Высокодоступный домен Astra Linux Directory

Архитектура и описание

2017

Высокодоступный домен Astra Linux Directory: Архитектура и описание

Настоящий документ содержит краткое описание и архитектуру Высокодоступного домена ALD. Высокодоступный домен Astra Linux Directory разработанный «Лабораторией 50» — решение для создания домена Astra Linux Directory операционной системы Astra Linux Special Edition в конфигурации высокой готовности.

Дата публикации: 16 июня 2017 г.

ООО «Лаборатория 50»
198216, Санкт-Петербург, Ленинский проспект, дом 140 литер И, офис 422В

Содержание

1 Введение

Служба Astra Linux Directory операционной системы специального назначения Astra Linux Special Edition — это система управления единым пространством пользователей. Единое пространство пользователей представляет собой средства организации работы пользователя в сети компьютеров, работающих под управлением ОС. В основу положен доменный принцип построения сети, подразумевающий объединение в одну сеть логически связанных компьютеров, например принадлежащих одной организации. При этом пользователь получает возможность работы с сетевыми ресурсами сети и взаимодействия с другими пользователями.

Организация ЕПП обеспечивает:

— сквозную аутентификацию в сети;
— централизацию хранения информации об окружении пользователей;
— централизацию хранения настроек системы защиты информации на сервере.

Высокодоступный домен Astra Linux Directory — это надстройка над штатной службой Astra Linux Directory, обеспечивающая высокую доступность службы домена при сбоях программного или аппаратного обеспечения.

Высокодоступный домен ALD предназначен для работы в рамках программно-аппаратного комплекса, обладающего повышенной готовностью за счёт дублирования аппаратного обеспечения.

Разработанный Лабораторией 50 высокодоступный домен это:

— горячий резерв штатного Astra Linux Directory;
— минимальное время простоя и время переключения;
— сохранение всех штатных функций оригинального ПО.

2 Назначение

2.1 Astra Linux Directory

Служба Astra Linux Directory (ALD) операционной системы специального назначения Astra Linux Special Edition представляет собой систему управления единым пользовательским пространством. В терминах привычных пользователям Windows, Astra Linux Directory — это *домен*.

ALD выполняет следующие основные функции:

— хранение базы данных учётных записей пользователей;

— обеспечение единой аутентификации и авторизации пользователей;

— предоставление сетевых домашних каталогов пользователей;

— управление пользователями, службами, мандатными атрибутами и пр.

ALD является надстройкой над технологиями LDAP, Kerberos 5, CIFS и обеспечивает автоматическую настройку всех необходимых файлов конфигурации служб, реализующих перечисленные технологии, а так же предоставляет интерфейс управления и администрирования. Настройка окружения пользователя при входе в систему обеспечивается PAM-модулем ALD, который выполняет следующие функции:

— получение параметров окружения пользователя с сервера домена;

— проверка возможности входа пользователя на данный компьютер по списку разрешённых пользователю компьютеров;

— проверка возможности использования пользователем типа ФС его домашнего каталога;

— настройка параметров окружения пользователя;

— монтирование домашнего каталога пользователя;

— включение доменного пользователя в заданные локальные группы.

2.2 Высокодоступный домен ALD

Служба Astra Linux Directory содержит базовые средства организации резервного сервера. Однако, встроенные средства обладают следующими недостатками:

— не обеспечивают работу с домашними каталогами пользователей;

— резервный сервер ALD не является горячим резервом и требует вмешательства администратора для переключения;

— переключение не является невидимым для пользователей домена.

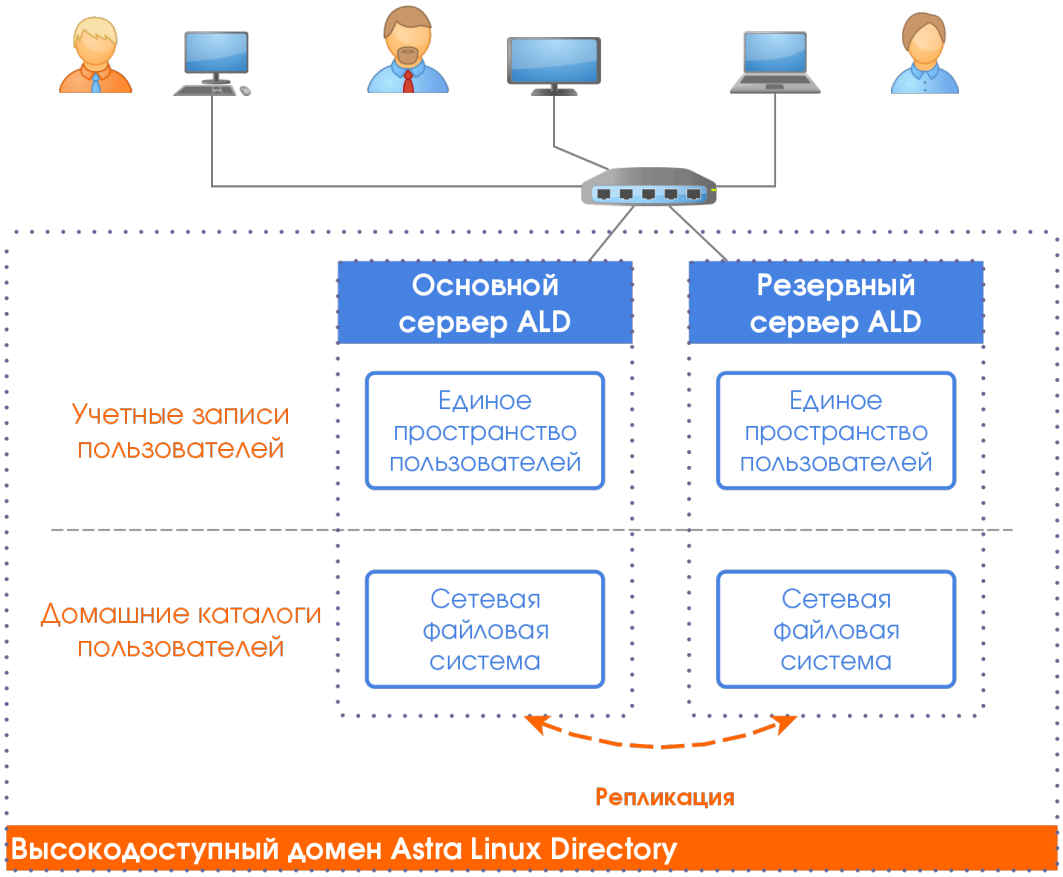
Высокодоступный домен Astra Linux Directory Лаборатории 50 — решение для создания домена ALD в конфигурации высокой готовности.

Разработанный Лабораторией 50 высокодоступный домен это:

— горячий резерв штатного Astra Linux Directory;

— минимальное время простоя и время переключения;

— сохранение всех штатных функций оригинального ПО.



Программное обеспечение вносит минимальные изменения в штатное ПО, поставляемое в составе дистрибутива Astra Linux Special Edition.

Высокодоступный домен ALD в стандартной конфигурации не использует разделяемых хранилищ. Все данные между серверами непрерывно реплицируются. Тем не менее, для хранения домашних каталогов пользователей вы можете использовать сетевое хранилище данных (SAN, NAS).

2.3 Совместимость

Высокодоступный домен ALD предназначен для работы с ОС СН Astra Linux Special Edition версий 1.3, 1.4 и 1.5.

2.4 Требования к аппаратной части

Для обеспечения отказоустойчивости необходимо соблюдение ряда требований к серверам высокодоступного домена ALD. Аппаратная часть должна быть совместима с операционной системой Astra Linux Special Edition.

Электропитание. Для обеспечения требований отказоустойчивости по питанию каждый сервер должен быть оснащён двумя блоками питания. Каждый блок питания должен быть достаточной мощности для работы сервера в случае отказа второго блока питания. Также необходима функция горячей замены блока питания без выключения сервера.

Подсистема хранения. При отсутствии выделенной системы хранения данных должна обеспечиваться отказоустойчивая конфигурация подсистемы хранения. Рекомендуется использовать RAID массив в отказоустойчивой конфигурации (уровни 1, 6) с безбатарейным кэшем (на основе флеш-памяти).

Сеть. Для обеспечения сетевой избыточности необходимо как минимум два сетевых интерфейса Ethernet, обладающих одинаковыми характеристиками. При использовании сетевого агрегирования рекомендуется объединять сетевые интерфейсы с различных сетевых плат. Такая схема устойчива к отказу одной из сетевых плат или PCI (PCI-E) моста.

3 Архитектура

Архитектура Высокодоступного домена Astra Linux Directory отражает решение следующих основных задач:

— обеспечение доступности сервисов домена при отказах программного и аппаратного обеспечения;

— прозрачное подключение клиентов Astra Linux Directory;

— сохранение всех функций домена;

— минимальное вмешательство в оригинальный продукт.

3.1 Обеспечение готовности

Доступность ресурсов домена ALD при программных или аппаратных отказах достигается путём дублирования всех элементов. Высокодоступный домен Astra Linux Directory представляет собой двухузловой отказоустойчивый кластер.

3.1.1 Аппаратная часть

Программный комплекс предназначен для работы в кластере из двух серверов в целях обеспечения отказоустойчивости. Кластер должен соответствовать требованиям по уровню резервирования сетевой подсистемы, а также подсистем хранения данных и электропитания.

Отказоустойчивость сетевой подсистемы как правило обеспечивается комбинацией решений следующих задач: а) отказоустойчивости соединений; б) отказоустойчивости активного оборудования. В состав программного комплекса ВД ALD включены необходимые средства для настройки избыточности сетевых каналов.

Отказоустойчивость подсистемы электропитания может достигаться за счёт дублирования блока питания в каждом сервере, а также сопутствующей внешней периферии.

Высокодоступный домен ALD способен работать как с внешним отказоустойчивым хранилищем, так и с внутренними средствами на используемых серверах.

3.1.2 Программное обеспечение

В основе Высокодоступного домена Astra Linux Directory лежит система управления кластером высокой готовности «Pacemaker». Pacemaker определяет отказы программного обеспечения и аппаратных средств и немедленно осуществляет перезапуск приложения или систем без вмешательства оператора.

Такой процесс называется преодолением отказа. В процессе преодоления отказа система управления кластером может производить подготовку узла для запуска на нём приложения. Например, монтировать сетевую файловую систему, настраивать сетевые интерфейсы, запускать требуемое вспомогательное ПО.

Основные возможности Pacemaker:

— обнаружение и восстановление сбоев узлов и сервисов;

— широкие варианты конфигурации создаваемой избыточности;

— узловой и ресурсный фенсинг;

— задание отношений и групп между управляемыми ресурсами;

— автоматическая репликация конфигурации в кластере;

— не требует разделяемого хранилища.

3.2 Структура программного комплекса

Домен Astra Linux Directory, входящий в состав ОС Astra Linux Special Edition, состоит из ряда структурных элементов, централизующих следующие функции:

— сквозная аутентификация в сети;

— хранение информации об окружении пользователей;

— хранение настроек системы защиты информации на сервере;

— настройка правил регистрации событий безопасности в рамках домена;

— учёт подключаемых устройств;

— хранение домашних каталогов пользователей.

Kerberos 5

Для сквозной аутентификации в сети используется протокол Kerberos 5. В качестве реализации в Astra Linux Special Edition используется система MIT Kerberos. Пароли и ключи сервисов и пользователей хранятся во встроенной БД MIT Kerberos. В состав MIT Kerberos входят два основных элемента: службы KAdmin и KDC.

Служба KAdmin предназначена для управления учётными записями пользователей и сервисов домена. KDC — служба, управляющая выдачей билетов Kerberos.

В высокодоступном домене ALD репликация базы данных Kerberos выполняется встроенными средствами MIT Kerberos. При этом Службы KDC функционируют параллельно на двух серверах домена, таким образом повышая производительность при нормальной работе кластера.

OpenLDAP

Информация о пользователях, настройках защиты, регистрации событий и пр. хранится в каталогах LDAP. В качестве службы каталогов в Astra Linux Directory используется сервер OpenLDAP.

В высокодоступном домене Astra Linux Directory используется мастер-мастер репликация двух серверов OpenLDAP. Изменения в каталогах LDAP, внесённые через один сервер, непрерывно транслируются второму. При этом каждый сервер работает со своей базой данных, расположенной на локальном носителе.

ALD

В состав домена Astra Linux Directory входит служба aldd. Служба управляет всеми элементами домена, однако все данные хранит в каталогах LDAP.

Samba

Централизованное хранение домашних каталогов пользователей осуществляется с помощью сетевой защищённой ФС (СЗФС), в основу которой положена CIFS, работающая по протоколу SMB/CIFS. Протокол СЗФС содержит в себе сообщения, которые передают информацию о стандартных и расширенных атрибутах (атрибутах безопасности), а также сообщения для передачи мандатной метки субъекта доступа.

СЗФС состоит из сервера и клиента. Сервер представляет собой расширенный сервер Samba и выполняет следующие задачи: управление разделяемыми ресурсами и контроль доступа к разделяемым ресурсам. При подключении клиента сервер устанавливает мандатную метку процесса, обслуживающего запросы клиента, в соответствии с мандатной меткой этого клиента. Этим обеспечивается мандатный контроль доступа к разделяемым файлам на стороне сервера.

СЗФС состоит из нескольких компонентов:

— `smbd` — сервисная служба, которая обеспечивает работу службы печати и разделяемого хранилища;

— `nmbd` — сервисная служба, которая обеспечивает работу службы имен NetBIOS, а также может использоваться для запроса других сервисных служб имен.

Домен Astra Linux Directory в составе Astra Linux Special Edition располагает встроенными возможностями по использованию выделенных хранилищ данных для размещения домашних каталогов пользователей.

Высокодоступный домен ALD предлагает встроенные средства для организации репликации домашних каталогов пользователей на основе DRBD. DRBD — репликация блочных устройств по локальной сети. DRBD поддерживает как син-

хронную, так и асинхронную репликацию. Также есть возможность использовать промежуточный протокол, при котором запись считается успешной, если она завершилась на локальный диск и удалённый узел подтвердил получение (но не локальную запись) данных.

Структурная схема

Программный комплекс состоит из двух идентичных серверов. Переключение режима работы главный — резервный производится автоматически системой управления кластером. Клиенты подключаются к сервисам домена по плавающему IP-адресу, который в каждый момент времени соответствует конкретному серверу.

Структурная схема Высокодоступного домена Astra Linux Directory показана на рис. 3.1.

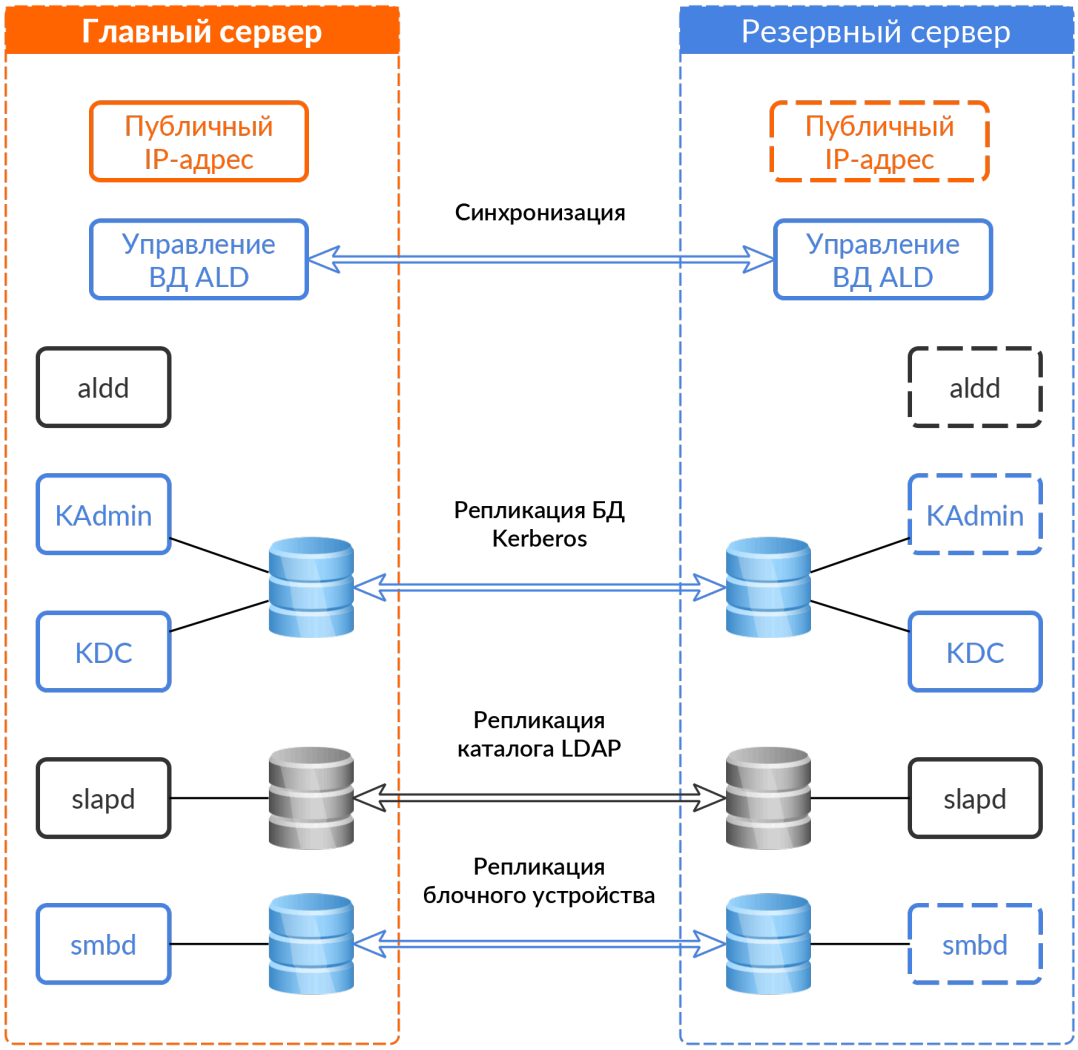


Рис. 3.1: Структурная схема ВД ALD

Службы KAdmin, smbd, aldd и плавающий IP-адрес функционируют только на главном сервере. При смене режима сервера, эти службы автоматически вклю-

чаются и выключаются по необходимости. Службы KDC, slapd (OpenLDAP) и drbd постоянно работают на узлах кластера, производя репликацию между серверами.

Управление службами производится полностью автоматически Службой haald и не требует вмешательства оператора. Тем не менее, системный администратор по своему усмотрению может переключать режимы серверов, управлять службами и производить другие необходимые действия.

Безопасность

Программное обеспечение Высокодоступного домена Astra Linux Directory не вносит каких-либо изменений в комплекс средств защиты информации ОС Astra Linux Special Edition. Репликации баз данных служб ALD происходит во внутренней сети кластера, не имеющей внешних подключений. В простейшем случае эту сеть возможно организовать путём прямого соединения двух серверов.

Пользовательские подключения происходят через внешнюю сеть на плавающий IP-адрес.

4 Подключение пользователей

Программное обеспечение Высокодоступного домена Astra Linux Directory вносит минимальные изменения в оригинальное ПО ОС Astra Linux Special Edition. Пользовательские подключения происходят через внешнюю сеть на плавающий IP-адрес. Схема взаимодействия и протоколы подключения не изменяются. С точки зрения внешних подключений программный комплекс полностью совместим с исходным Astra Linux Directory.

Плавающему IP-адресу должно соответствовать имя узла сервера ALD, используемое при настройке клиентов ALD. Однако, существует возможность использования двух служб KDC, расположенных на разных серверах кластера. Эта штатная возможность MIT Kerberos, предназначенная для повышения доступности сервиса.