Settings» задать виртуальный IP-адрес для **Control Plane** в переменной **CONTROL_PLANE_IP**, имя сетевого интерфейса в переменной **KEEPALIVED_INTERFACE** и маску подсети в переменной **KEEPALIVED_NETWORK_MASK**. Пример приведен ниже:

```
#=====
#-----HIGH ABILITY SETTINGS-----
#=====
CONTROL_PLANE_IP="10.116.48.2"
CONTROL_PLANE_PORT="9443"
KEEPALIVED_INTERFACE="eth0"
KEEPALIVED_NETWORK_MASK="24"
```

-  IP-адреса узлов, будут браться из интерфейса, указанного в переменной **KEEPALIVED_INTERFACE**.

Например: если на узлах определено несколько интерфейсов **eth0, eth1**.

```
Хост-1 eth0 10.116.41.10/24
      eth1 10.116.48.10/24

Хост-2 eth0 10.116.41.11/24
      eth1 10.116.48.11/24

Хост-3 eth0 10.116.41.12/24
      eth1 10.116.48.12/24
```

При указании **KEEPALIVED_INTERFACE="eth1"** после инициализации кластера для просмотра IP-адресов интерфейса **eth1** необходимо ввести команду:

```
sudo kubectl get nodes -o wide
```

В результате выполнения команды в столбце **INTERNAL-IP** будут выведены IP-адреса интерфейса **eth1**. Пример приведен на рис. 39.

```
ladmin@u542sb111:~$ sudo kubectl get nodes -o wide
NAME      STATUS    ROLES     AGE      VERSION   INTERNAL-IP      EXTERNAL-IP   OS-IMAGE     KERNEL-VERSION
u542sb111  Ready    control-plane   6m51s   v1.29.6   10.116.42.111  <none>       Astra Linux  6.1.50-1-generic
u542sb112  Ready    control-plane   6m      v1.29.6   10.116.42.112  <none>       Astra Linux  6.1.50-1-generic
u542sb113  Ready    control-plane   6m1s    v1.29.6   10.116.42.113  <none>       Astra Linux  6.1.50-1-generic
```

Рисунок 39 – Результат выполнения команды просмотра IP-адресов интерфейса

(i) В случае применения DNS решения отказоустойчивости кластера (см. подраздел 6.2) необходимо указать следующие данные:

```
USE_DNS_BALANCER="false"
# Флаг включение отказоустойчивости через DNS

CLUSTER_DNS_NAME="edo.cluster"
# доменное имя кластера

CLUSTER_DNS_PORT="6443"
# Порт для доступа к Control Panel

CLUSTER_DNS_INTERFACE="eth0"
# Имя сетевого интерфейса, на котором будет работать кластер

DNS_SERVERS="10.100.1.111 10.100.1.112"
# Адрес корпоративного DNS сервера

DNS_BALANCER_HOSTS="10.100.200.101 10.100.200.102"
# Адреса узлов, где будет развернут DNS сервер кластера
```

где:

USE_DNS_BALANCER – флаг включения отказоустойчивости через DNS.
Значение «false» – выключен, «true» – включен.

- в блоке «**Database config**» указать параметры подключения к СУБД.
Пример приведен ниже:

```
DB_IP="10.116.48.5"
DB_PORT="5432"
DB_USER="edodbususer"
DB_NAME="EDOdb"
INSTALL_POSTGRESQL="false"
```

! В данной версии комплекса необходимо использовать внешнюю СУБД «Jatoba» для обеспечения отказоустойчивой работы кластера.

Для использования внешней СУБД в кластере необходимо в переменной **INSTALL_POSTGRESQL** ввести значение «**false**».

Использование встроенной СУБД запрещено, поэтому выставлять значение «**true**» не допустимо.

- 4) Задать обязательный параметр сервера NTP для синхронизации времени на узлах кластера. Значение указывается в переменной **NTP_SERVER**. Например:

```
NTP_SERVER="NTP.SERVER"
```

Можно указать несколько серверов NTP, разделяя их пробелами.

- 5) Запустить скрипт **./__install.sh -h** для просмотра описания этапов установки можно, выполнив следующую команду:

```
sudo ./__install.sh -h
```

- 6) Процесс установки состоит из 8 этапов, для выполнения необходимо последовательно запустить скрипт **./__install.sh** с указанными ниже ключами.
Пример команды:

```
sudo ./__install.sh -s0
```

где:

s0 – подготовительный этап. Проверяется наличие файлов `.env` и `inventory`. На узле устанавливаются зависимости (docker), загружается образ с инсталляционным модулем. Запускается контейнер с установщиком ПК «Efros DO»;

s1 – настройка доступа к узлам кластера, генерируются SSH-ключи и копируются на узле кластера, которые описаны в `inventory`,

- В случае установки кластера с использованием `ssh private keys`, необходимо выключить запрос пароля для sudo на время установки.

s2 – запуск валидатора для проверки узлов на соответствие требованиям;

- ! Проверить содержимое файла `./logs/validation-system.log` на соответствие узлов требованиям, описанным в таблице 3. В случае наличия ошибок, привести узлы в соответствие с требованиями.

s3 – внутри docker-контейнера запускается сценарий (роль `install_deps`) по установке всех зависимостей на узлы (deb-пакеты и утилиты) для загрузки образов компонентов кластера;

s4 – проверка содержимого файла `./logs/validation-ports.log` на соответствие узлов требованиям, описанным в таблице 3 для проверки необходимых портов на доступность;

s5 – создание кластера `Kubernetes` с помощью утилиты `Kubeadm`;

- ! При установке кластера на подготовленные ЭВМ необходимо последовательно выполнить шаги установки с s0 по s5. После шага s5 необходимо зайти на узел `master-1` и выполнить команду `sudo kubectl get nodes`. У всех узлов должен появиться статус `STATE Ready`, это может занять некоторое время. Затем продолжить выполнение шагов с s6 по s8. Все шаги выполняются из скрипта `./_install.sh`.

s6 – установка в кластер дополнительных компонентов – `Certmanager`;

s7 – задание пароля для доступа к базе данных и установка ПК «Efros DO»;

--load-images – дополнительный ключ скрипта для загрузки образов ПК «Efros DO» на узлы кластера (выполнять при необходимости);

s8 – для удаления контейнера установки.

(i) В случае установки кластера с использованием **ssh private keys**, необходимо выключить запрос пароля для sudo.

- 7) После установки перейти на **master-1** и выполнить команду **kubectl get po -n edo**. Команда выведет список подов. У всех сервисов, кроме двух, должен быть статус **Running**. У сервисов **edo-radius** и **edo-tacacs** должен быть статус **Init** до тех пор, пока комплекс не пройдет активацию (рис. 40).

NAME	READY	STATUS	RESTARTS	AGE
edo-acs-service-8576cd6c7f-s2bk6	1/1	Running	0	43m
edo-agent-service-6b5c6686c4-ntdkx	1/1	Running	0	43m
edo-ci-route-service-64bbc44745-rjmwrt	1/1	Running	0	42m
edo-ci-service-68b4f6db4d-sd9cz	1/1	Running	0	43m
edo-dns-manager-7bbcfc974c5-mfghq	1/1	Running	2 (26m ago)	43m
edo-dns-service-bfd7cd586-q8tbl	1/1	Running	0	42m
edo-email-sender-service-54c4b66cf7-xs8tl	1/1	Running	0	43m
edo-flow-collector-64b95b7499-v9fbk	1/1	Running	0	43m
edo-flow-collector-dhcp-7976f94db8-jjgcl	1/1	Running	0	43m
edo-flow-collector-sflow-5bf845d84d-ql4vs	1/1	Running	0	43m
edo-flow-service-549dc6d9d-9krj8	1/1	Running	0	42m
edo-gateway-service-575c44d89f-fzlg4	1/1	Running	0	43m
edo-gateway-service-575c44d89f-rklq	1/1	Running	0	43m
edo-gateway-service-575c44d89f-s6hsp	1/1	Running	0	43m
edo-guest-portal-service-5996db7c48-k6tvr	1/1	Running	0	43m
edo-hierarchy-service-55bb46b566-b2nlw	1/1	Running	0	43m
edo-hierarchy-service-55bb46b566-l9rxl	1/1	Running	0	43m
edo-hierarchy-service-55bb46b566-m22pb	1/1	Running	0	43m
edo-identity-service-86dbb56455-x259b	1/1	Running	0	43m
edo-k8s-operator-service-7b9688c9d5-w99rv	1/1	Running	0	43m
edo-kafka-cluster-entity-operator-77b4b9968c-plgnj	2/2	Running	0	23m
edo-kafka-cluster-kafka-0	1/1	Running	0	25m
edo-kafka-cluster-kafka-1	1/1	Running	0	24m
edo-kafka-cluster-kafka-2	1/1	Running	0	23m
edo-kafka-cluster-zookeeper-0	1/1	Running	0	26m
edo-kafka-cluster-zookeeper-1	1/1	Running	0	25m
edo-kafka-cluster-zookeeper-2	1/1	Running	0	26m
edo-knowledge-base-service-9dd78f649-rmldl	1/1	Running	0	43m
edo-license-service-74cc79cb56-lb7cv	1/1	Running	0	43m
edo-metrics-collector-6fd4cc5ff9-4fp16	1/1	Running	0	43m
edo-metrics-service-85dd955587-f5sf8	1/1	Running	0	43m
edo-radius-75db8d6685-8z4dk	0/1	Init:0/1	0	42m
edo-radius-75db8d6685-w8n6z	0/1	Init:0/1	0	42m
edo-radius-75db8d6685-xhltf	0/1	Init:0/1	0	42m
edo-report-portal-service-5b5b4b7bb9-qdrpm	1/1	Running	0	43m
edo-schedule-service-6ccb8c5fb9-gtb7b	1/1	Running	0	43m
edo-so-service-67b6df854-qfvkc	1/1	Running	0	43m
edo-store-minio-0	1/1	Running	0	43m
edo-tacacs-6f485dc88c-ggv72	0/1	Init:0/1	0	42m

Рисунок 40 – Статусы сервисов

- 8) Затем необходимо перейти на главную страницу ПК «Efros DO» https://{{VIRTUAL_IP}}. Например: <https://10.116.48.2>.

(i) Если пароль от БД был введен неверно, на **master-1** необходимо выполнить скрипт, который обновит значение поля **password** в **efros-posgresqlbit-postgresql secret**:

```
sudo kubectl create secret generic efros-posgresqlbit-
postgresql -n edo \
```

```
--from-literal=password={мой_пароль} \
--save-config \
--dry-run=client -o yaml | \
sudo kubectl apply -f -
```

- (i)** В случае применения DNS решения отказоустойчивости кластера для проверки работоспособности и корректности установки необходимо перейти на главную страницу ПК «Efros DO», используя ссылку: <https://{IP одной из узлов}>. Например: <https://10.116.48.43>.

Дополнительно в корпоративном DNS необходимо добавить зону безусловной пересылки по «edo.cluster», который должен быть настроен на IP-адрес внутреннего DNS на 1 и 3 узлах.

6.4.3 Проверка отказоустойчивости

Для проверки отказоустойчивости необходимо выполнить следующие действия:

- 1) Зайти на веб-интерфейс https://{VIRTUAL_IP}. Проверить доступ к ПК «Efros DO».
- (i)** В случае применения DNS решения зайти на веб-интерфейс используя ссылку: <https://web.edo.cluster>.
- 2) Выключить один из узлов, подключившись к ней напрямую по SSH и выполнив команду:

```
sudo poweroff
```
- 3) Проверить доступность веб-интерфейса комплекса: в течении 5 минут работоспособность должна восстановиться.
- 4) Включить ранее выключенный узел.

6.4.4 Настройка почтовых уведомлений

Изменения состояния компонентов кластера фиксируются в ПК «Efros DO» (раздел «События» → «Системные события» → вкладка «Общие»).

Для отслеживания состояния компонентов кластера необходимо настроить отправку почтовых уведомлений в разделе «Администрирование» → «Планировщик» → вкладка «По событию».

6.5 Обновление сертификатов

i Безопасность кластера реализуется с помощью сертификатов безопасности, используемых при проверке аутентификации пользователей и реализации защиты канала связи.

При необходимости замены самоподписанных сертификатов, которые автоматически генерируются при установке комплекса, на пользовательские сертификаты (custom certificate), нужно воспользоваться инструкцией, приведенной ниже.

Выпуск СА-сертификатов для модулей кластера реализуется на базе пакета ***cert-manager*** из состава кластера.

При выпуске корневого сертификата с помощью ***cert-manager*** для ПК «Efros DO» автоматически генерируются необходимые дочерние сертификаты для работы модулей комплекса, кроме RADIUS-сертификата. Процесс выпуска самоподписанных сертификатов СА и дочерних сертификатов, происходит автоматически при установке кластера, хранение осуществляется в ***secrets*** кластера.

При необходимости выпуска и установки пользовательского сертификата необходимо выполнить следующие операции на узле ***master-1***:

- 1) Выпустить сертификаты ***ca.crt***, ***tls.crt***, ***tls.key***, используя доверенный удостоверяющий центр, в требуемом формате. Пример формата приведен ниже.

Пример формата:

ca.crt

-----BEGIN CERTIFICATE-----

MII DhzCCAm+gAwIBAgIQJ84S+krRb7hEJpGh8CNefTANBgkqhkiG9w0BAQsFADBWMRM
wEQYKCZIm

iZPyLGQBGRYDZGV2MRMwEQYKCZImiZPyLGQBGRYDYXBwMRQwEgYKCZImiZPyLGQBGRY
EZGF0YTEU

MBIGA1UEAxMLZGF0YS1TUlYtQ0EwHhcNMjMwNTAyMTE0ODMyWhcNMjgwNTAyMTE1ODM
xWjBWMRMw

EQYKCZImiZPyLGQBGRYDZGV2MRMwEQYKCZImiZPyLGQBGRYDYXBwMRQwEgYKCZImiZP
yLGQBGRYE

ZGF0YTEUMBIGA1UEAxMLZGF0YS1TUlYtQ0EwgxEiMA0GCSqGSIb3DQEBAQUAA4IBDwA
wgGEKAoIB

AQDC+nmWOvo92NQuSOM9YY7r91cgPjishSqOf01SOrbXxWv8+DGPxg/gUcq2pNkVxeC
t5eSHuz3n

ACbs2FKmWnxMxwjCbw+nIrZqKhfrV3+T1uaMd8VTbkQ9fPH4oJqBRonErYeIpuPEE/N
o0FTxkwxA

krHAy/+kqKedxVSfx7veC3wM15Sg/oTdajLKZWauaxjhGhkfFsbjGr4k18D/73W9LR1
GvVK3V5Xb

6U4Q4vak5umW8dvbUJKrt8cE0g5Cx2GWG/V8+xdgPzJC130tJHGUL9nSTa4n6Mc0Yg/
H2neK3HC3

DdngYkMuQYD9TxrtBiOqfsUGORxZJoUKuhC8EGp5AgMBAAGjUTBPMAsGA1UdDwQEAvI
BhjAPBgNV
HRMBAf8EBTADAQH/MB0GA1UdDgQWBBSnbfKzyZk0kFeHAX2m04qo/V+aWjAQBgkrBgE
EAYI3FQEE
AwIBADANBgkqhkiG9w0BAQsFAAOCAQEANEKqxVxgjgZEVxNFhnsb1B8Sh7y7/aDDGrr
TK8W2TbEG
TkXJYFmPvtf6oDHaEs7ZaOZZlk0BYb654sOkCN7YV8VyItH3Ut+k+8s8Vk+DdhD1B+g9
/BmYAMraJ
XoanbFkTRUowPuVzJtblF75auAYm85EI3YR2LKLb513zFClaEzs8jMfw0YIBXM4nNsK
fLhcW9+m7
21+jj20Fm8rAgnCG8TyxBw30yIUHRPrxDPLE1MqWhKhTvb0Oa3xQDRnNyRrywMEQp3m
jzKeeAOB+
3SLBLmTztEtpsLFxNBCUl9s1XgRb60xsgxTlZ1QIWm/fqlLbrLRMNb2JIjdirxx7UA
Q6Q==
-----END CERTIFICATE-----

tls.crt

-----BEGIN CERTIFICATE-----
MIIFLzCCBBeAwIBAgITagAAC75icSKxtB8SAAAAAAALjANBgkqhkiG9w0BAQsF
ADBWMRMwEQYKCZImiZPyLGQBGRYDZGV2MRMwEQYKCZImiZPyLGQBGRYDYXBwMRQw
EgYKCZImiZPyLGQBGRYEZGF0YTEUMBIGA1UEAxMLZGF0YS1TU1YtQ0EwHhcNMjQx
MDE3MTQwODU4WhcNMjYxMDE3MTQwODU4WjATMREwDwYDVQQDEwh1ZG8tbXQtMTCC
ASIwDQYJKoZIhvCNQEBBQADggEPADCCAQoCggEBALjQ40kwuLfspi1hYSAn7+o
mwXsjX0JZde4756u+OuV412LumbolbmNwAO1RyH57kJX/oKhSDKCSI4+cCohH++
sR6aKzgIKCefi7TVrWXiuPh4GpqbRjmdFE7bWm9L1qL+x5VsLPqxmaniYAu9QaGN
kWaNYNEOBaeI1sq/wn9Cu1GsubpNNRGFqf65tSL8G0xjsJor5iSq/sQnryMxnXw/
gGdSdufBZtMMiYTuN76M5yTpZtsx+TVCKkOH41SgD/cpOfkMCouP2g1MA/6UTpse
v1Q9312xKmSesPz5iop5YFCUPaXyEACutJSj/JtpIrbxceHLutmN37v7/twExp0C
AwEAAaOCAjcwggIzMCEGCSsGAQQBgjcUAgQUhIAVwBlAGIAUwBlAHIAdgBlAHId
DgYDVR0PAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMB0GA1UdDgQWBBS4
6Y2LLraqhEOWGxf4a4OmIpfgfTAZBqNVHREEejaQggh1ZG8tbXQtMYcECnQpozAf
BgNVHSMEGDAWgBSnbfKzyZk0kFeHAX2m04qo/V+aWjCBYQYDVR0fBIHBMIG+MIG7
oIG4oIG1hoGybGRhcDovLy9DTj1kYXRhLVNSVi1DQSxDTj1zcnyS049Q0RQLENO
PVB1YmxpYyUyMetleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbZpZ3V
YXRpb24sREM9ZGF0YSxEqz1hCHAsREM9ZGV2P2N1cnRpZmljYXR1UmV2b2NhdG1v
bkxpc3Q/YmFzzT9vYmp1Y3RDbGFzc1jUkxEaN0cmliidXRpb25Qb21udDCBwQYI
KwYBBQUHAQEEgbQwgbEwga4GCCsGAQUFBzAChoGhbGRhcDovLy9DTj1kYXRhLVNS
Vi1DQSxDTj1BSUEsQ049UHVibGljJTIws2V5JTIwU2VydmljZXMsQ049U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1kYXRhLERDPWFwcCxEQz1kZXY/Y0FDZXJ0
aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25BdXRob3JpdHkw
DQYJKoZIhvCNQELBQADggEBACUhG+3ppitPDJOi7a9KP8Fs01BWG0hXeKvk+Uv3
LLXMcSJJKoOKgIUFDEYYGFCGff6RdONy5Fc+ES5wRTXZaEt7gupjz+zoN07mYua
Ozdg7hEAG4w50eJEHRF+A8+c8AQs/2Crg4sZnt3nZGBowANLBHbjDGL4y9EDG7cI
U0m3Jts1Xw5Cq6AX7SmaxUP2gBV/h+g0++fTvvXUIMNEhJnEIjgfGp8yrN2Hfd6E
91LPuvBQtte3UY/u3WUTCNoy/Kpi3dHIEY6YJXd2rjOwQNdTYifmt1I3yhmdJCSA
8IpiogoJLeEzwA4oW9ViTaJ7bQGExxr4N4gDhI5VB//4J9Y=

-----END CERTIFICATE-----

tls.key

-----BEGIN RSA PRIVATE KEY-----

```
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQC40ONJMLi37KYt
YWegJ5+/qJsF7I19CWXXu0+ervjrleJdi7pm6NW5jcADpUch+e5CV/6CoUgygkoh
OPnAqIR/vrEemis4CCgnn4u01a114rj4eBqam0Y5nRRO21pvS9ai/seVbCz6sZmp
4mALvUGHjZFmjWDRDgWniNbKv8J/QrtRrLm6TTURhan+ubUi/BtMY7CaK+Ykqv7E
J68jMZ18P4BnUnbnwWbTDImE7je+jOck6WbbMfk1QipDh+NUoA/3KTn5DAj1D9oJ
TAP+1E6bHr9UPd5dsSpknrD8+YqKeWBQ1D218hAArrSUo/ybask28Xhy7rZjd+7
+/7cBF6dAgMBAAECggEAWD6FB6FX0ZoRD0h8mhnRUPX0bzOvqxAdrI8E+sOY3wPF
/dyFuDVcNyjTkeoMuNBZTxwszbqselFzi8FknbTxrxciAvahxDNA2Qp47nNIQ+mp
YBoYudGCCmhSFgTufU28wj7c1R/9qgW61T7d1T1cZQLvdgPzQ15rnL7dsBk3iQNH
w2ieY0c1gvKIJ4k704ibHevV8prbh6hqP7O3ImSw+1Va+IhoJvqwM3P995NB3Sze
Uj+JLu64XC0Q8F31/Psi11YQXRuaoojLf5Wm1XOA+cEl1yC7HJuBO+KzIjUJRv4m7
vhm1wti5NIGdRz/87u0qnIMoDj2MCq9VNTMV0tM0EQKBgQDMLiq1aMjvp4Eejsp+
MU/6CN+jPsJHqSC0YmEy+Hpha37/ueoxS/6wcwHk/G4mtWyIY3xzhPHXE5KAn5Sn
5Jyzq73rEnvyxln20h4ZDkoh5CnILknKTYf41PCJdJ6gPGfqXT7ThnN2yHaqIX0E
n2F63txPlH5x+3AM+NeMyRWBwwKBgQDnuJhrDzRwAM9G/petBbvIdnnnHJONE/pmw
HrUu/ILIff+VeXJYZaUBdZKIsEhbhxWTbsiA47GYelpU3VjmV35i8eoaf4Lz2k
lCOOoarjE01EK1DKfGqYQxmTzLmPrUyhtDJ3Z4hRLxk7oH9ScUutIbJ3a0OXy8vR
Wc01Wm04HwKBgEM8TKoSsGDKqvUyFA5H1MuEUoiCKR3J7tAXuWQ8eKhN6rMxOJJ1
MQhPxubtzSQICCdhGTR+YVWl56tbh1fac6s1kyreI94i7WAeZLMptLEPJID1B6/
KzBLc24ALiAb5ChD7mVfV/RcjN73SIDUjxgT/T5jasQEBWDwLKLasK9bAoGAVaKm
0YoA+xORhs84Br2DtIX0Y2CCjVD6Q1hV5VN0kdrexMLpOzn1TSDCUrmzRBdkopp/
egaOkUpGFKK/U1uumzbJRrepccggjY9tLeL7OhLTv8r1/UhXA3xyNK04RlcOZ+ni5
3d7pRfd9/8dExpcQPJ+jcPa3ODYc0PW7Fv7gNkkCgYBfQeHCYHACuYNlhJbZBIxo
rPxxklaq8aKOsqX/rJpItmaVhyyT1uyLeLAx8oiHUD1vvpx6jej1CuxWTankullJ
sy8QCBQybN48notmKf5b1ss0PgcmVX1XGPyp8VKWFPOZJLRK8eKMbkxhkzku2mhf
e7MyYu3x4mD8yo9krj7iA==
```

-----END RSA PRIVATE KEY-----

- 2) Создать **secret** командой, где по порядку передаются аргументы: корневой сертификат, сертификат и ключ.

```
./load_cert.sh ca.crt tls.crt tls.key
```

- 3) Поменять имя **secret** в **ingress** на **edo-custom-certs**:

```
kubectl edit ingress -n edo edo-gateway-ingress
```

Для этого в открывшемся файле на редактирование необходимо произвести следующие изменения и сохранить.

прежнюю редакцию:

```
```yaml
tls:
- hosts:
```

```
- 10.116.41.163
 secretName: gw-ip-cert-secret
````
```

заменить на новую редакцию:

```
```yaml
tls:
- hosts:
 - 10.116.41.163
 secretName: edo-custom-cert
````
```

4) Заменить имя *secret* в *deployment*.

```
kubectl edit deployment -n edo efros-ingress-nginx-controller
```

Для этого в открывшемся файле на редактирование необходимо произвести следующие изменения и сохранить.

прежнюю редакцию:

```
```yaml
containers:
- args:
 - /nginx-ingress-controller
 - --publish-service=$(POD_NAMESPACE)/efros-ingress-nginx-
controller
 - --election-id=ingress-controller-leader
 - --controller-class=k8s.io/ingress-nginx
 - --configmap=$(POD_NAMESPACE)/efros-ingress-nginx-
controller
 - --default-ssl-certificate=edo/gw-ip-cert-secret
````
```

заменить на новую редакцию:

```
```yaml
containers:
- args:
 - /nginx-ingress-controller
 - --publish-service=$(POD_NAMESPACE)/efros-ingress-nginx-
controller
 - --election-id=ingress-controller-leader
 - --controller-class=k8s.io/ingress-nginx
 - --configmap=$(POD_NAMESPACE)/efros-ingress-nginx-
controller
 - --default-ssl-certificate=edo/edo-custom-cert
````
```

6.6 Работа с узлами кластера

6.6.1 Добавление узла кластера

Для добавления узла кластера необходимо выполнить следующие действия:

- 1) Отредактировать файл *inventory_join*, используя *inventory_join.example*:

```
cp -v inventory_join.example inventory_join
```

- 2) Определить переменные, связанные с адресами узлов и именами учетных записей для доступа к ним с помощью редактора *nano*:

— файл *inventory_join*:

- в группе «k8s_node» задается уже существующий узел кластера *master_1* с необходимыми параметрами *ansible_host* (IP-адрес интерфейса, через который осуществляется доступ к узлам), *ansible_user*, *ansible_become_pass*;
- в группе «master» указываются master-узлы, которые требуется добавить в кластер;
- в группе «worker» указываются worker-узлы, которые требуется добавить в кластер.



Необходимо учитывать уже существующую нумерацию узлов из файла *inventory*. Например, если уже определены *master_1*, *master_2* и *master_3*, то при добавлении дополнительного узла *master*, нужно указать *master_4*.

Перед запуском добавления узла, нужно удалить не используемые группы из файла *sudo*. Пример:

```
[k8s_node]
master_1    ansible_host=10.100.200.101    ansible_user=ladmin
ansible_become_pass=Gazprom09

[master]
master_4    ansible_host=10.100.200.104    ansible_user=ladmin
ansible_become_pass=Gazprom09

[worker]
worker_1    ansible_host=10.100.200.105    ansible_user=ladmin
ansible_become_pass=Gazprom09
```

```
[all:vars]
ansible_connection=ssh
ansible_private_key_file=/root/.ssh/id_rsa
```

- 3) Запустить скрипт `__join_new_node.sh` с ключами `-s0`, `-s1`, `-s2`, `-s3`, `-s4` последовательно, где:
 - s0** – подготовительный этап. Запускается контейнер с установщиком ПК «Efros DO», если еще не запущен.
 - s1** – настройка доступа к узлам кластера, генерируются SSH-ключи и копируются на узлы кластера, которые описаны в `inventory_join`.
 - s2** – проверки новых узлов на соответствие требованиям.
 - s3** – внутри docker-контейнера запускается сценарий (роль `install_deps`) по установке всех зависимостей на узлы (deb-пакеты и утилиты).
 - s4** – запускается процесс подключения новых узлов к существующему кластеру.
- 4) Произвести проверку наличия нового узла в существующем кластере, запустив команду на `master_1`:

```
kubectl get nodes -o wide
```

- 5) Добавить новый узел в файл `inventory`.
- 6) Добавить новый узел в файл `pg_hba.conf`.

6.6.2 Добавление узла кластера с ролью

В комплексе на базе Kubernetes доступно разворачивание дополнительных узлов со следующими ролями в системе:

- 1) «Универсальные» – для балансировки нагрузки.
- 2) «NAC» – для размещения обязательных сервисов модуля «Efros NAC»:
 - RADIUS (`edo-radius-service`);
 - TACACS+ (`edo-tacacs-service`);
 - гостевой портал (`edo-guest-portal-service`).

 Для роли «NAC» дополнительно могут быть добавлены любые другие сервисы комплекса.

Для добавления узла кластера с ролью необходимо:

- 1) Добавить узел кластера, выполнив шаги, указанные в пункте 6.6.1.
- 2) Определить роль для узла кластера.

Для определения роли «NAC» для узла кластера необходимо произвести следующие действия:

- 1) В файле `.env` в значение параметра **NAC_NODES** добавить имя ролевого узла, подключенной к **master-узлу**:

```
NAC_NODES="{имя_master_узла}, {имя_рабочего_ролевого_узла}"
```

Имена должны соответствовать значениям, указанным в файле *inventory*.

- 2) Запустить скрипт `./install.sh` из директории с дистрибутивом комплекса с ключом «-s7» для подключения установленных компонентов.
- 3) Ввести пароль доступа к базе данных и дождаться завершения установки компонентов комплекса.
- 4) Проверить, что созданные узлы получили метку **NAC=true**, выполнив команду:

```
kubectl get nodes -l nac=true -o custom-columns=:metadata.name --no-headers
```

- 5) Проверить, что все поды перешли в состояние **Running**, выполнив команду:

```
kubectl get po -n edo -o wide
```

6.6.3 Удаление или изменение ранее назначенной на узел роли

 При изменении роли сервисы модуля «Efros NAC» перемещаются на следующие узлы:

1. Узлы с назначенной меткой **NAC=true** при его определении.
2. Произвольные узлы в соответствии с доступными ресурсами при удалении метки **NAC=true** с выбранного узла.

Для изменения или удаления роли узла кластера необходимо произвести следующие действия:

- 1) Изменить или удалить роль на узле в файле `.env` путем изменения строки **NAC_NODES**:

```
NAC_NODES="{имя_мастер_узла}, {имя_рабочего_ролевого_узла}"
```

Имена должны соответствовать значениям, указанным в файле *inventory*.

- 2) Запустить скрипт `./install.sh` из директории с дистрибутивом комплекса с ключом

- «-s7» для подключения установленных компонентов.
- 3) Ввести пароль доступа к базе данных и дождаться завершения установки компонентов комплекса.
 - 4) Проверить, что для узла метка была изменена, выполнив команду:

```
kubectl get nodes -l nac=true -o custom-columns=:metadata.name --no-headers
```

- 5) Проверить, что все поды перешли в состояние *Running*, выполнив команду:

```
kubectl get po -n edo -o wide
```

6.7 Размещение гостевого портала в ДМЗ

Размещение гостевого портала в демилитаризованной зоне (ДМЗ) обеспечивает дополнительную защиту инфраструктуры, ограничивая доступ к серверному сегменту сети и корректный ролевой доступ к ресурсам защищаемых устройств. Доступ в защищенную сеть будет разрешаться только после аутентификации клиентов.

Для реализации внешнего гостевого портала необходимо создать отдельный узел Kubernetes (внешний гостевой портал) и присвоить ей роль **NAC_NODE**.

Описание назначения ролей узлам приведено в подразделе 6.6.2.

 Для корректной работы гостевого портала на выделенном интерфейсе при настройке точки доступа требуется обеспечить корректный адрес RADIUS сервера.

 Внешний гостевой портал использует собственный интерфейс для внешних подключений.

Перед настройкой узла с ролью «NAC» и гостевого портала с внешним интерфейсом необходимо выполнить команду:

```
sudo sysctl -w net.ipv4.conf.eth1.rp_filter=0
```

Проверку наличия и факта включения соответствующего узла можно провести в файле **.env**:

```
# Список узлов для внешнего гостевого портала
```

```
NAC_NODES=""  
GUEST_PORTAL_IP="" # IP адрес узла с guest portal
```

После создания выделенного узла внешнего гостевого портала требуется присвоить в файле **.env** выделенный IP-адрес внешнего интерфейса:

```
# Список узлов для внешнего гостевого портала  
NAC_NODES="master_3"  
GUEST_PORTAL_IP="10.0.16.166" # IP адрес узла с guest portal
```

где:

NAC_NODES – имя узла NAC;

GUEST_PORTAL_IP – адрес внешнего интерфейса (указывается IP-адрес).

Внутренний адрес узла NAC в кластере будет обеспечиваться средствами Kubernetes и не требует специального определения.

После настройки гостевой портал будет доступен по настроенному адресу (например, «10.0.16.166:5802») либо «guest.edo.cluster:5802», где:

edo.cluster – доменное имя кластера,

5802 – статично заданный порт.

Для корректного разграничения доступа и возможности входа по адресу «guest.edo.cluster:5802» требуется обеспечить реализацию сетевых политик путем реализации ingress-правил в Cilium.



При настройке гостевого портала в ДМЗ необходимо учитывать:

- Узел NAC не может использовать адрес VIP кластера.
- Работа с выделенным гостевым порталом возможна только по [https](https://).
- RADIUS-сервер при использовании внешнего гостевого портала доступен на IP-адресе узла, где работает RADIUS-сервер, по следующим портам: аутентификация – 1812; аккаунтинг – 1813.

6.8 Остановка и запуск кластера ПК «Efros DO»

Штатная остановка кластера

Основные правила штатной остановки кластера:

- 1) Для штатной остановки кластера необходимо отключить виртуальные машины, на которых запущены узлы кластера ПК «Efros DO» (по умолчанию 3 узла).

- 2) Отключение виртуальных машин необходимо выполнять с наименьшим интервалом по времени, чтобы избежать процедуры переезда подов с одного узла на другой. Допускается задержка в 10-30 секунд.
- 3) В случае работы 2 из 3 узлов необходимо отключить 2 виртуальные машины, также с наименьшим интервалом по времени.

Запуск кластера

Основные правила запуска кластера:

- 1) Для запуска кластера необходимо включить виртуальные машины, на которых развернуты узлы кластера ПК «Efros DO» (по умолчанию 3 узла).
- 2) Перед включением виртуальных машин необходимо убедиться:
 - виртуальные машины с развернутыми узлами кластера находятся в выключенном состоянии;
 - узлы кластера находятся в состоянии Ready. Выполнить проверку можно командой:

```
kubectl get nodes
```

- 3) Результат выполнения команды приведен на рисунке 41.

| NAME | STATUS | ROLES | AGE | VERSION |
|---------------------|--------|---------------|-----|---------|
| edo-cluster-astra-1 | Ready | control-plane | 47h | v1.29.6 |
| edo-cluster-astra-2 | Ready | control-plane | 47h | v1.29.6 |
| edo-cluster-astra-3 | Ready | control-plane | 47h | v1.29.6 |

Рисунок 41 – Узлы кластера со статусом Ready

- 4) Одновременно включить виртуальные машины, допускается задержка в 10-30 секунд.
- 5) После включения виртуальных машин необходимо проверить состояние сервисов ПК «Efros DO». У всех сервисов, должен быть статус *Running*.

Выполнить проверку можно командой:

```
kubectl get po -n edo
```

Результат выполнения команды приведен на рисунке 42.

- 6) Восстановление работы комплекса может занять около 10 минут с момента загрузки ОС на узле.

| NAME | READY | STATUS | RESTARTS | AGE |
|--|-------|---------|-----------------|-----|
| edo-acs-service-5d86b7bb69-w45qg | 1/1 | Running | 2 (5h15m ago) | 26h |
| edo-agent-service-687bc69466-vdk7c | 1/1 | Running | 0 | 26h |
| edo-ci-route-service-54bb688d59-7kqww | 1/1 | Running | 0 | 26h |
| edo-ci-service-6fb6484bc6-xz4sx | 1/1 | Running | 0 | 26h |
| edo-dns-collector-76d64c9c4c-lq52b | 1/1 | Running | 194 (6m18s ago) | 26h |
| edo-dns-manager-87c5686-r4655 | 1/1 | Running | 4 (26h ago) | 26h |
| edo-dns-service-86d7cffb5-dlv84 | 1/1 | Running | 0 | 26h |
| edo-email-sender-service-b5d7749fd-vq7ht | 1/1 | Running | 0 | 26h |
| edo-flow-collector-5bc8b589b4-7r5cn | 1/1 | Running | 3 (26h ago) | 26h |
| edo-flow-collector-dhcp-5f595bc547-92mhx | 1/1 | Running | 4 (26h ago) | 26h |
| edo-flow-collector-sflow-6d7576685-w7nmf | 1/1 | Running | 3 (26h ago) | 26h |
| edo-flow-service-75fc4b7bc7-5rsz2 | 1/1 | Running | 0 | 26h |
| edo-gateway-service-7d94f55d94-dpm89 | 1/1 | Running | 0 | 26h |
| edo-gateway-service-7d94f55d94-wp652 | 1/1 | Running | 0 | 26h |
| edo-gateway-service-7d94f55d94-wr5d2 | 1/1 | Running | 0 | 26h |
| edo-guest-portal-service-5b98f7b99f-jwnms | 1/1 | Running | 0 | 26h |
| edo-hierarchy-service-98799df5-fxdgq | 1/1 | Running | 1 (26h ago) | 26h |
| edo-hierarchy-service-98799df5-gmw45 | 1/1 | Running | 0 | 26h |
| edo-hierarchy-service-98799df5-j9t6h | 1/1 | Running | 0 | 26h |
| edo-identity-service-789ddcc4f7-w58gp | 1/1 | Running | 0 | 26h |
| edo-k8s-operator-service-5df67d4c54-kxq8k | 1/1 | Running | 7 (6h44m ago) | 26h |
| edo-kafka-cluster-entity-operator-6f575bb7c9-sf5fz | 2/2 | Running | 0 | 26h |
| edo-kafka-cluster-kafka-0 | 1/1 | Running | 0 | 26h |
| edo-kafka-cluster-kafka-1 | 1/1 | Running | 0 | 26h |
| edo-kafka-cluster-kafka-2 | 1/1 | Running | 0 | 26h |
| edo-kafka-cluster-zookeeper-0 | 1/1 | Running | 0 | 26h |
| edo-kafka-cluster-zookeeper-1 | 1/1 | Running | 0 | 26h |
| edo-kafka-cluster-zookeeper-2 | 1/1 | Running | 0 | 26h |
| edo-knowledge-base-service-5f87cd95fb-phr5j | 1/1 | Running | 0 | 26h |
| edo-license-service-6568fd7665-c4wfr | 1/1 | Running | 0 | 26h |
| edo-metrics-collector-69d95bcc74-pg5s8 | 1/1 | Running | 1 (26h ago) | 26h |
| edo-metrics-service-6669b98c67-5pscj | 1/1 | Running | 0 | 26h |

Рисунок 42 – Сервисы со статусом Running

6.9 Возможные ошибки при работе с кластером и способы их устранения

6.9.1 Ошибка инициализации кластера или соединения узлов при установке кластера

При создании кластера **Kubernetes** с помощью утилиты **Kubeadm** (шаг «-s4») возможны проблемы инициализации кластера или присоединения узлов. Перед повторным запуском необходимо выполнить шаги по удалению **kubernetes** кластера.

Одна из ошибок при установке может иметь следующий текст:

```
kubeadm_init : Launch kubeadm init from bash script]
[ERROR CRI]: container runtime is not running: output: time=\"2024-06-10T16:02:02+03:00\" level=fatal msg=\"validate service connection: validate CRI v1 runtime API for endpoint \\\\"unix:///run/containerd/containerd.sock\\\\"; rpc error: code = Unimplemented desc = unknown service runtime.v1.RuntimeService\\\"\n, error: exit status 1\\n\"

```

Для решения проблемы нужно выполнить рестарт сервиса **containerd** на каждом из узлов следующей командой:

```
sudo systemctl restart containerd
```

После можно выполнить проверку командой:

```
sudo crictl ps
```

6.9.2 Ошибка загрузки образов после установки комплекса

После установки комплекса у некоторых сервисов, развернутых на **master_1**, могут появиться ошибки вида **image pull failed: Back-off pulling image**.

Для устранения данной проблемы необходимо выполнить следующие действия:

- 1) Загрузить образы на узел следующей командой:

```
sudo nerdctl load -i /opt/images/edo/{имя образа}.tar.gz
```

- 2) После загрузки необходимо выполнить перезапуск сервиса командой:

```
kubectl rollout restart -n edo deployment/{имя сервиса}
```

6.9.3 Ошибка в работе сервиса edo-radius

Проблема с сервисом **edo-radius**. **0/3 nodes are available: 3 node(s) didn't match Pod's node affinity/selector.preemption: 0/3 nodes are available: 3 Preemption is not helpful for scheduling.**

Для устранения данной проблемы необходимо выполнить следующие действия:

- 1) Добавить лейблы **type=master-node** на **master-узле**:

```
kubectl label nodes {имя узла} type=master-node
```

- 2) После загрузки необходимо выполнить перезапуск сервиса **edo-radius** командой:

```
kubectl rollout restart -n edo deployment/edo-radius
```

6.9.4 Ошибка при запуске кластера

После перезагрузки одной или нескольких узлов кластер может не запуститься. Главная из причин такого поведения включение SWAP со стороны гипервизора.

Для точной диагностики нужно проверить статус *kubelet*, выполнив команду:

```
systemctl status kubelet, и его логи journalctl -u kubelet
```

Пример ошибки:

```
[ERROR Swap]: running with swap on is not supported. Please disable swap
```

Для решения, рекомендуется удалить раздел, куда монтируется SWAP.

6.9.5 Восстановление отдельного хоста с Nexus

 Рекомендуется иметь резервную копию файлов *.env* и *inventory* существующего кластера, который располагается на отдельном хосте с **Nexus** (см. пункт 6.3.2).

При отказе отдельного хоста с **Nexus** необходимо выполнить следующие действия для восстановления хоста:

- 1) Создать узел с аналогичными характеристиками, которые были у предыдущего хоста: с аналогичной ОС и таким же IP-адресом.
- 2) Выполнить шаги по установке **Nexus** (см. пункт 6.3.1).
- 3) Скопировать сохраненные файлы *.env* и *inventory* или заполнить данные файлы согласно шагам из раздела 6.4.

6.9.6 Удаление недоступного узла кластера

В случае недоступности узла и отсутствия возможности вывести его из кластера стандартными способами через `kubectl`, необходимо удалить информацию о нем из метаданных текущего кластера Kubernetes.

 Компоненты Kubernetes на отказавшем узле должны быть полностью удалены. Например, если возможно, следует выполнить команду `kubeadm reset` и удалить конфигурационные файлы и сертификаты в `/etc/kubernetes/`, `/var/lib/kubelet/`, `/var/lib/etcd/`, чтобы избежать незапланированного повторного подключения узла к кластеру.

6.9.6.1 Удаление недоступного узла

Для удаления недоступного узла из кластера необходимо выполнить следующие действия:

- 1) Определить название недоступного узла, вводом команды проверки состояния узлов:

```
kubectl get no -owide
```

Результат выполнения команды приведен на рисунке 43.

В списке узлов недоступный узел будет в статусе **NotReady**.

| | | | | | | | | | |
|--------|----------|---------------|-----|---------|------------|--------|-------------|------------------|----------------------|
| k8s-m1 | Ready | control-plane | 23h | v1.29.6 | 10.10.10.1 | <none> | Astra Linux | 6.1.90-1-generic | containerd://1.7.22 |
| k8s-m2 | NotReady | control-plane | 23h | v1.29.6 | 10.10.10.2 | <none> | Astra Linux | 6.1.90-1-generic | containerd://Unknown |
| k8s-m3 | Ready | control-plane | 23h | v1.29.6 | 10.10.10.3 | <none> | Astra Linux | 6.1.90-1-generic | containerd://1.7.22 |

Рисунок 43 – Таблица со списком узлов

- 2) Удалить информацию о поде с недоступного узла. Пример команды для узла **k8s-m2**:

```
node='k8s-m2'; kubectl get pods --all-namespaces -o wide | grep "$node" | awk '{print $1, $2}' | xargs -L1 kubectl delete pod --grace-period=0 --force -n
```

- 3) Удалить недоступный узел. Пример команды удаления для узла **k8s-m2**:

```
kubectl delete node k8s-m2
```

Если обычной командой удаление не производится, то можно указать ключи для принудительного удаления:

```
kubectl delete node k8s-m2 --force --grace-period=0
```

- 4) Убедиться, что узел удален, вводом команды проверки состояния узлов:

```
kubectl get no -owide
```

- 5) Убедиться, что недоступный узел (например, **k8s-m2**) удален из **etcd**. Просмотр

информации об узлах в **etcd**:

```
ETCDCTL_API=3 etcdctl \
--endpoints=https://127.0.0.1:2379 \
--cacert=/etc/kubernetes/pki/etcd/ca.crt \
--cert=/etc/kubernetes/pki/etcd/server.crt \
--key=/etc/kubernetes/pki/etcd/server.key \
get / --prefix --keys-only | grep "/registry/minions/"

/registry/minions/k8s-m1
/registry/minions/k8s-m3
```

-  Исполняемый файл **etcdctl** можно скачать с Nexus дистрибутива ПК «Efros DO». Например, http://127.0.0.1:8081/repository/dependencies/bin_utils/etcd-v3.5.17-linux-amd64.tar.gz.

Если запись все еще существует, то необходимо ее удалить с помощью команды:

```
ETCDCTL_API=3 etcdctl \
--endpoints=https://127.0.0.1:2379 \
--cacert=/etc/kubernetes/pki/etcd/ca.crt \
--cert=/etc/kubernetes/pki/etcd/server.crt \
--key=/etc/kubernetes/pki/etcd/server.key \
del /registry/minions/k8s-m2
```

- 6) Если недоступный узел был **master-узлом**, требуется удалить запись о соответствующем **member** из кластера **etcd**. Для этого необходимо произвести следующие действия:
- Определить **MEMBER_ID**, выполнив команду:

```
ETCDCTL_API=3 etcdctl \
--endpoints=https://127.0.0.1:2379 \
--cacert=/etc/kubernetes/pki/etcd/ca.crt \
--cert=/etc/kubernetes/pki/etcd/server.crt \
--key=/etc/kubernetes/pki/etcd/server.key \
member list -w table
```

Результат выполнения команды приведен на рисунке 44.

| ID | STATUS | NAME | PEER ADDRS | CLIENT ADDRS | IS LEARNER |
|------------------|---------|--------|-------------------------|-------------------------|------------|
| 2288655769347fe3 | started | k8s-m2 | https://10.10.10.2:2380 | https://10.10.10.2:2379 | false |
| 379a62d4bcdce61f | started | k8s-m3 | https://10.10.10.3:2380 | https://10.10.10.3:2379 | false |
| ea26e4b22c1bfe4b | started | k8s-m1 | https://10.10.10.1:2380 | https://10.10.10.1:2379 | false |

Рисунок 44 – Таблица со значениями **MEMBER_ID**

Таблица со значениями **MEMBER_ID** не показывает актуальное состояние узлов **etcd** (статус **Started** не меняется динамически).

Так как известно, что узел **k8s-m2** недоступен, то можно сразу перейти к удалению, используя **MEMBER_ID**, соответствующий названию узла.

- Удалить недоступный **member** из кластера **etcd** на **master-узле** с помощью команды:

```
etcdctl member remove <MEMBER_ID>
```

Например, для узла **k8s-m2** ID соответствует значению 2288655769347fe3:

```
ETCDCTL_API=3 etcdctl \
--endpoints=https://127.0.0.1:2379 \
--cacert=/etc/kubernetes/pki/etcd/ca.crt \
--cert=/etc/kubernetes/pki/etcd/server.crt \
--key=/etc/kubernetes/pki/etcd/server.key \
member remove 2288655769347fe3
```

- Проверить состояние кластера и подтвердить удаление недоступного **master-узла**, выполнив команду просмотра состояния кластера **etcd**:

```
ETCDCTL_API=3 etcdctl \
--endpoints=https://127.0.0.1:2379 \
--cacert=/etc/kubernetes/pki/etcd/ca.crt \
--cert=/etc/kubernetes/pki/etcd/server.crt \
--key=/etc/kubernetes/pki/etcd/server.key \
endpoint health --cluster -w table
```

Результат выполнения команды приведен на рисунке 45.

| ENDPOINT | HEALTH | TOOK |
|---|--------|------------|
| https://10.10.10.1:2379 | true | 12.99748ms |
| https://10.10.10.3:2379 | true | 10.61678ms |

Рисунок 45 – Таблица состояния кластера

По таблице состояния кластера видно, что остались две доступные конечные точки. По IP-адресам можно сопоставить названия и ID доступных узлов в таблице **MEMBER_ID** (см. рис. 44).

6.9.6.2 Решение проблемы с подами в статусе Pending

Статус **Pending** у подов возникает из-за невозможности подключения Persistent Volume (PV), привязанного к недоступному узлу через Local Volume Provisioner.

Поскольку PV с типом Local имеют жесткую привязку к конкретному узлу, а узел недоступен, связанный Persistent Volume Claim (PVC) не может получить доступ к требуемому хранилищу.

Для решения проблемы необходимо выполнить следующие действия:

- 1) Удалить PVC с метками недоступного узла. Пример команды для недоступного узла **k8s-m2**:

```
node=k8s-m2; kubectl get pvc -n edo -o jsonpath='{range .items[?(@.metadata.annotations.volume\\.kubernetes\\.io/selected-node=="$node\\")]}{.metadata.name}{\'\\n\'}{end}' | xargs -L1 kubectl delete pvc -n edo
```

- 2) Удалить PV связанные с недоступным узлом. Пример команды для недоступного узла **k8s-m2**:

```
node=k8s-m2; kubectl get pv -o jsonpath='{range .items[?(@.metadata.annotations.local\\.path\\.provisioner/selected-node=="$node\\")]}{.metadata.name}{\'\\n\'}{end}' | xargs -L1 kubectl delete pv
```

После удаления ресурсов под будет запущен с использованием доступных ресурсов.

6.9.6.3 Восстановление работы Minio

В случае если сервис «edo-store-minio» был расположен на недоступном узле и его PV был удален, то для восстановления работы сервиса необходимо заново создать ресурс PVC со следующими параметрами:

```
kubectl apply -f - <<EOF
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: minio-local-volume
  namespace: edo
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
EOF
```

В результате под сервиса «edo-store-minio» будет запущен.

6.9.6.4 Добавление нового узла с ролью «NAC»

В случае если был удален узел с ролью «NAC», то на новой необходимо указать соответствующую метку, выполнив команду:

```
kubectl label nodes <название ноды> nac=true
```

Затем перезапустить сервис гостевого портала «edo-guest-portal-service» командой:

```
kubectl rollout restart deploy edo-guest-portal-service -n edo
```

В результате сервис гостевого портала должен запуститься на указанном узле.

6.10 Дополнительные функциональные возможности кластера

Перечень дополнительных функциональных возможностей при работе с кластером:

- 1) Резервное копирование кластера.

Описание приведено в документе «Инструкция по резервному копированию кластера ПК «Efros DO».

- 2) Интеграция с системой мониторинга кластера «Zabbix» версии 6.4 и выше.

Работа с программным обеспечением «Zabbix» доступно при установке комплекса на базе Kubernetes на ЭВМ под управлением Astra Linux Special Edition (v. 1.7.4).

Программное обеспечение «Zabbix» можно скачать на сайте www.zabbix.com либо запросить в службе технической поддержки ПК «Efros DO».

Описание установки приведено в документе «Инструкция по установке системы мониторинга кластера «Zabbix».

- 3) Интеграция с облачной инфраструктурой «Selectel».

Описание приведено в документе «Инструкция по установке кластера «Selectel».

Инструкции расположены в архиве «Инструкции Efros DO.zip», который входит в комплект пользовательской документации ПК «Efros DO».

6.11 Обновление комплекса на базе Kubernetes

6.11.1 Требования при обновлении комплекса

Для корректного обновления комплекса на базе Kubernetes необходимо выполнение следующих требований:

- 1) Перед обновлением комплекса рекомендуется сделать резервную копию БД системы через раздел «Настройки» → «Резервные копии» (подробнее см. документ «Руководство пользователя. Часть 1. Настройка и администрирование»). Дополнительно можно сделать резервную копию кластера в соответствии с документом «Инструкция по резервному копированию кластера ПК «Efros DO».
- 2) Перед обновлением необходимо вывести комплекс из домена. После завершения обновления при необходимости ввести комплекс в домен.
- 3) Перед выполнением процедуры обновления кластерной версии комплекса необходимо предварительно удалить старую версию комплекса со всех используемых ВМ.
- 4) Проводить обновление комплекса необходимо с Nexus-хоста (см. пункт 6.3.2).
- 5) При необходимости перехода на плагин **Cilium** нужно произвести действия, приведенные в пункте 6.11.3.

- (i)** При обновлении комплекса следует учитывать, что время запуска сервиса `edo-ci-service` увеличено (до часа). Время зависит от количества шифруемых данных БД (паролей, ключей).

6.11.2 Обновление комплекса

- (i)** Ниже приведен пример описания обновления ПК «Efros DO» версии 2.12 до версии 2.13 (версия дистрибутива для обновления: 0.0.8).

Для обновления ПК «Efros DO» необходимо выполнить следующие действия:

- 1) В папке **Nexus** запустить `./delete.sh` для удаления зависимостей дистрибутива 2.12.
- 2) Запустить `./deploy.sh` (запуск производится около 5-7 минут), аналогично действиям указанным в пункте 6.3.1.
- 3) Дождаться автоматической распаковки архив с дистрибутивом новой версии 2.13 в папку `/opt/edo-distr_2_13`.
- 4) Переместить файл `inventory` и `.env` из папки с дистрибутивом со старой версией 2.12 в папку `/opt/distr_2_13/`.
- 5) Открыть файл `.env` в папке `/opt/distr_2_13/` и добавить следующие переменные в конце файла:

```
NEXUS_REGISTRY_ADDRESS="http://10.200.200.8:5000"
# Адрес docker-registry для установки образов (указывается ip-адрес хоста, где развернут nexus)

NEXUS_REPOSITORY_ADDRESS="http://10.200.200.8:8081"
# Адрес репозитория для установки зависимостей (указывается тот ip-адрес хоста, где развернут nexus)

CUSTOM_REGISTRY_ADDRESS=""
# Адрес custom docker-registry для установки кластера EDO из клиентского или из облачного docker-registry
```

где:

NEXUS_REGISTRY_ADDRESS – адрес docker-registry для установки образов комплекса. Указывается IP-адрес хоста с Nexus и порт;

NEXUS_REPOSITORY_ADDRESS – адрес репозитория для установки зависимостей. Указывается IP-адрес хоста с Nexus и порт;

CUSTOM_REGISTRY_ADDRESS – адрес custom docker-registry для установки кластера из клиентского или облачного docker-registry. Параметр можно оставить

пустым.

Удалить следующие переменные в конце файла `.env`:

```
NEXUS_PROTOCOL="http"  
NEXUS_ADDRESS="10.116.41.140"  
REGISTRY_PORT="5000"  
REPOSITORY_PORT="8081"
```

-  При обновлении комплекса версии 2.11 или ниже дополнительно в файл `.env` необходимо добавить следующие переменные:

```
# Список узлов для сервисов NAC  
NAC_NODES="master_3,worker_2"  
  
# Флаг для установки standalone версии  
SINGLE_NODE="false"
```

где:

`NAC_NODES` – содержит список узлов (как в файле *inventory*) для ролей модуля «Efros NAC», поле может быть пустым;

`SINGLE_NODE` – флаг для установки версии кластера на базе на базе Docker-контейнера (*standalone*), для установки кластера должен иметь значение «*false*».

- 6) В папке `/opt/distr_2_13/` запустить шаги по очереди: `-s0, -s1, -s3`.
- 7) Запустить шаг `-s7`. Выведется предупреждение о необходимости сохранения ключа шифрования. Для продолжения установки необходимо ввести «*Y*» или «*у*».

-  В процессе обновления ПК «Efros DO» выполняется шифрование чувствительных данных в базе данных.

После обновления комплекса для сохранения ключа шифрования рекомендуется сделать резервную копию ресурса Kubernetes – **`machine-id-config`**.

Для этого можно использовать команду:

```
kubectl get configmap machine-id-config -n edo -o yaml | base64 -w0 > machine-id-config.yaml
```

- 8) В появившемся меню требуется выбрать 1 (Обновить EDO).

Текущая установленная версия EDO: 2.12, дистрибутив: efros-do-0.0.7
Версия EDO для обновления: 2.13, дистрибутив: efros-do-0.0.8

Выберите действие:

- 1 – Обновить EDO
- 2 – Прервать установку

i После завершения обновления комплекса версии 2.10 или ниже автоматически производится запуск миграции SNMP профилей из БД, в которой хранятся данные контроля устройств, в БД микросервиса объектов защиты.

- 9) Проверить, что ПК «Efros DO» корректно обновилась, выполнив команду:

```
kubectl get po -n edo
```

- 10) Для сохранения ключа шифрования БД рекомендуется сделать резервную копию ресурса Kubernetes – **machine-id-config**, выполнив команду:

```
kubectl get configmap machine-id-config -n edo -o yaml | base64 -w0 > machine-id-config.yaml
```

! Если при обновлении комплекса до версии 2.13 произошла ошибка, то шаг «Установка Nginx Ingress Controller» не будет выполнен.

Для продолжения обновления необходимо произвести следующие действия:

1. Проверь текущую версию комплекса командой:

```
helm list -n edo
```

2. Если комплекс не обновился, то необходимо исправить ошибку, которая помешала обновлению. После повторно запустить шаг с ключом **-s7**.
3. Если комплекс обновился и указана версия 2.13, то необходимо запустить шаг с ключом **-s6** (Установить Nginx Ingress Controller). После повторно запустить шаг с ключом **-s7**.

6.11.3 Переход на плагин *Cilium*

-  Переход на плагин *Cilium* доступен для обновляемых комплексов версии 2.11 (или 2.12) до версии 2.13.

Переход на плагин *Cilium* необходимо производить для оптимизации связи между узлами кластера.

Для перехода на плагин *Cilium* требуется произвести следующие действия:

- 1) Открыть порты 8472/UDP, 4240/TCP между узлами кластера.
- 2) Убедиться, что менеджер репозиториев *Nexus* работает корректно, перейдя на веб-интерфейс *Nexus*.
- 3) Скопировать helm-chart *cilium-1.16.4.tgz* из папки хоста с Nexus */opt/edo-distr-2_13/roles/install_cni/files/* на домашнюю директорию первого узла, выполнив команду:

```
sudo scp /opt/edo-distr-2_13/roles/install_cni/files/cilium-1.16.4.tgz {пользователь}@{ip адрес 1 узла}:~/
```

- 4) Из домашней директории скопировать helm-chart *cilium-1.16.4.tgz* в папку */opt/efros-do/helm-charts/* на первом узле, выполнив команду:

```
sudo cp cilium-1.16.4.tgz /opt/efros-do/helm-charts/
```

- 5) Удалить *weave CNI* на первом узле, выполнив команду:

```
sudo kubectl delete -n kube-system -f /opt/efros-do/weave.yml
```

- 6) Удалить файл */etc/cni/net.d/10-weave.conf* на каждом из узлов, используя команду:

```
sudo rm /etc/cni/net.d/10-weave.conf
```

- 7) Удалить *kube-proxy daemonset*, выполнив команду:

```
sudo kubectl delete daemonset -n kube-system kube-proxy
```

8) Удалить **weave** интерфейс каждом из узлов, используя команду:

```
sudo ip link set weave down
sudo ip link del weave
```

9) Проверить права и владельца папки **ls -al /opt/cni/** на каждом узле, используя команду:

```
ls -al /opt/cni/
итого 12
drwxr-xr-x 3 root root 4096 янв 14 10:15 .
drwxr-xr-x 8 root root 4096 янв 16 10:16 ..
drwxr-xr-x 2 root root 4096 янв 16 10:38 bin
# Если владелец не root и права отличные от того, что выше, то
нужно привести в соответствие
sudo chown -R root:root /opt/cni/
```

10) На первом узле перейти в папку **/opt/efros-do/helm-charts/** и установить Cilium, выполнив команду:

```
helm install cilium cilium-1.16.4.tgz --namespace kube-system \
--set k8sServiceHost=<ip адрес VIP> \
--set k8sServicePort=<порт VIP> \
--set image.repository=":<порт
nexus>/cilium/cilium" \
--set hubble.relay.image.repository=":<порт
nexus>/cilium/hubble-relay" \
--set hubble.backend.image.repository=":<порт
nexus>/cilium/hubble-ui-backend" \
--set hubble.frontend.image.repository=":<порт
nexus>/cilium/hubble-ui" \
--set envoy.image.repository=":<порт
nexus>/cilium/cilium-envoy" \
--set operator.image.repository=":<порт
nexus>/cilium/operator" \
--set ipam.operator.clusterPoolIPv4PodCIDRList=10.242.0.0/16
```

Для обновления IP-адресов сервисов нужно выполнить следующие действия:

- 1) Дождаться запуска плагина **Cilium**. Для просмотра состояния необходимо использовать команду:

```
sudo kubectl get po -n kube-system -w
```

- 2) Перезапустить **core-dns**, выполнив команду:

```
sudo kubectl delete pod -n kube-system -l k8s-app=kube-dns
```

- 3) Перезапустить поды **certmanager** на первом узле, выполнив команду:

```
sudo kubectl delete po -n certmanager -l app.kubernetes.io/instance=cert-manager
```

- 4) Перезапустить поды комплекса, поочередно выполнив следующие команды:

```
sudo kubectl get deployments -n edo -o name | xargs -I {} sudo kubectl rollout restart {} -n edo
sudo kubectl get sts -n edo -o name | xargs -I {} sudo kubectl rollout restart {} -n edo
# Последовательно удалить поды zookeeper, kafka и entity-operator, дожидаясь пока поды перейдут в состояние Running
sudo kubectl delete po -n edo edo-kafka-cluster-zookeeper-0
sudo kubectl delete po -n edo edo-kafka-cluster-zookeeper-1
sudo kubectl delete po -n edo edo-kafka-cluster-zookeeper-2
sudo kubectl delete po -n edo edo-kafka-cluster-kafka-0
sudo kubectl delete po -n edo edo-kafka-cluster-kafka-1
sudo kubectl delete po -n edo edo-kafka-cluster-kafka-2
sudo kubectl delete po -n edo edo-kafka-cluster-entity-operator-<hash пода>
```

- 5) Проверить работоспособность системы, выполнив команду:

```
sudo kubectl get po -n edo
```

После завершения перехода на плагин **Cilium**, между узлами могут остаться открытые порты 6783,6784/UDP и 6783/TCP. При необходимости их можно закрыть.

6.11.4 Обновление ОС узла кластера

На узлах кластера ПК «Efros DO» установлена операционная система Astra Linux SE.

- i Ниже приведен пример описания обновления Astra Linux SE v. 1.7.4 до v. 1.7.6.
- i Команды необходимо вводить от имени суперпользователя **root** либо, используя команду **sudo**.

Для онлайн обновления ОС Astra Linux SE узла кластера необходимо произвести следующие действия:

- 1) Установить утилиту обновления, выполнив команду:

```
sudo apt install astra-update
```

- 2) На первом узле выполнить команду обновления:

```
sudo astra-update -A -r
```

Результат успешного выполнения команды:

```
Обновление успешно установлено
```

```
Для применения изменений в ядре или модулях нужна перезагрузка
```

- 3) Выполнить команду перезагрузки узла:

```
sudo reboot
```

- 4) Проверить статусы состояния узла, выполнив команду:

```
kubectl get nodes
```

Дождаться, когда статус узла примет значение «Ready».

- 5) Проверить статусы всех подов, выполнив команду:

```
kubectl get pods -n edo
```

Дождаться, когда статусы подов примут значения «Running».

- 6) Повторить последовательность действий на узлах 2 и 3.

6.12 Удаление кластера

Для удаления ПК «Efros DO» из ***kubernetes*** кластера необходимо на Nexus-хосте (см. пункте 6.3.2) выполнить следующую команду:

```
./__install.sh -u
```

! При удалении ПК «Efros DO» также будут удалены ключ шифрования базы данных и сертификаты.

Это означает, что данный экземпляр БД невозможно будет использовать при новой установке комплекса, данные будут утеряны.

Если при новой установке необходимо будет использовать текущий экземпляр БД, необходимо сохранить настройки ресурса ***edo\configmap\machine-id-config***. Для сохранения ключа шифрования БД рекомендуется использовать команду:

```
kubectl get configmap machine-id-config -n edo -o yaml |  
base64 -w0 > machine-id-config.yaml
```

Для сохранения сертификатов рекомендуется использовать команду:

```
kubectl get secrets -n edo --field-selector  
type=kubernetes.io/tls -o yaml > tls-secrets-backup.yaml
```

Сохраненные параметры можно будет применить при новой установке перед шагом «Установка/Обновление EDO».

В открывшемся меню «Выберите способ» необходимо выбрать один из вариантов:

- 1) Soft Reset EDO (удаление только чарта) – удаление компонентов ПК «Efros DO», может использоваться при ошибке обновления;
- 2) Hard Reset EDO (удаление чарта и хранилищ) – удаление компонентов ПК «Efros DO», ***namespace edo*** и хранилища для ***opensearch*, *kafka* и *minio***, может использоваться для последующей установки обновленной версии ПК «Efros DO» в кластер;
- 3) Hard Reset k8s (полное удаление кластера и его компонентов) – удаление кластера k8s с узлов. При выборе данного варианта появится еще одно подменю для того, чтобы удостовериться, что пользователь точно готов удалить кластер:
 - параллельно (если установка выполняется с отдельного узла) – удаление происходит быстрее за счет параллельности;

- последовательно (если установка выполняется с одного из узлов кластера) – удаление выполняется последовательно: удаляются компоненты с **master_3**, **master_2**, **master_1**.
- 4) Hard Reset k8s custom node (удаление конкретного узла кластера) – удаление узла кластера, который указан в файле *inventory*. Имя узла вводится вручную.

7 Работа с ПК «Efros DO»

Для работы с комплексом необходимо открыть браузер и ввести IP-адрес сервера, на котором производилась установка.

При возникновении предупреждения о ненадежности сертификата безопасности необходимо продолжить открытие веб-сайта, после чего отобразится интерфейс комплекса. Пользователю необходимо выполнить ряд действий:

- активировать комплекс;
- настроить ПК «Efros DO» в соответствии с руководством пользователя.

7.1 Аутентификация пользователя

После установки ПК «Efros DO» в БД комплекса автоматически создается учетная запись пользователя с ролью «GlobalAdministrator»: с логином «SuperAdmin» и паролем «\$Qwerty123456». При первом запуске ПК «Efros DO» для такого пользователя открывается окно смены пароля (рис. 46), в котором необходимо указать в качестве старого пароля значение «\$Qwerty123456», дважды указать новый пароль и нажать кнопку «Сменить пароль».



Рисунок 46 – Окно смены пароля

Будет выполнена автоматическая проверка соответствия пароля заданной в комплексе сложности. По умолчанию пароль должен:

- быть не менее 8 символов;
- содержать хотя бы одну цифру;
- содержать хотя бы одну латинскую букву верхнего регистра;
- содержать хотя бы одну латинскую букву нижнего регистра;
- содержать хотя бы один специальный символ;
- отличаться от предыдущего пароля хотя бы на 3 символа;

— не совпадать с предыдущими тремя паролями пользователя.

При возникновении ошибки в ходе смены пароля в верхней части страницы авторизации отобразится соответствующее сообщение об ошибке.

После успешной смены пароля вновь откроется страница авторизации. Для доступа к веб-приложению ПК «Efros DO» администратору необходимо выполнить повторную авторизацию в комплексе с новым паролем.

7.2 Лицензирование

Для проведения активации комплекса необходимо перейти в раздел «Администрирование», подраздел «Лицензия» (рис. 47).

Возможны два варианта проведения активации комплекса:

- online активация – при наличии подключения к серверу лицензирования;
- offline активация – при отсутствии подключения к серверу лицензирования.

(i) Управление лицензиями для серверов ПК «Efros DO» в системе с иерархией серверов выполняется для каждого сервера ПК «Efros DO» отдельно

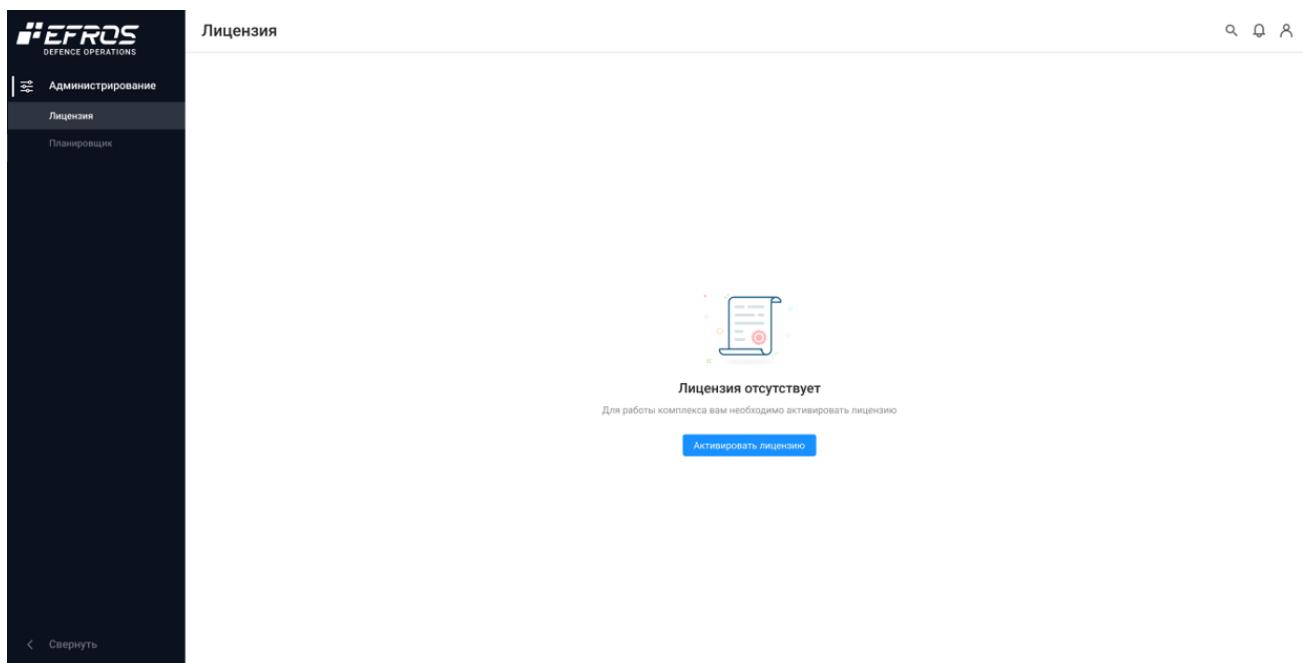


Рисунок 47 – Подраздел «Лицензия»

7.3 Online активация комплекса

Online активация комплекса осуществляется при наличии подключения к сети Интернет и возможности подключения к серверу лицензирования ООО «Газинформсервис».

Для online активации ПК «Efros DO» необходимо нажать кнопку «Активировать лицензию» (см. рис. 47). При подключении к сети Интернет и к серверу лицензирования ООО «Газинформсервис» появится диалоговое окно (рис. 48):

- 1) В окне необходимо указать ключ лицензии, полученный при покупке комплекса.

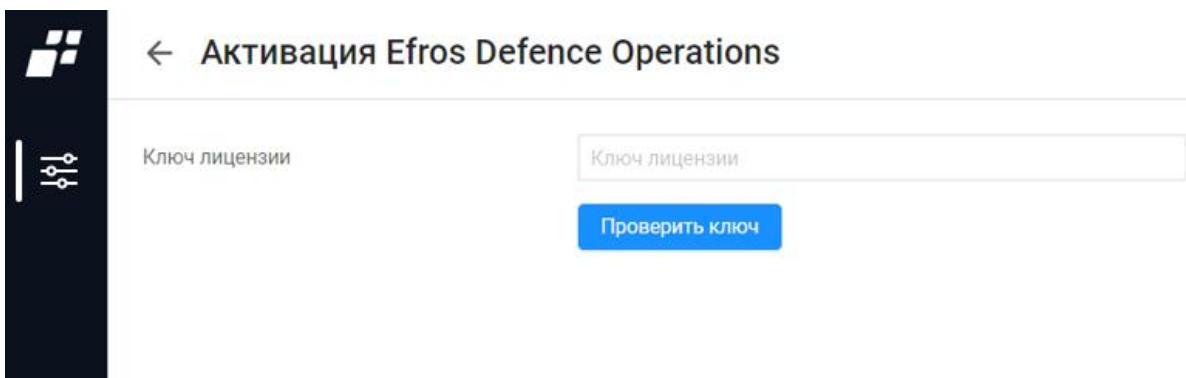


Рисунок 48 – Окно online активации комплекса. Проверка ключа

- 2) Нажать кнопку «Проверить ключ». При успешной проверке напротив ключа лицензии появится галочка «✓».
- 3) Далее указать данные (электронную почту) для получения ключа активации лицензии (рис. 49).

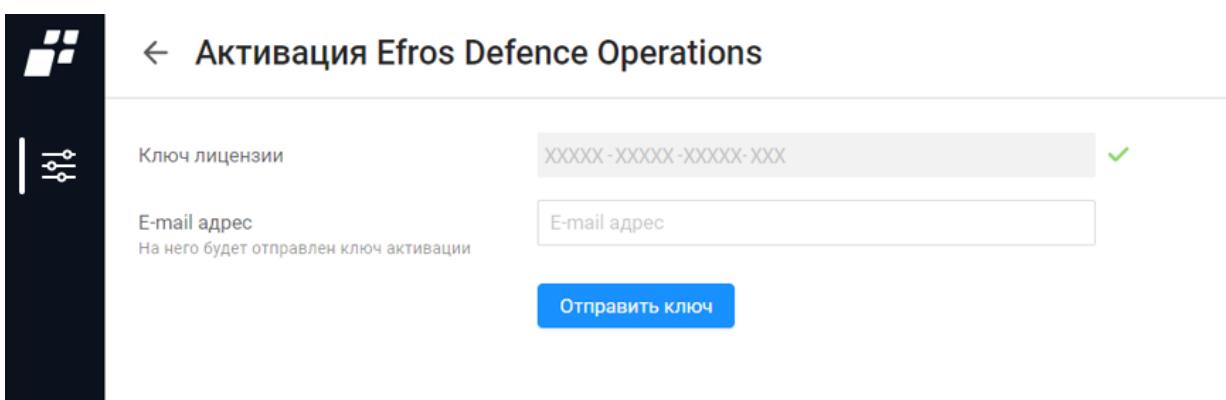


Рисунок 49 – Окно online активации комплекса. Отправка ключа

- 4) Нажать кнопку «Отправить ключ». На указанный адрес электронной почты придет письмо с ключом для активации продукта.



Активацию комплекса необходимо провести в течение 20 минут после формирования запроса на активацию.

- 5) Ввести ключ активации в соответствующее поле (рис. 50) и нажать кнопку «Активировать». Если ключ не был использован в течение 20 минут, то по истечении срока необходимо нажать кнопку «Повторить отправку». На указанную почту придет новое письмо с новым ключом активации лицензии.

Рисунок 50 – Указание необходимых данных для активации

Активация комплекса завершена, на электронный адрес будет отправлен архив *license.zip* с файлом лицензии *license.bin*. Данный файл в дальнейшем можно использовать для переноса лицензии.

После успешного завершения активации лицензии откроется окно с данными лицензии в соответствии с рис. 51. В блоке полей «Информация о лицензии» страницы отобразятся:

- статус лицензии «Активная»;
- использованный при активации ключ лицензии (часть символов заменена символом «*»);
- дата окончания действия лицензии;
- кнопка «Обновить» (подробнее см. подраздел 7.6);
- кнопка «Удалить лицензию» (подробнее см. подраздел 7.7).

В блоке «Техническая поддержка» отобразятся параметры включенной в лицензию технической поддержки:

- статус поддержки «Активная»;
- вид поддержки «Базовая» или «Расширенная»;
- дата окончания технической поддержки;
- количество оставшихся дней до окончания технической поддержки.

Далее на странице в отдельных блоках выведена информация о параметрах включенных в лицензию модулей ПК «Efros DO». Для каждого модуля отображается информация:

- название модуля;
- описание функций;

- количество доступных лицензий на оборудование для каждого модуля (кроме модуля «Efros SDNS»).

Лицензия

Информация о лицензии Активная

Ключ лицензии: FX83J-*****-****-TNF Дата окончания: 29 марта 2074 г.

Обновить Удалить лицензию

Техническая поддержка Активная Расширенная

Дата окончания: 10 февраля 2031 г.

До конца срока действия: 2183 дня

Подключенные модули

Контроль конфигураций и топологии сети NETWORK ASSURANCE

- Контроль изменения конфигураций сетевого оборудования
- Контроль изменения конфигураций межсетевых экранов
- Проверки соответствия безопасности сетевого оборудования
- Проверки соответствия безопасности межсетевых экранов

Доступно лицензий: 462 из 500

Оптимизация и настройка межсетевых экранов FIREWALL ASSURANCE

- Отчет оптимизации правил – выявление теневых, избыточных, неиспользуемых правил
- Зонный анализ – проверка правил межсетевых экранов на соответствие требованиям запрета или разрешения транзитного трафика между зонами
- Стандарты межсетевых экранов – проверка правил на соответствие требованиям безопасности

Доступно лицензий: 469 из 500

Анализ уязвимостей и построение векторов атак VULNERABILITY CONTROL

- Выявление известных уязвимостей на основе версии ОС
- Получение уязвимостей из сторонних сканеров (MaxPatrol®, ReadCheck, SafeERP)
- Построение векторов атак

Доступно лицензий: 484 из 500

Контроль целостности и проверки соответствия INTEGRITY CHECK COMPLIANCE

- Контроль изменения конфигураций ОС, ППО, виртуализации, контейнеров и средств оркестрации
- Проверка соответствия безопасности ОС, ППО, виртуализации, контейнеров и средств оркестрации

Доступно лицензий: 497 из 500 Доступно лицензий: СУБД, 498 из 500

Доступно лицензий: Гипервизоры, 500 из 500 Доступно лицензий: Ноды контейнеризации, 500 из 500

Сбор статистики по потокам данных в сети NETWORK FLOW ANALYSIS

- Представление информации по соединениям с параметрами скорости, длительности и принадлежности к адресам
- Сбор статистики использования сетевого трафика по соединениям и анализ активности
- Работа с протоколами NetFlow, sFlow, IPFIX и NetStream

Доступно лицензий (источники трафика): 500 из 500

Разграничение и контроль доступа в сети NETWORK ACCESS CONTROL

- Аутентификация и авторизация устройств в сети посредством 802.1x, MAB, профилирования
- Поддержка протоколов RADIUS, в том числе RADIUS CoA, TACACS+

Доступно лицензий: 222 из 501

Сетевое оборудование: 279
Активные сессии доступа в сеть: 0
Активные сессии доступа на оборудование: 0

Рисунок 51 – Активация комплекса завершена

7.4 Offline активация комплекса

Проведение offline активации осуществляется при отсутствии подключения к сети Интернет либо, если связь с сервером лицензирования ООО «Газинформсервис» не установлена. В таком случае, при нажатии кнопки «Активировать лицензию», откроется окно с соответствующим сообщением (рис. 52).

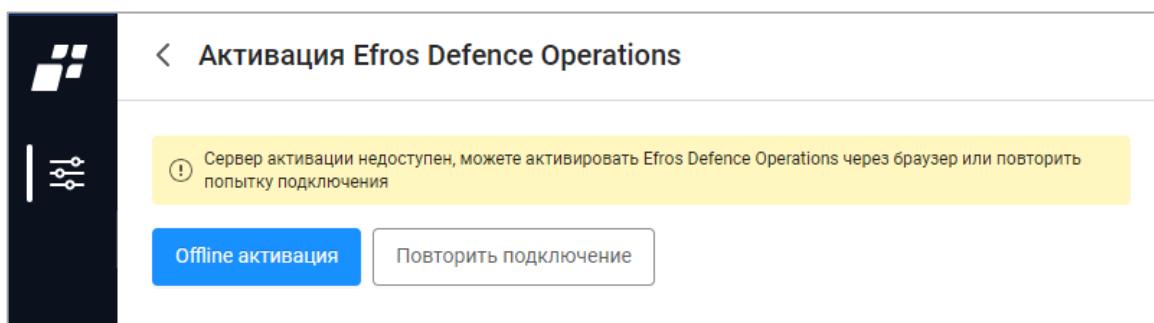


Рисунок 52 – Окно активации

Для offline активации ПК «Efros DO» необходимо выполнить следующие действия:

- 1) Нажать кнопку «Активировать лицензию» (см. рис. 47). Откроется диалоговое окно (см. рис. 52).
- 2) Нажать кнопку «Offline активация», откроется окно ввода параметров offline активации программного комплекса (рис. 53).

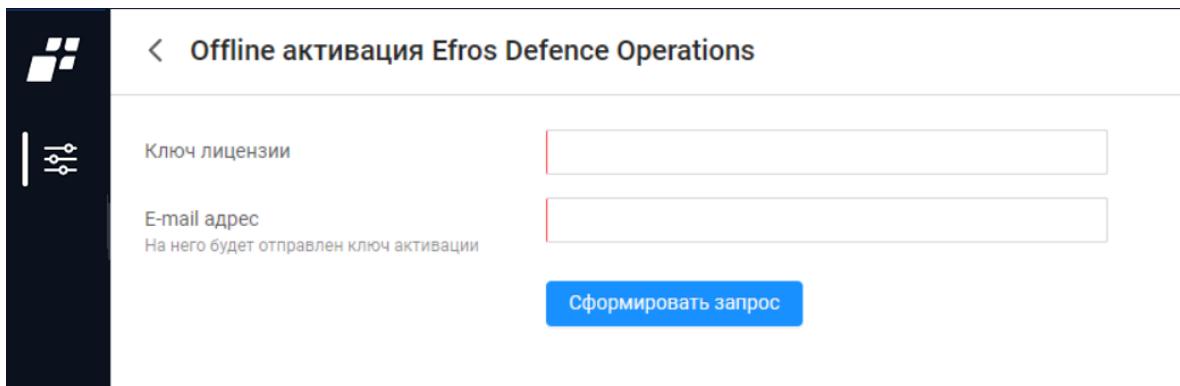


Рисунок 53 – Окно ввода параметров offline активации

- 3) Указать ключ активации, адрес электронной почты и нажать кнопку «Сформировать запрос». В результате будет сформирован файл с запросом на лицензию формата .json – **request.json** (рис. 54).

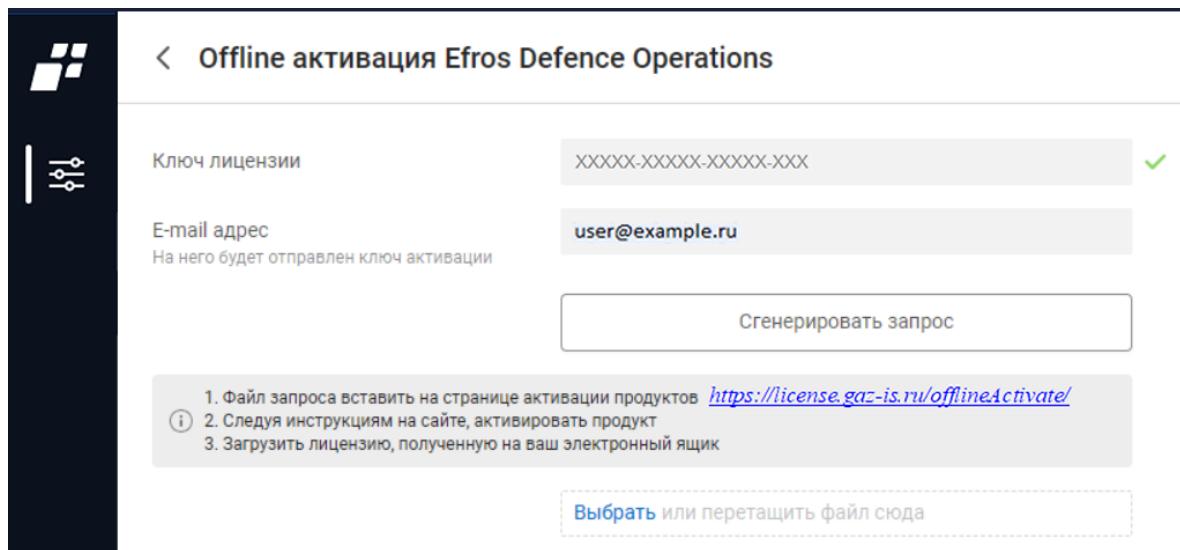


Рисунок 54 – Формирование файла с запросом на лицензию для offline активации

- 4) Перейти на другую ЭВМ с устойчивым подключением к сети Internet, открыть браузер и указать адрес для проведения offline активации продукта: <https://license.gaz-is.ru/offlineActivate/> (рис. 55).
- 5) Открыть ранее сгенерированный файл **request.json** и скопировать содержимое файла в соответствующее окно (см. рис. 55) либо воспользоваться кнопкой «Выберите файл», затем нажать кнопку «Активировать». Будет отправлено

письмо на электронную почту, указанную для запроса, с ключом активации (рис. 56).

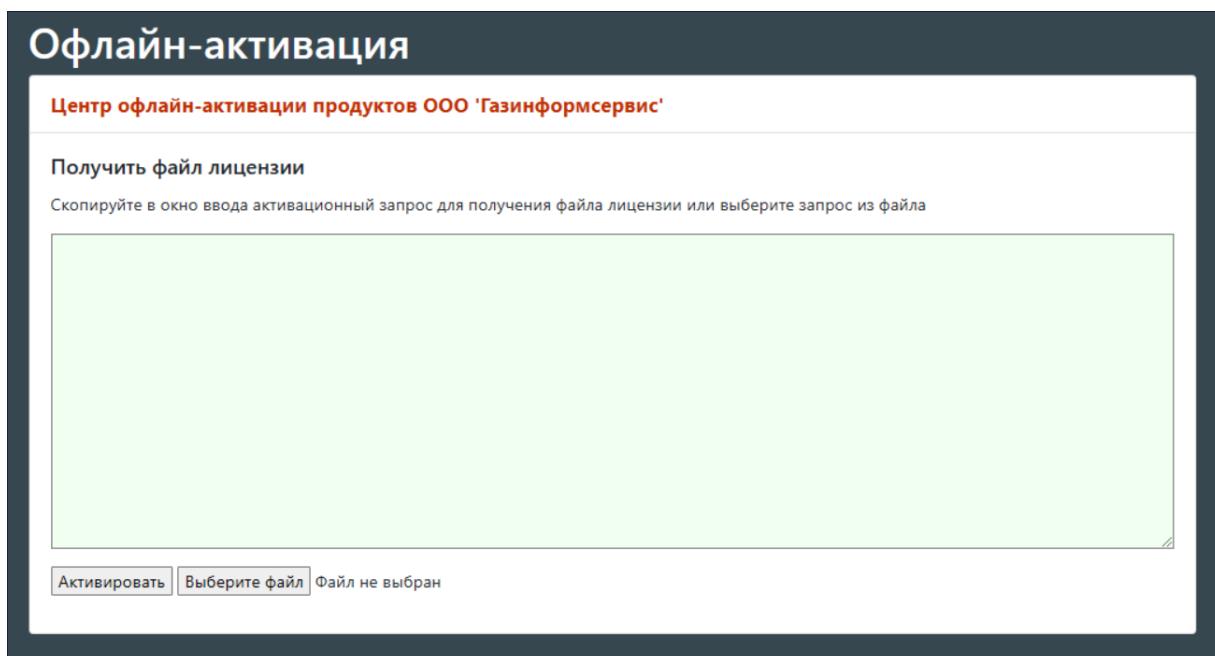


Рисунок 55 – Центр активации продуктов

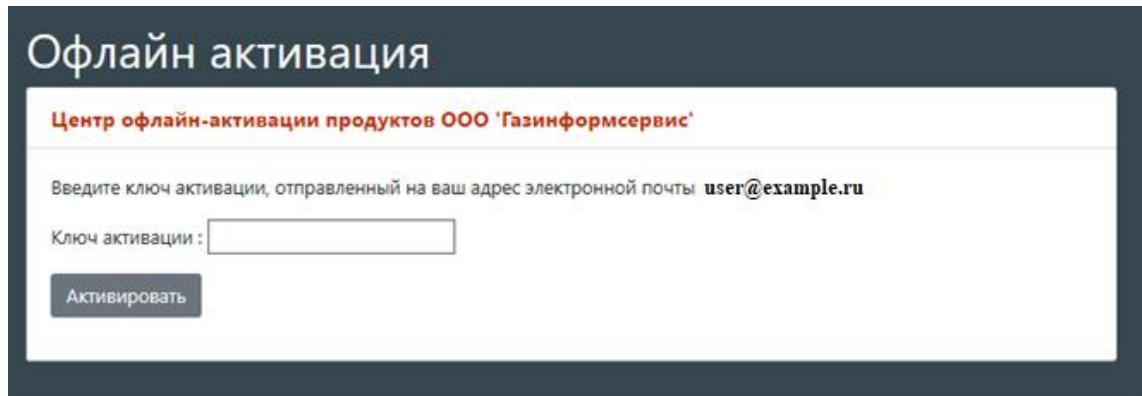


Рисунок 56 – Окно для ввода ключа активации

- 6) Указать полученный ключ активации и нажать кнопку «Активировать». В случае успешного прохождения активации на электронный адрес будет отправлено письмо с архивом *license.zip*, в котором содержится файл *license.bin* и появится соответствующее информационное сообщение в веб-браузере (рис. 57).
- 7) Перейти на ЭВМ, на которой необходимо активировать комплекс, и в окне offline активации (см. рис. 54) с помощью кнопки «Загрузить лицензию», загрузить полученный файл лицензии *license.bin*. Автоматически откроется вкладка с активированной лицензией. Offline активация комплекса завершена.

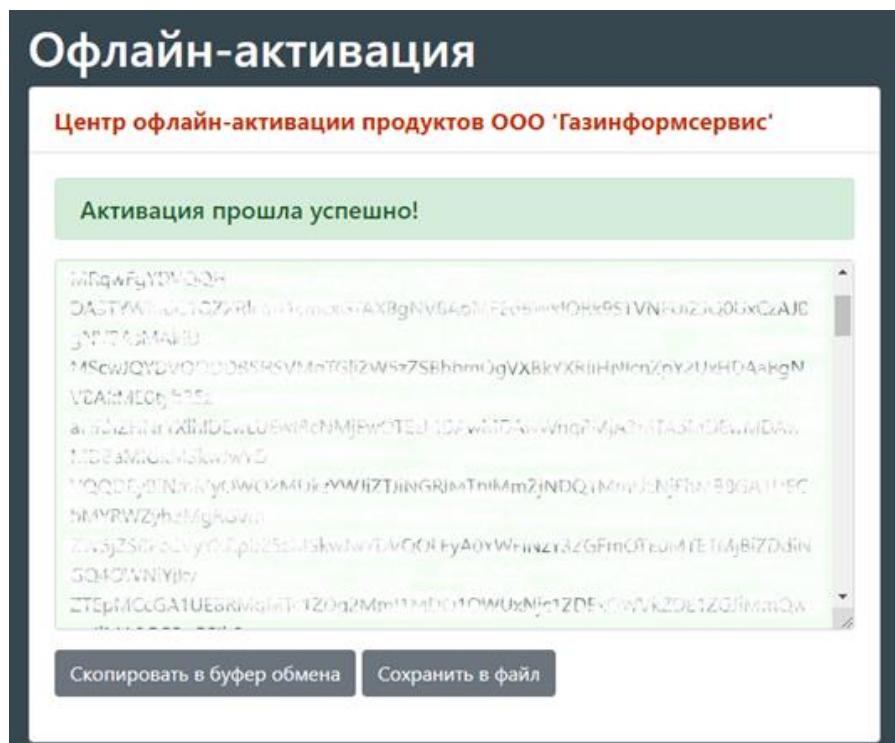


Рисунок 57 – Успешное прохождение активации

После успешного завершения активации лицензии на странице «Лицензия» веб-приложения комплекса отобразятся данные лицензии, в поле «Информация о лицензии» отобразится статус лицензии «Активная» (см. рис. 51).

7.5 Реактивация лицензии комплекса

Для осуществления переноса лицензии необходимо после установки комплекса на другую ЭВМ, выполнить следующие действия:

- 1) Перейти в диалоговое окно активации комплекса (Администрирование/Лицензия) и указать ключ лицензии, полученный при покупке комплекса. Нажать кнопку «Активировать лицензию», появится сообщение в соответствии с рис. 58.

Активация Efros Defence Operations

Данная лицензия была активирована ранее, вы можете ее реактивировать или ввести другой ключ.
При реактивации лицензии, активированная ранее лицензия будет деактивирована.

Ключ лицензии

XXXXX - XXXXX - XXXXX - XXX

Реактивировать

Проверить снова

Рисунок 58 – Повторная активация лицензии

- 2) Нажать кнопку «Реактивировать». При наличии устойчивого подключения к сети Internet, дальнейшая активация комплекса осуществляется online. При успешном завершении проверки введенного ключа активации напротив поля появится галочка «».

← Активация Efros Defence Operations

Ключ лицензии

Файл лицензии

E-mail адрес
На него будет отправлен ключ активации

Отправить ключ

For the 'License Key' field, there is an information message: **ⓘ Для реактивации необходимо приложить файл ранее активированной лицензии**.

Рисунок 59 – Ввод данных

- 3) Приложить файл **license.bin**, который был получен ранее при активации комплекса на другой ЭВМ.
- 4) Указать электронную почту и нажать кнопку «Отправить ключ» (см. рис. 59).

- ⓘ** Необходимо указать адрес электронной почты, который использовался при прошлой активации комплекса. В случае, если адреса электронной почты не будут совпадать, появится сообщение «Для данного ключа уже задан e-mail. Для изменения свяжитесь с технической поддержкой».
- 5) На указанный адрес электронной почты будет отправлен ключ активации продукта.
- ⓘ** Активацию комплекса необходимо провести в течение 20 минут после формирования запроса на активацию (рис. 60).
- 6) Ввести ключ активации, полученный по электронной почте, в соответствующее поле (см. рис. 60) и нажать кнопку «Активировать». Перенос ключа активации лицензии завершен.

← Активация Efros Defence Operations

Ключ лицензии ✓

(i) Для реактивации необходимо приложить файл ранее активированной лицензии

Файл лицензии [Скачать](#)

E-mail адрес

На него будет отправлен ключ активации

Ключ активации Повторить отправку

Ключ отправлен. Время действия ключа 19:55

[Активировать](#)

Рисунок 60 – Ввод ключа активации

Реактивация лицензии возможна также в offline режиме. Алгоритм действий аналогичен проведению offline активации комплекса (см. пункт 7.4).

7.6 Обновление лицензии комплекса

Для обновления лицензии необходимо выполнить следующие действия:

- 1) Перейти в раздел «Администрирование» → «Лицензия».
- 2) На открывшейся странице управления лицензией комплекса (см. рис. 51) нажать кнопку «Обновить».
- 3) При наличии подключении к сети Интернет и к серверу лицензирования ООО «Газинформсервис» произойдет подключение к серверу и проверка наличия обновления лицензии. При наличии обновления будет выполнено обновление лицензии. При отсутствии обновления будет выведено соответствующее сообщение.

При отсутствии подключения к сети Интернет и к серверу лицензирования будет выведено соответствующее сообщение. Пользователю для внесения обновлений в лицензию необходимо удалить текущую лицензию в соответствии с пунктом 7.7 и выполнить Offline активацию комплекса с обновленной лицензией в соответствии с пунктом 7.4.

7.7 Удаление лицензии

Для удаления лицензии необходимо выполнить следующие действия:

- 1) Перейти в раздел «Администрирование» → «Лицензия».
- 2) На открывшейся странице управления лицензией комплекса (см. рис. 45) нажать кнопку «Удалить».
- 3) Подтвердить операцию удаления лицензии в открывшемся окне подтверждения.

- 4) Произойдет возврат на страницу управления лицензией комплекса, пользователю в интерфейсе ПК «Efros DO» будет доступен только раздел «Администрирование» → «Лицензия» для активации новой лицензии.

8 Windows-агент ПК «Efros DO»

8.1 Установка windows-агента

Windows-агент устанавливается на контролируемые сервера под управлением ОС MS Windows и предназначен для обеспечения операций контроля целостности файловых объектов. Для установки windows-агента необходимо войти на контролируемый сервер от имени учетной записи с правами администратора этого сервера, скопировать на контролируемый сервер файл ***Efros Config Inspector Agent <версия>.msi*** и запустить его на исполнение.

Откроется окно мастера установки windows-агента, в котором следует выбрать папку для установки агента или оставить заданную по умолчанию (**C:\Program Files\EFROS Config Inspector 4**) и нажать кнопку «Далее» (рис. 61).

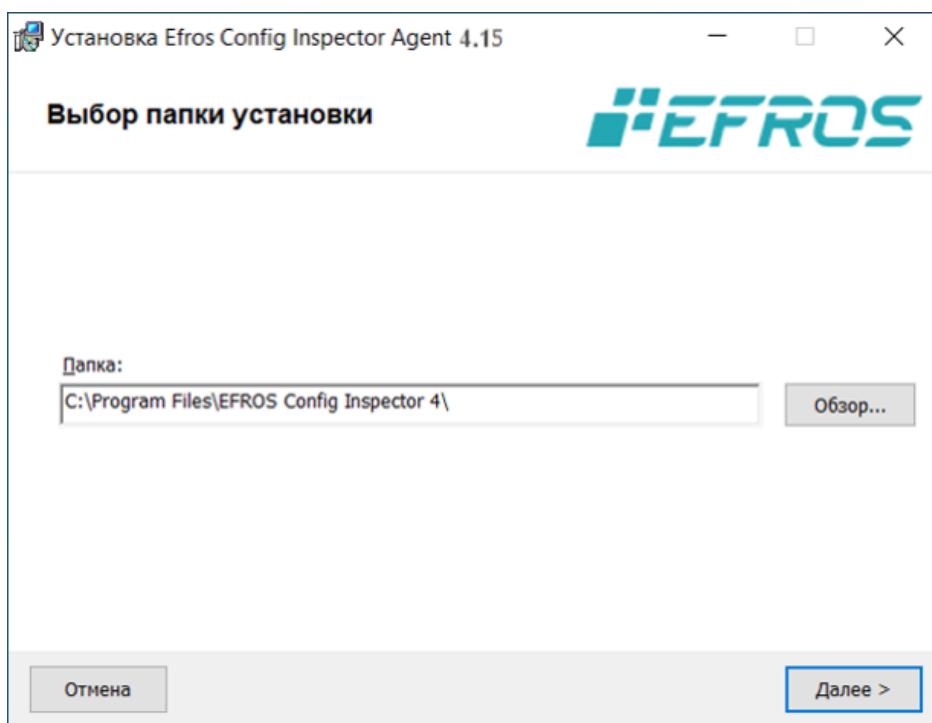


Рисунок 61 – Диалоговое окно выбора папки для установки windows-агента

В диалоговом окне готовности мастера к установке (рис. 62) для запуска процесса установки с заданными ранее параметрами следует нажать кнопку «Установить».

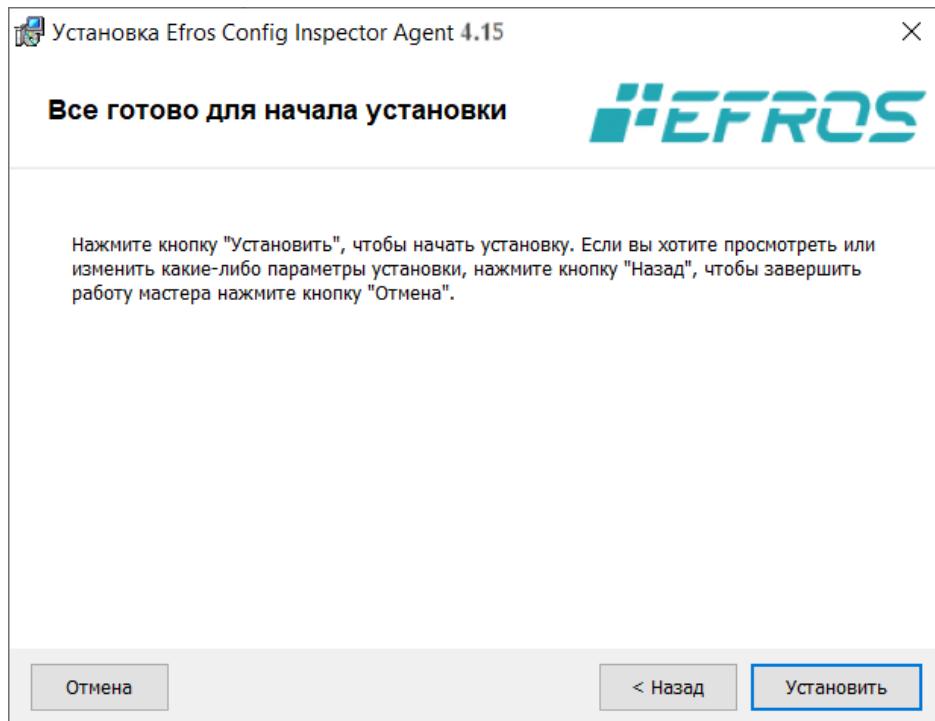


Рисунок 62 – Диалоговое окно готовности к установке

Ход установки windows-агента программного комплекса будет отображаться в окне мастера установки (рис. 63).

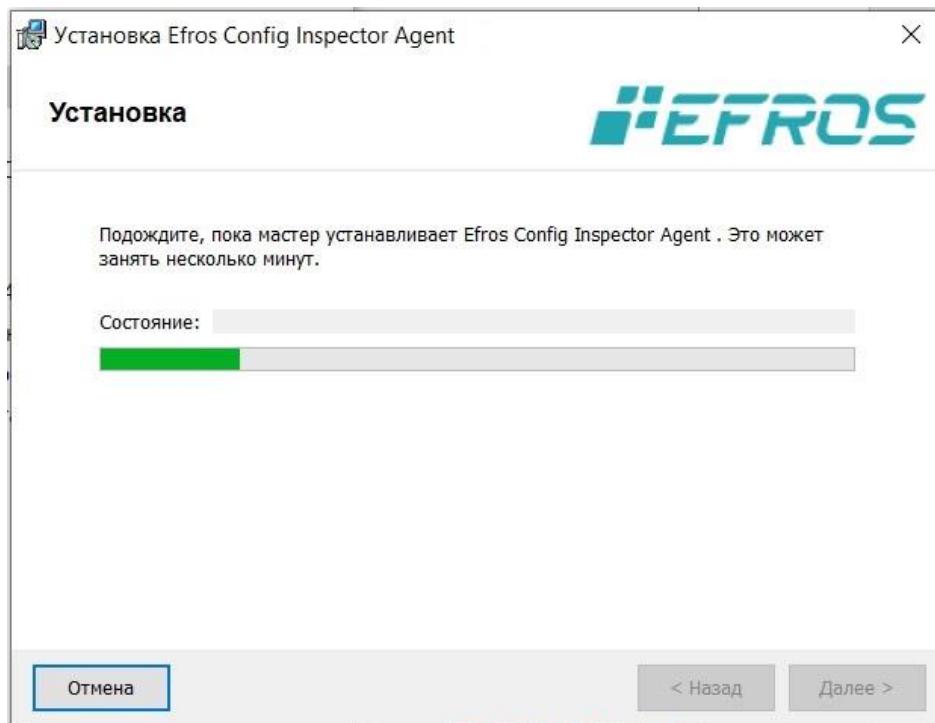


Рисунок 63 – Диалоговое окно процесса установки

После окончания установки windows-агента откроется диалоговое окно завершения работы мастера установки (рис. 64), в котором следует нажать кнопку «Готово».

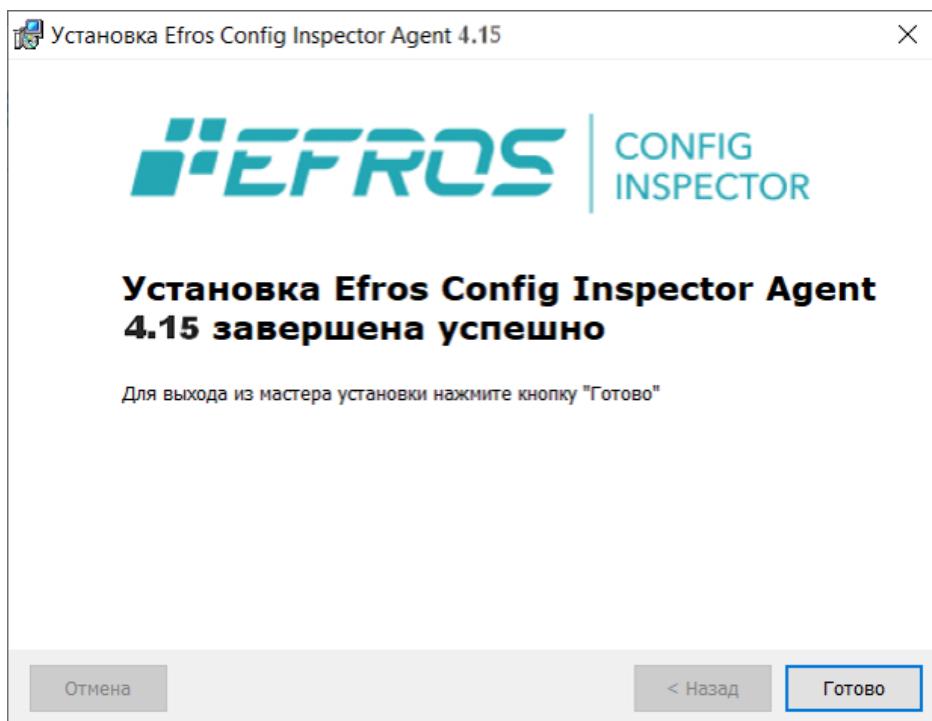


Рисунок 64 – Диалоговое окно завершения работы мастера установки

Windows-агент устанавливается на контролируемый рабочий сервер в качестве службы **EFROS CI Agent Service 4**, которая запускается в автоматическом режиме при загрузке ОС от имени системной учетной записи (Local System).

Настройка параметров службы Windows-агента выполняется в окне настройки параметров службы **EFROS CI Agent Service 4** (**C:\Program Files\EFROS Config Inspector 4\Agent\WASetup.exe**).

8.2 Настройка параметров службы windows-агента

Вызов окна настройки параметров службы EFROS CI Agent Service 4 осуществляется путем запуска файла **WASetup.exe** из директории **C:\Program Files\EFROS Config Inspector 4\Agent**.

После запуска появится окно с вкладкой «Службы» для настройки параметров службы «Efros Config Agent» (рис. 65). Состав и описание полей вкладки «Службы» приведены в таблице 16.

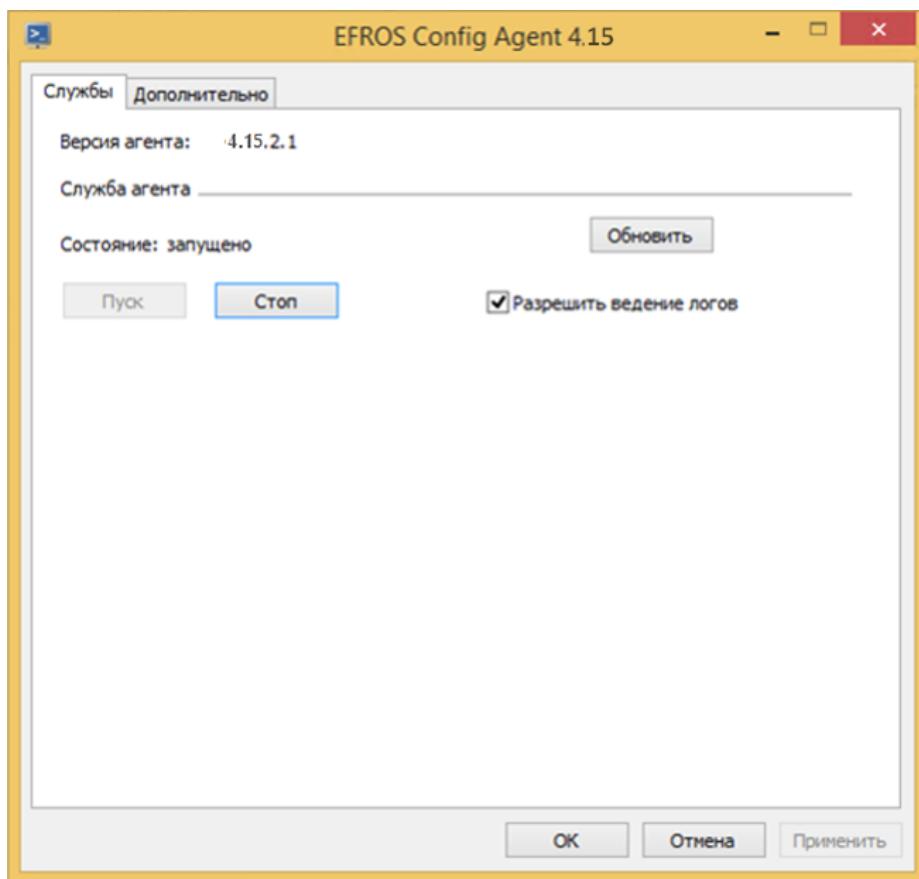


Рисунок 65 – Вкладка «Службы» окна настройки параметров службы EFROS CI Agent Service 4

Таблица 16 – Состав и описание полей вкладки «Службы» окна настройки параметров службы EFROS CI Agent Service 4

| Поле | Описание |
|--------------------------------|--|
| Поле «Версия агента» | Отображает последнюю версию установленного агента |
| Раздел «Служба агента» | |
| Поле «Состояние» | Отображает статус агента «запущено» или «остановлено» |
| Поле «Разрешить ведение логов» | Включает/отключает ведение логов программы настройки windows-агента WSetup |
| Кнопки управления | |
| Пуск | Запуск службы windows-агента |
| Стоп | Остановка службы windows-агента |
| Обновить | Для обновления статуса службы windows-агента |

При переходе на вкладку «Дополнительно» отображаются дополнительные настройки службы (рис. 66). Состав и описание полей вкладки «Дополнительно» приведены в таблице 17.

После завершения настройки службы windows-агента, необходимо нажать кнопку «Применить» и кнопку «OK» для закрытия окна. После этого, настроенные параметры будут приняты и вступят в силу при следующем запуске службы windows-агента. В случае, если агент запущен, будет предложен перезапуск.

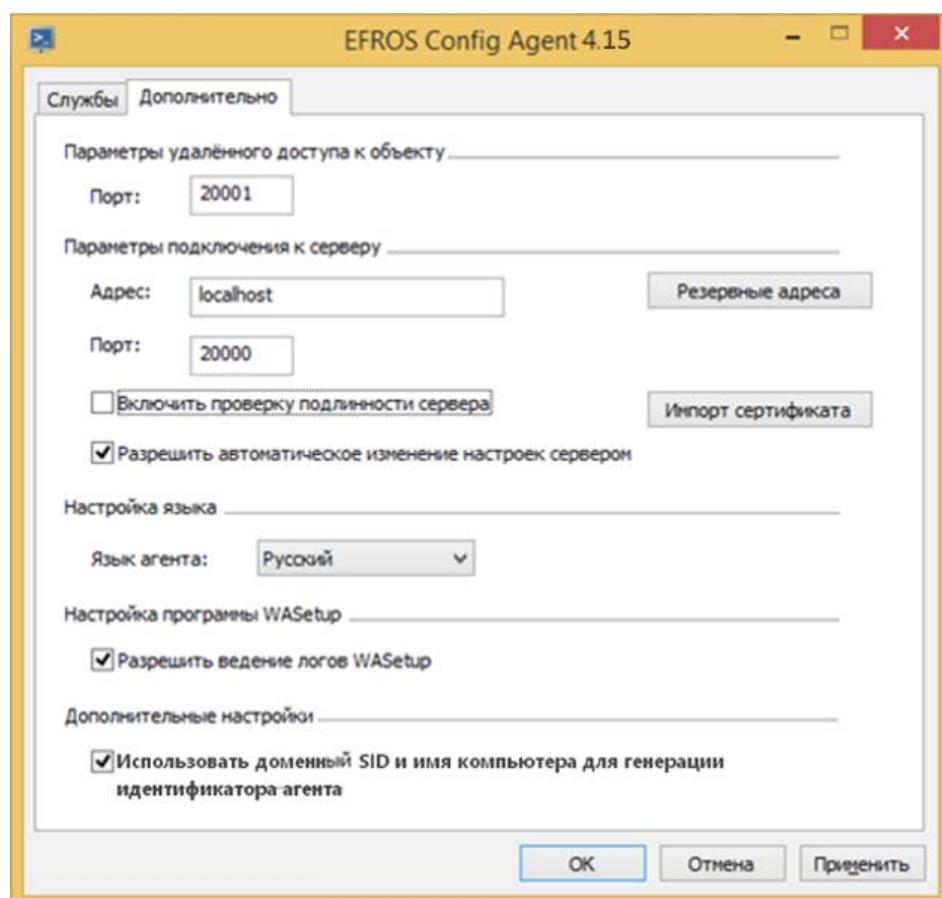


Рисунок 66 – Вкладка «Дополнительно» окна настройки параметров службы EFROS CI Agent Service 4

Таблица 17 – Состав и описание полей вкладки «Дополнительно» окна настройки параметров службы EFROS CI Agent Service 4

| Поле | Описание |
|--|---|
| Параметры удаленного доступа к объекту | |
| Поле «Порт» | Номер порта, используемого для установки связи между сервером ПК «Efros DO» и windows-агентом (для оповещения о включении windows-агента) |
| Параметры подключения к серверу | |
| Поле «Адрес» | IP-адрес сервера ПК «Efros DO» или его DNS-имя |
| Поле «Порт» | Номер порта, используемого для подключения сервера ПК к windows-агенту |
| Поле «Включить» | При включенном параметре (флаг в поле установлен) |

| Поле | Описание |
|---|--|
| проверку подлинности сервера» | происходит проверка сервера ПК «Efros DO» и windows-агента с помощью сертификата.
При первом подключении устройства с установленным windows-агентом проверка подлинности должна быть выключена как в окне настройки windows-агента, так и в настройках модуля «Windows» в веб-интерфейсе ПК «Efros DO» (см. документ «Руководство пользователя. Часть 1. Настройка и администрирование»).
После первого успешного подключения устройства для использования проверки подлинности сервера по сертификату необходимо включить проверку подлинности в окне настройки windows-агента и в веб-интерфейсе ПК «Efros DO», после чего windows-агент принимает сертификат сервера ПК «Efros DO». Во время взаимодействия сервера ПК «Efros DO» и windows-агента происходит проверка, основанная на принятом сертификате. Другие серверы ПК «Efros DO», не имеющие данного сертификата, не смогут установить соединение с windows-агентом |
| Кнопка «Импорт сертификата» | Позволяет устанавливать сертификат взаимодействия с серверной частью вручную |
| Поле «Разрешить автоматическое изменение настроек сервером» | При включенном параметре (флаг в поле установлен) настройки windows-агента (адрес сервера, проверка подлинности сертификатом) могут быть автоматически изменены сервером ПК «Efros DO» |
| Кнопка «Резервные адреса» | Позволяет задавать резервные адреса для установки связи с резервными серверами комплекса. В случае работы комплекса в режиме отказоустойчивости, windows-агент получает информацию о резервных серверах, с которыми он может работать в случае отказа основного сервера ПК «Efros DO» |
| Настройка языка | |
| Поле «Язык агента» | Позволяет выбрать язык windows-агента (русский, английский) |
| Настройка программы WASetup | |
| Поле «Разрешить ведение логов WASetup» | Включает/отключает ведение логов программы настройки windows-агента WASetup |
| Дополнительные параметры | |
| Поле «Использовать SID домена и имя компьютера для генерации идентификатора агента» | Позволяет автоматически генерировать uuid windows-агента на основе SID домена при подключении ОС в домен. Используется для обеспечения уникальности uuid windows-агента в случае клонирования виртуальных машин с предустановленным windows-агентом |

9 Агент ПК «Efros DO»

Агент ПК «Efros DO» (далее – агент) устанавливается на контролируемые устройства. Агент ПК «Efros DO» совместно с ПК «Efros DO» реализует проверку устройства на соответствие требованиям политик безопасности.

Инсталляционные пакеты агентов ПК «Efros DO» для различных ОС входят в комплект поставки. Также инсталляционный пакет можно скачать в веб-интерфейсе комплекса («Агенты» → «Установка и обновление» → «Инсталляционные пакеты»).

Инсталляционный пакет представляет собой архив формата .zip с набором файлов, необходимых для установки на устройство пользователя, и содержит:

- дистрибутив агента ПК «Efros DO»;
- дистрибутив модуля «Контроль целостности до загрузки ОС» – предназначен для проверки политики контроля целостности объектов до загрузки операционной системы;
- дополнительные файлы:
 - описание изменений версий агента ПК «Efros DO»;
 - описание отдельных компонентов и всего инсталляционного пакета;
 - модуль сбора информации об ОС для корректного обновления агента;
 - данные о версии пакета и операционной системе, для которой предназначен пакет;
 - описание компонентов в архиве.

При установке агента необходимо убедиться, что версия ОС устройства совпадает с версией, указанной в инсталляционном пакете.

 В процессе установки/удаления агента команды необходимо вводить от имени суперпользователя *root* либо, используя команду *sudo*.

9.1 Установка и удаление агента ПК «Efros DO» (ОС MS Windows)

9.1.1 Установка агента (MS Windows)

 Предварительно необходимо проверить наличие на устройстве обязательных библиотек для работы с сетевыми интерфейсами. Если обязательных библиотек нет, то в ходе установки агента следует выбрать установку программы «WinPcap» для управления сетью при работе со встроенным модулем «Суппликант» (см. рис. 70). Требования к агенту приведены в пункте 1.2.6.

Для установки агента ПК «Efros DO» необходимо скопировать на устройство с ОС MS Windows файл *edo-agent-<версия агента>.msi* и запустить его на исполнение.

Откроется окно мастера установки «EDO Agent» (рис. 67).

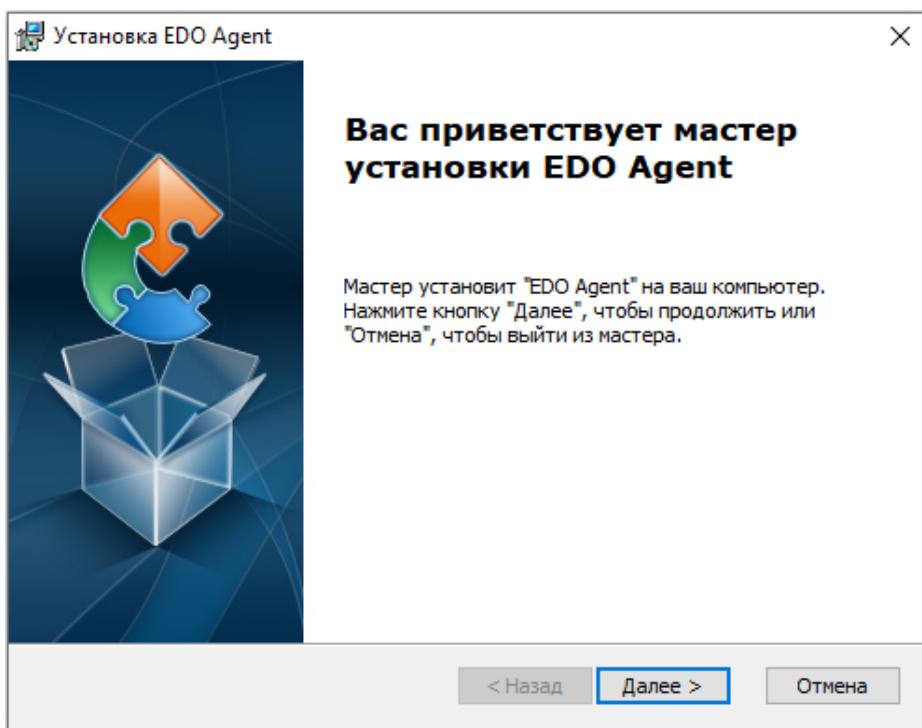


Рисунок 67 – Диалоговое окно мастера установки «EDO Agent»

В диалоговом окне мастера установки нажать кнопку «Далее».

Откроется диалоговое окно выбора папки установки, в котором следует выбрать папку для установки агента или оставить заданную по умолчанию (**C:\Program Files\EDO\Agent**) и нажать кнопку «Далее» (рис. 68).

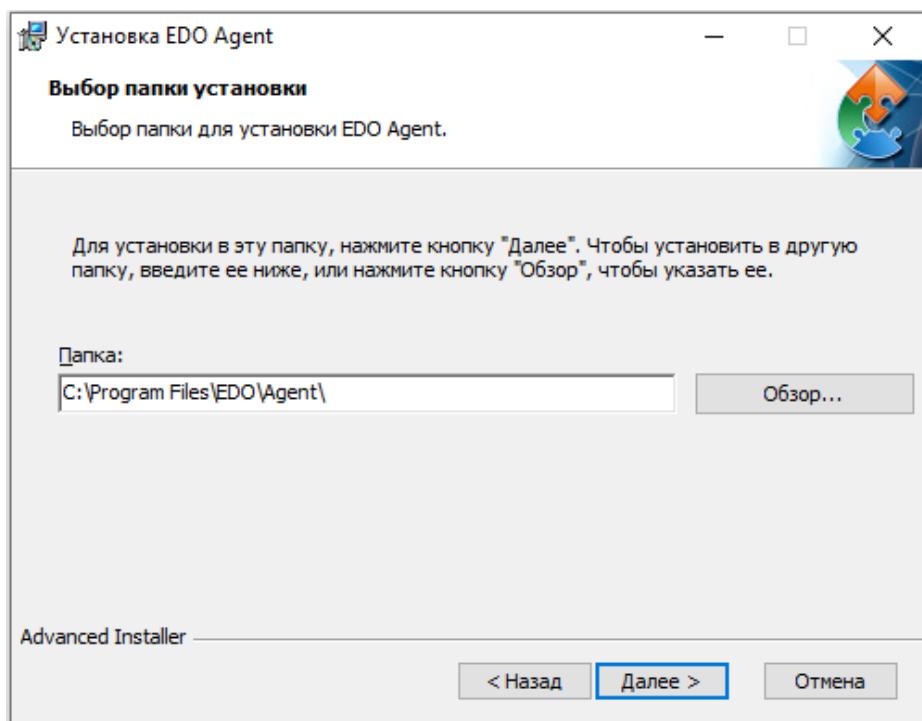


Рисунок 68 – Диалоговое окно выбора папки установки

В диалоговом окне настройки агента (рис. 69) есть возможность применить следующие параметры:

- применить для агента удаленное управление сервером ПК «Efros DO». Для этого необходимо установить флаг в поле «Под управлением Efros Defence Operations сервера» и ввести адрес сервера и порт в поле «Адрес сервера и порт», значение по умолчанию: <https://edo-gateway-service:8443>. Если флаг в поле «Под управлением Efros Defence Operations сервера» убран, то будет применено локальное управление агентом;
- включить модуль суппликанта агента, установив флаг в поле «Включить модуль Суппликант»;
- включить модуль взаимодействия с VPN клиентами, выбрав из раскрывающегося списка значение «NGate» или «S-Terra».

Изменить параметры агента можно будет в графическом интерфейсе агента (см. документ «Руководство пользователя. Часть 4. Контроль доступа и агенты. Приложение И. Работа с агентами ПК «Efros DO»).

Для продолжения установки нажать кнопку «Далее».

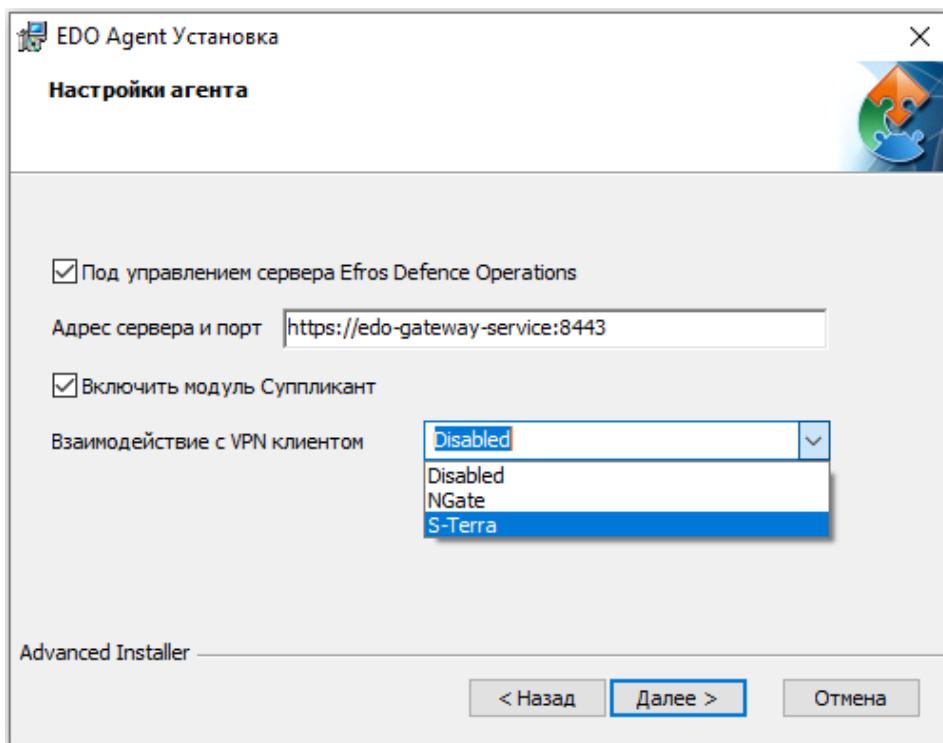


Рисунок 69 – Диалоговое окно настройки агента

В диалоговом окне выбора дополнительных компонентов для установки (рис. 70) есть возможность добавить установку программы «WinPcap» для управления сетью при работе с суппликантом. При нажатии на раскрывающийся список выбора установки «WinPcap» доступны следующие значения:

- «Будет установлен на локальный жесткий диск»;

- «Этот компонент будет полностью установлен на локальный жесткий диск»;
- «Компонент будет полностью недоступен» – значение по умолчанию.

Для установки программы «WinPcap» необходимо выбрать первое или второе значение – установка будет производиться одинаково.

Для продолжения нажать кнопку «Далее».

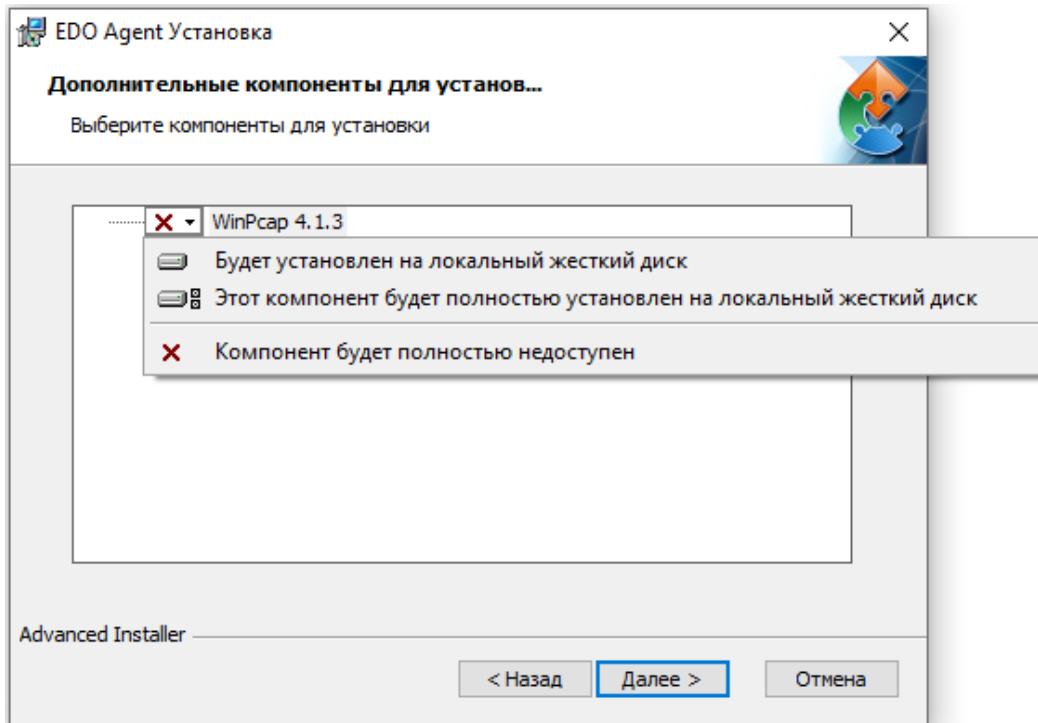


Рисунок 70 – Диалоговое окно выбора дополнительных компонентов для установки

В диалоговом окне готовности мастера к установке (рис. 71) для запуска процесса инсталляции с заданными ранее параметрами следует нажать кнопку «Установить».

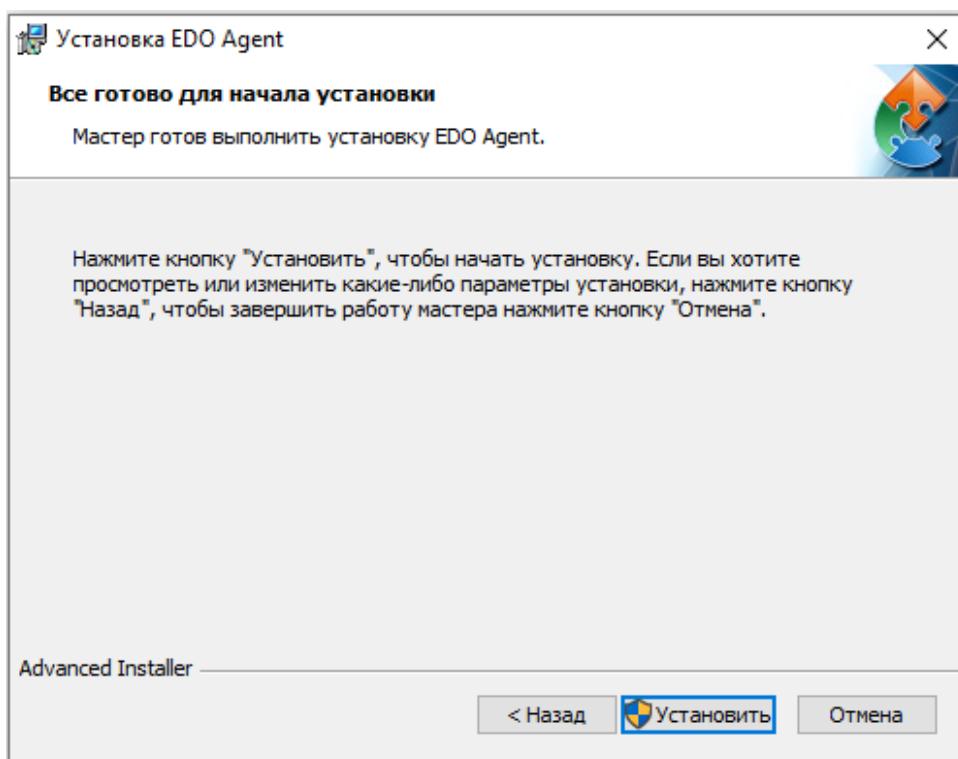


Рисунок 71 – Диалоговое окно готовности к установке

Ход установки «EDO Agent» программного комплекса будет отображаться в окне мастера установки (рис. 72).

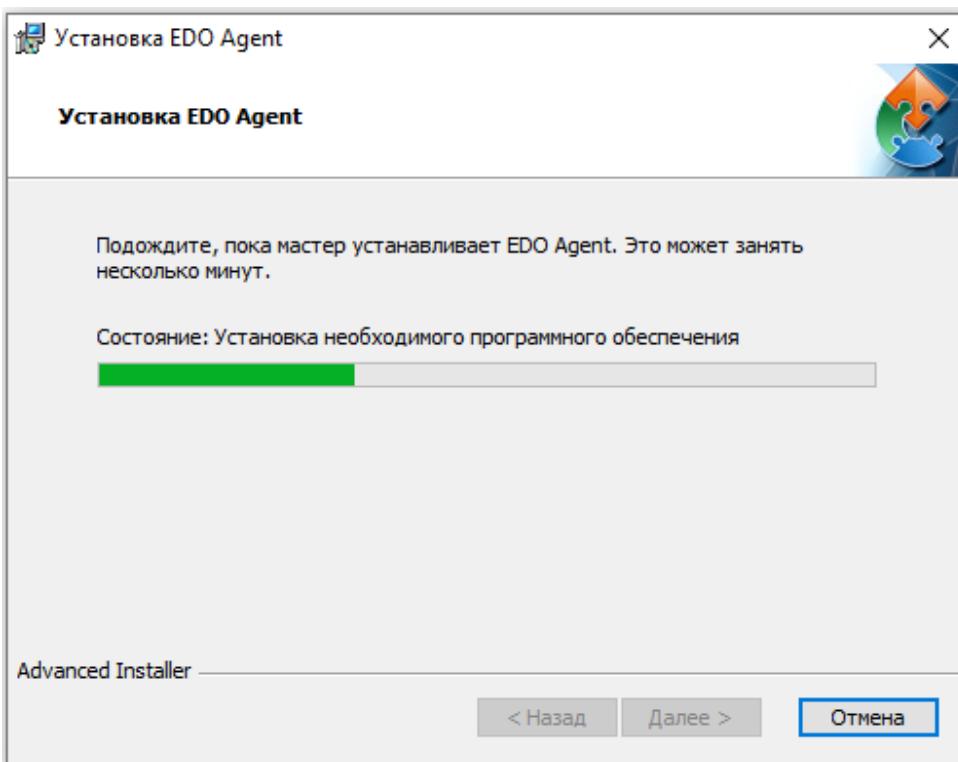


Рисунок 72 – Диалоговое окно процесса установки

- ⓘ При появлении диалогового окна операционной системы «Разрешить этому приложению вносить изменения на вашем устройстве?» следует нажать кнопку «Да».

После окончания установки «EDO Agent» откроется диалоговое окно завершения работы мастера установки (рис. 73), в котором следует нажать кнопку «Готово».

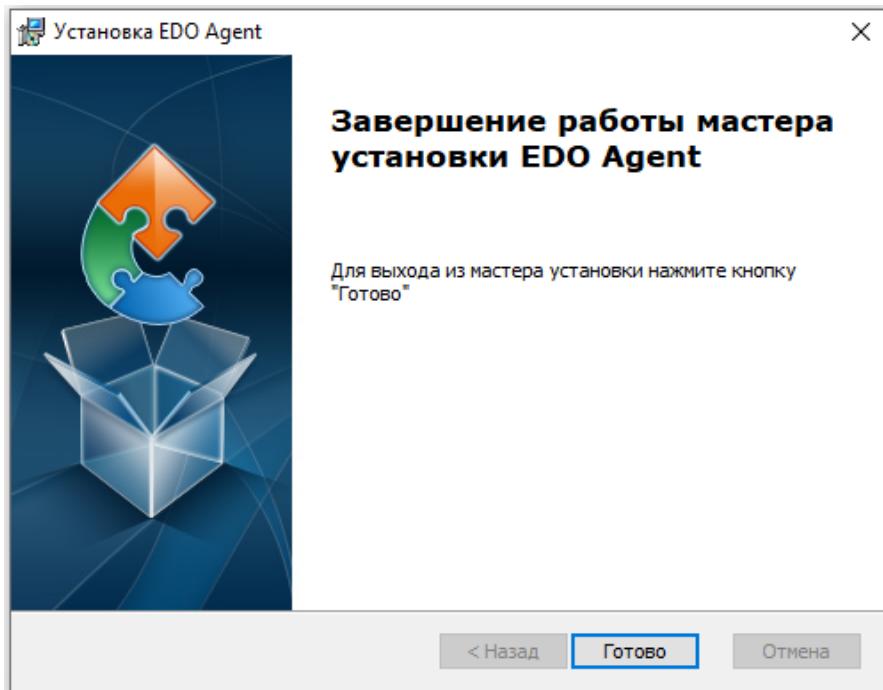


Рисунок 73 – Диалоговое окно завершения работы мастера установки

Установка агента с помощью MSIEXEC

Для установки агента с использованием средства установщика MS Windows **MSIEXEC** необходимо выполнить следующую команду:

```
msiexec /i "<путь к инсталлятору msi>\edo-agent-<версия агента>.msi"
```

Для установки агента с параметрами необходимо воспользоваться следующей командой:

```
msiexec /i "<путь к инсталлятору msi>\edo-agent-<версия агента>.msi" IS_EDO_INSTALLATION=TRUE  
EDO_SERVER_ADDRESS="https://<ip-адрес>:<номер порта>"  
IS_SUPPLICANT=TRUE
```

где:

IS_EDO_INSTALLATION – настройка управления агентом. При значении «true» для

агента будет применено удаленное управление сервером ПК «Efros DO»; «false» – для агента будет применено локальное управление;

IS_SUPPLICANT – включение модуля «Суппликант». При значении «true» модуль «Суппликант» будет включен; «false» – выключен;

EDO_SERVER_ADDRESS – адрес сервера ПК «Efros DO».

Завершение установки агента

После завершения установки агента в окне программы «Службы» появятся и автоматически запустятся службы «EDO Agent Service» и «EDO Supplicant Service» (рис. 74).

Описание работы со службами агента приведено в подразделе 9.6.

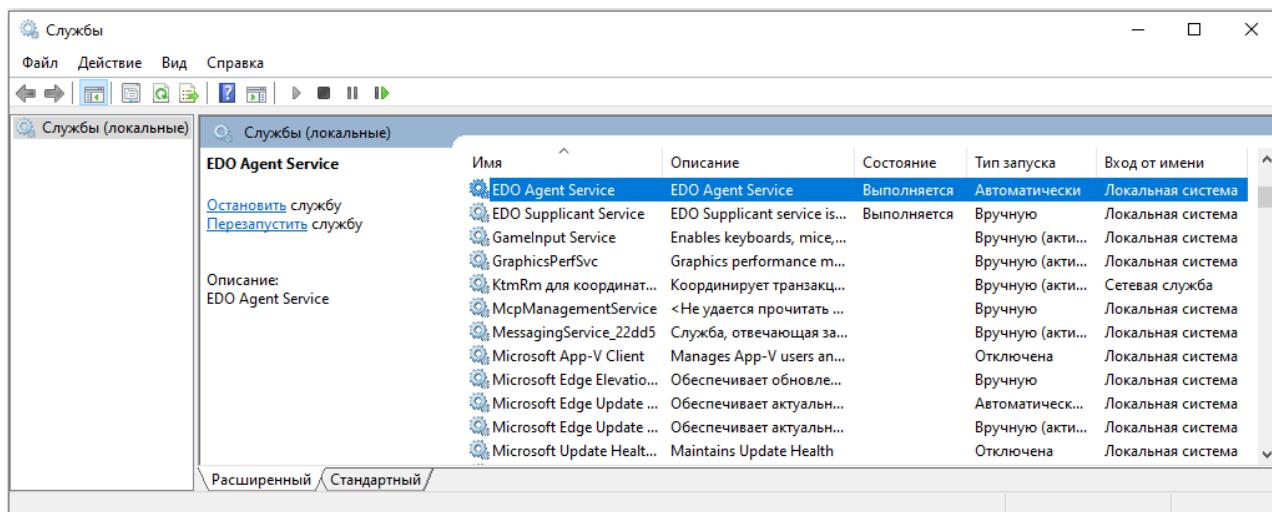


Рисунок 74 – Запущенные службы агента и суппликанта

В веб-интерфейсе ПК «Efros DO» в разделе «Агенты» появится соответствующий агент, для которого будут применены проверки текущей политики безопасности.

9.1.2 Удаление агента (MS Windows)

Для удаления агента ПК «Efros DO» с ОС MS Windows необходимо выполнить переход «Панель управления» → «Программы» → «Программы и компоненты» («Удаление программы»). В списке программ найти «EDO Agent», выбрать его и нажать кнопку «Удалить».

Удаление агента с помощью MSIEXEC

Для удаления с использованием средства MS Windows **MSIEXEC** необходимо найти GUID агента и выполнить следующую команду:

```
wmic product get name, identifyingnumber  
msiexec /x {<GUID = identifyingnumber>} /quiet
```

Удаление агента с помощью командной строки

Для удаления агента с помощью командной строки необходимо выполнить:

```
wmic product where "name='EDO Agent'" call uninstall
```

9.2 Установка и удаление агента ПК «Efros DO» (ОС Linux)

9.2.1 Установка агента (Linux)

При установке агента ПК «Efros DO» на устройство с ОС Astra Linux SE или ОС Ubuntu необходимо использовать установочный файл **edo-agent-<версия>.deb**.

При установке агента ПК «Efros DO» на устройство с РЕД ОС необходимо использовать установочный файл **edo-agent-<версия>.rpm**.

Для установки агента необходимо выполнить следующие действия:

- 1) Скопировать на контролируемую конечную точку необходимый файл.
- 2) В интерфейсе командной строки поочередно ввести команды, указанные ниже.

Установка агента на ОС Astra Linux SE или ОС Ubuntu осуществляется с помощью команды:

```
sudo dpkg -i edo-agent-<версия агента>.deb
```

Установка агента на РЕД ОС осуществляется с помощью команды:

```
sudo rpm -Uv edo-agent-<версия агента>.rpm
```

Для установки агента с параметрами необходимо воспользоваться следующими командами, в соответствии с целевой ОС:

— для ОС Astra Linux SE или ОС Ubuntu:

```
sudo IS_EDO_INSTALLATION=TRUE IS_SUPPLICANT=TRUE  
EDO_SERVER_ADDRESS="https://<ip-адрес>:<номер порта>" dpkg -i edo-  
agent-<версия агента>.deb
```

— для РЕД ОС:

```
sudo env IS_EDO_INSTALLATION=TRUE EDO_SERVER_ADDRESS="https://<ip-адрес>:<номер порта>" IS_SUPPLICANT=TRUE rpm -Uv edo-agent-<версия агента>.rpm
```

где:

IS_EDO_INSTALLATION – настройка управления агентом. При значении «true» для агента будет применено удаленное управление сервером ПК «Efros DO»; «false» – для агента будет применено локальное управление;

IS_SUPPLICANT – включение модуля «Суппликант». При значении «true» модуль «Суппликант» будет включен; «false» – выключен;

EDO_SERVER_ADDRESS – адрес сервера ПК «Efros DO».

После завершения установки агента автоматически запустится служба «EDO Agent Service». Описание работы со службами агента приведено в подразделе 9.6.

Изменение настроек будет доступно в графическом интерфейсе агента ПК «Efros DO».

После завершения установки в веб-интерфейсе ПК «Efros DO» в разделе «Агенты» появится соответствующий агент, для которого будут применены проверки текущей политики безопасности.

9.2.2 Удаление агента (Linux)

Для удаления агента ПК «Efros DO» с ОС Astra Linux SE или ОС Ubuntu необходимо выполнить следующие действия:

- 1) В интерфейсе командной строки ввести следующую команду:

```
sudo dpkg -r edo-agent
```

- 2) Ввести пароль пользователя ОС.

- 3) Согласиться с выполнением операции.

Удаление агента ПК «Efros DO» завершено.

Для удаления агента ПК «Efros DO» с РЕД ОС необходимо выполнить следующие действия:

- 1) В интерфейсе командной строки ввести следующую команду:

```
sudo rpm -e edo-agent-<версия агента>
```

- 2) Ввести пароль пользователя ОС.

- 3) Согласиться с выполнением операции.

Удаление агента ПК «Efros DO» завершено.

9.3 Установка и удаление агента ПК «Efros DO» (ОС macOS)

9.3.1 Установка агента (macOS)

При установке агента ПК «Efros DO» на устройство с macOS необходимо использовать установочный файл ***edo-agent-<версия агента>.pkg***.

Для установки агента необходимо выполнить следующие действия:

- 1) Скопировать на контролируемую конечную точку необходимый установочный файл и скрипт установки *install_edo_agent.sh*.

(i) Установочный файл и скрипт установки должны располагаться в одной директории.

- 2) В интерфейсе командной строки ввести следующую команду:

```
sudo installer -pkg 'edo-agent-<версия агента>.pkg' -target
```

Для установки агента с параметрами необходимо воспользоваться следующей командой:

```
sudo ./install_edo_agent.sh IS_EDO_INSTALLATION=TRUE  
EDO_SERVER_ADDRESS="https://<ip-адрес>:<номер порта>"
```

где:

IS_EDO_INSTALLATION – настройка управления агентом. При значении «true» для агента будет применено удаленное управление сервером ПК «Efros DO», «false» – для агента будет применено локальное управление;

EDO_SERVER_ADDRESS – адрес сервера ПК «Efros DO».

После завершения установки агента автоматически запустится служба «EDO Agent Service». Описание работы со службами агента приведено в подразделе 9.6.

Изменение настроек будет доступно в графическом интерфейсе агента ПК «Efros DO».

После завершения установки в веб-интерфейсе ПК «Efros DO» в разделе «Агенты» появится соответствующий агент, для которого будут применены проверки текущей политики безопасности.

9.3.2 Удаление агента (macOS)

Для удаления агента ПК «Efros DO» с macOS необходимо выполнить следующие действия:

- 1) Скопировать на контролируемую конечную точку файл *uninstall_edo_agent.sh*.
- 2) Выполнить следующие команды:

```
sudo launchctl stop edo.agent
sudo launchctl unload /Library/LaunchDaemons/edo.agent.plist
sudo rm /Library/LaunchDaemons/edo.agent.plist
sudo rm -rf /Applications/EDO/EDO Agent.app
sudo pkgutil --forget gis.edo.agent
```

- 3) В интерфейсе командной строки ввести следующую команду:

```
sudo ./uninstall_edo_agent.sh
```

Удаление агента ПК «Efros DO» завершено.

9.4 Модуль «Контроль целостности до загрузки ОС» (ICM)

Модуль агента «Контроль целостности до загрузки ОС» предназначен для проверки политики контроля целостности объектов до загрузки ОС.

Модуль «Контроль целостности до загрузки ОС» имеет альтернативное название: «Integrity Control Module» (далее – модуль «ICM» или «Контроль целостности до загрузки ОС»).

Пример настройки агента приведен в документе «Руководство пользователя. Часть 4. Контроль доступа и агенты. Приложение И. Работа с агентами ПК «Efros DO».

9.4.1 Предварительные настройки перед установкой модуля

Перед установкой модуля «Контроль целостности до загрузки ОС» (ICM) необходимо произвести следующие настройки:

- 1) Установить на устройстве актуальную версию агента ПК «Efros DO».
- 2) Проверить, что для устройства отключен параметр «Secure Boot» в настройках EFI/UEFI BIOS. Это необходимо для корректной работы модуля «Контроль целостности до загрузки ОС» и компьютера.
- 3) Создать требования политики контроля целостности до загрузки ОС в разделе «Агенты». Описание раздела «Агенты» веб-интерфейса ПК «Efros DO» приведено в документе «Руководство пользователя. Часть 4. Контроль доступа и агенты».

9.4.2 Установка и включение модуля «Контроль целостности до загрузки ОС»

- !** Параметр «Secure Boot» должен быть отключен в настройках EFI/UEFI BIOS целевого устройства для корректной работы модуля «Контроль целостности до загрузки ОС» и компьютера.

Установка модуля «Контроль целостности до загрузки ОС» должна осуществляться на физическую ЭВМ.

Поддерживаемые операционные системы для установки модуля «Контроль целостности до загрузки ОС» приведены в пункте 1.2.6.

Дополнительно после установки необходимо включить модуль через веб-интерфейс комплекса и перезагрузить устройство с модулем. Подробнее описано ниже.

Установка модуля

Установка модуля «Контроль целостности до загрузки ОС» производится при запуске расписания обновления агента в разделе «Агенты» в веб-интерфейсе ПК «Efros DO».

Описание раздела «Агенты» приведено в документе «Руководство пользователя. Часть 4. Контроль доступа и агенты».

Включение модуля

Включение модуля «Контроль целостности до загрузки ОС» производится в настройках агента в веб-интерфейсе ПК «Efros DO». Также нужно применить необходимую политику контроля целостности.

Перезагрузка устройства с модулем

Для применения новых параметров агента и модуля «ICM» необходимо перезагрузить устройство.

В процессе первой перезагрузки устройства произведется первый запуск модуля. При первой загрузке модуля могут появиться дополнительные окна с выбором действий. Изменять значения при этом не нужно. Загрузка модуля будет произведена автоматически.

9.4.3 Работа с модулем «Контроль целостности до загрузки ОС»

На устройстве с включенным модулем «ICM» перед загрузкой ОС будет выводиться сообщение «Press F5 To Load ICM Console...» для возможности вызова аварийной консоли.

При штатной работе модуля «ICM» нет необходимости в использовании аварийной консоли.

Аварийную консоль необходимо использовать при возникновении ошибок, связанных с работой модуля и/или загрузкой ОС.

Описание работы с аварийной консолью приведено в документе «Инструкция по работе с аварийной консолью модуля агента «Контроль целостности до загрузки ОС» (ICM)». При необходимости инструкцию можно запросить через службу технической поддержки производителя.

9.4.4 Удаление модуля «Контроль целостности до загрузки ОС» (MS Windows)

Для удаления модуля «ICM» с ОС MS Windows необходимо выполнить следующие действия:

- 1) Запустить файл инсталлятора SafeNodeSL.exe. По умолчанию файл располагается в папке **C:\ProgramData\EDO\Agent\edo_agent_updater**.
- 2) Ввести пароль – идентификатор агента без дефисов «-».
- 3) Выбрать пункт «Удалить».
- 4) После завершения удаления следует перезагрузить устройство для применения изменений. Соответствующее уведомление появится в отдельном окне.

Удаление модуля «ICM» завершено.

9.4.5 Удаление модуля «Контроль целостности до загрузки ОС» (Linux)

Для удаления модуля «ICM» с ОС Astra Linux SE или РЕД ОС необходимо выполнить следующие действия:

- 1) В интерфейсе командной строки ввести следующую команду:

```
sudo /usr/share/sdz/bin/SafeNodeSystemLoader
```

- 2) Ввести логин «admin» и пароль. Паролем модуля является идентификатор агента без дефисов «-».
- 3) В нижней части консоли нажать на кнопку «Расширенный режим».
- 4) В разделе «Общие параметры» выбрать подраздел «Информация о продукте».
- 5) В верхней части формы раздела нажать кнопку «Удаление ПО» и подтвердить запрос на удаление в открывшемся окне.

Удаление модуля «ICM» завершено.

9.5 Изменение адреса сервера ПК «Efros DO»

Изменить адрес сервера ПК «Efros DO» можно следующими способами:

- 1) С помощью графического интерфейса агента в разделе «Настройки» → «Подключение» (подробнее см. в документе «Руководство пользователя. Часть 4. Контроль доступа и агенты. Приложение И. Работа с агентами ПК «Efros DO»).
- 2) С помощью командной строки.

9.5.1 Изменение адреса сервера с помощью командной строки (MS Windows)

Для изменения адреса сервера ПК «Efros DO» с помощью командной строки ОС MS Windows необходимо использовать следующую команду:

```
edo_agent_service.exe --EDO_URL="https://<ip-адрес>:<номер порта>"
```

Чтобы изменения вступили в силу, потребуется перезапуск службы агента. Описание работы со службами агента приведено в подразделе 9.6.

После завершения перезапуска служб изменение адреса сервера ПК «Efros DO» будет завершено.

9.5.2 Изменение адреса сервера с помощью командной строки (Linux и macOS)

Для изменения адреса сервера ПК «Efros DO» с помощью командной строки ОС Astra Linux SE, ОС Ubuntu, РЕД ОС или macOS необходимо использовать следующую команду:

```
edo_agent_service --EDO_URL="https://<ip-адрес>:<номер порта>"
```

Чтобы изменения вступили в силу, потребуется перезапуск службы агента. Описание работы со службами агента приведено в подразделе 9.6.

После завершения перезапуска служб изменение адреса сервера ПК «Efros DO» будет завершено.

9.6 Службы и процессы модулей агента

При установке агента ПК «Efros DO» на ОС MS Windows, Linux или macOS автоматически запускается служба «Edo Agent Service».

Описание работы службы модуля «Суппликант»:

- при остановке службы агента «EDO Agent Service» – служба модуля «Суппликант» будет автоматически остановлен (при наличии запущенной службы модуля);
- при запуске службы агента «EDO Agent Service» – служба модуля «Суппликант» будет автоматически запущена (при наличии включенного модуля на агенте);
- в момент включения модуля «Суппликант» на агенте – автоматически запускается служба данного модуля;
- в момент выключения модуля «Суппликант» на агенте – автоматически останавливается служба данного модуля.

Описание работы процессов модуля «Контроль целостности до загрузки ОС»:

- при остановке службы агента «EDO Agent Service» – процесс модуля «Контроль целостности до загрузки ОС» будут автоматически остановлен (при наличии запущенного процесса модуля);
- процесс модуля «Контроль целостности до загрузки ОС» будет автоматически запущен при применении политики контроля целостности до загрузки ОС;
- процесс модуля «Контроль целостности до загрузки ОС» будет автоматически остановлен после завершения применения политики контроля целостности до загрузки ОС.

9.6.1 Работа со службами агента на MS Windows

 Командную строку или «Windows PowerShell» необходимо запускать с правами администратора.

Запуск службы

Запустить службу агента можно следующей командой:

```
net start "EDO Agent Service"
```

Также доступен отдельный запуск службы суппликанта, выполнением команды:

```
net start "EDO Supplicant Service"
```

Остановка службы выполняется аналогичными командами, но вместо **start** используется **stop**.

Перезапуск службы

Перезапустить службу агента или суппликанта можно следующими командами:

```
net stop "EDO Agent Service" && net start "EDO Agent Service"  
net stop "EDO Supplicant Service" && net start "EDO Supplicant Service"
```

Работа со службами агента с помощью Windows PowerShell

Альтернативный вариант работы со службами агента является использование приложения «Windows PowerShell».

Запустить службу агента или суппликанта можно следующими командами:

```
Start-Service -Name "EDO Agent Service"  
Start-Service -Name "EDO Supplicant Service"
```

Остановка службы выполняется аналогичными командами, но вместо **Start** используется **Stop**.

Перезапуск службы выполняется аналогичными командами, но вместо **Start** используется **Restart**.

9.6.2 Работа со службами агента на Linux

Команда запуска службы агента для ОС Astra Linux SE, ОС Ubuntu и РЕД ОС:

```
sudo systemctl start edo-agent
```

Остановка службы выполняется аналогичными командами, но вместо **start** используется **stop**.

Перезапуск службы выполняется аналогичными командами, но вместо **start** используется **restart**.

9.6.3 Работа со службами агента на macOS

Команда запуска службы агента для macOS:

```
sudo launchctl start edo.agent
```

Остановка службы выполняется аналогичными командами, но вместо **start** используется **stop**.

Перезапуск службы выполняется аналогичными командами, но вместо **start** используется **restart**.

9.7 Обновление агента ПК «Efros DO»

Обновление агента ПК «Efros DO» можно произвести следующими способами:

- 1) Переустановить агент ПК «Efros DO» на устройстве, согласно описанию в подразделах 9.1 – 9.3.
- 2) Настроить обновление в веб-интерфейсе комплекса («Агенты» → «Установка и обновление» → «Обновление»).

Поддерживаемые версии агентов ПК «Efros DO» в комплексе версии 2.13:

- агент ПК «Efros DO» версии 1.5;
- агент ПК «Efros DO» версии 1.4;
- агент ПК «Efros DO» версии 1.3.

Для эксплуатации и эффективного применения агента ПК «Efros DO» рекомендуется использование последней версии.



Особенности установки или обновления агента ПК «Efros DO» при наличии на устройстве установленного суппликанта ПК «Efros DO» (отдельный суппликант из состава комплекса версии 2.8, 2.9 или 2.10):

- перед установкой агента версии 1.3 и выше рекомендуется удалить отдельный суппликант ПК «Efros DO»;
- профили подключения, которые были настроены на отдельном суппликанте, установленном на ОС семейства MS Windows, автоматически импортируются из реестра MS Windows на новый агент (импортируются только профили подключения с аутентификацией «IEEE 802.1X»);
- профили подключения, которые были настроены на отдельном суппликанте, установленном на ОС семейства Linux, не экспортируются. Их необходимо добавить вручную на новом агенте.

9.8 Графический интерфейс агента

Графический интерфейс агента ПК «Efros DO» представляет собой набор веб-страниц и предназначен для управления параметрами суппликанта агента и настройки параметров самого агента.

Для настройки агента в графическом интерфейсе необходимо на устройстве с установленным агентом открыть браузер и ввести адрес: <http://localhost:9123/>.

Подробное описание работы с графическим интерфейсом агента приведено в документе «Руководство пользователя. Часть 4. Контроль доступа и агенты. Приложение И. Работа с агентами ПК «Efros DO».

10 Сообщения администратору

ПК «Efros DO» не предусматривает каких-либо диагностических сообщений. Сообщения об ошибках в настройке ПК «Efros DO» либо об ошибках комплекса выводятся в виде стандартных диалоговых окон с соответствующими пояснениями.

Перечень сокращений

| | |
|---------|---|
| BIOS | – Basic Input Output System |
| CM | – Change Manager |
| DNS | – Domain Name System |
| FA | – Firewall Assurance |
| FAT32 | – File Allocation Table |
| HTTP | – HyperText Transfer Protocol |
| HTTPs | – HyperText Transfer Protocol Secure |
| GPT | – Globally Unique Identifier Partition Table |
| GSLB | – Global Server Load Balancing |
| ICC | – Integrity Check Compliance |
| ICM | – Integrity Control Module |
| IP | – Internet Protocol |
| IPFIX | – Internet Protocol Flow Information Export |
| MBR | – Master Boot Record |
| NA | – Network Assurance |
| NAC | – Network Access Control |
| NFA | – Network Flow Analysis |
| NTP | – Network Time Protocol |
| RADIUS | – Remote Authentication in Dial-In User Service |
| SE | – Special Edition |
| SID | – Security Identifier |
| SNMP | – Simple Network Management Protocol |
| SP | – Service Pack |
| TACACS+ | – Terminal Access Controller Access Control System plus |
| UEFI | – Unified Extensible Firmware Interface |
| VC | – Vulnerability Control |
| БД | – База данных |
| ДМЗ | – Демилитаризованная зона |
| ИБ | – Информационная безопасность |

| | |
|-----------------|---|
| ОЗ | – Объект защиты |
| ООО | – Общество с ограниченной ответственностью |
| ОС | – Операционная система |
| ПК | – Программный комплекс |
| СУБД | – Система управления базами данных |
| ФСТЭК
России | – Федеральная служба по техническому и экспортному контролю
России |
| ЦОД | – Центр обработки данных |
| ЭВМ | – Электронно-вычислительная машина |