Приложение Б.

Рекомендации производителя ООО «Русбитех-Астра» обновлению ALD Pro до версии 2.3.0

«ПЕРЕХОД с версии 1.4.1 на версию 2.3.0 ALD Pro»

описание архитектуры и Рекомендации

АО РНПК

содержание

[Назначение документа 4](#_Toc173683371)

[1 Функциональные возможности решения ALD Pro 6](#_Toc173683372)

[1.1 Задачи, решаемые продуктом 6](#_Toc173683373)

[1.2 Отказоустойчивость и высокая доступность 6](#_Toc173683374)

[1.3 Функционал управления 6](#_Toc173683375)

[1.4 Мониторинг 7](#_Toc173683376)

[1.5 Журналирование 7](#_Toc173683377)

[1.6 Доверительные отношениями 7](#_Toc173683378)

[1.7 Миграция 8](#_Toc173683379)

[2 Компонентный состав решения ALD Pro 9](#_Toc173683380)

[2.1 Описание подсистем ALD Pro 9](#_Toc173683381)

[2.2 Общая схема архитектуры ALD Pro 11](#_Toc173683382)

[3 Описание взаимодействия служб 13](#_Toc173683383)

[3.1 Общая схема взаимодействия служб ALD Pro 13](#_Toc173683384)

[3.2 Сервис службы динамической адресации (DHCP) 15](#_Toc173683385)

[3.3 Сервис точного времени 15](#_Toc173683386)

[3.4 Сервис службы имен 15](#_Toc173683387)

[3.5 Модуль синхронизации 16](#_Toc173683388)

[3.5.1 Рекомендации 17](#_Toc173683389)

[3.5.2 Схема построения инфраструктурных сервисов домена 18](#_Toc173683390)

[4 Интеграция ALD Pro c MS AD. 19](#_Toc173683391)

[4.1 Понятие доверительных отношений 19](#_Toc173683392)

[4.2 Доверительные отношения между ALD Pro и MS AD. 20](#_Toc173683393)

[4.2.1 Контроллеры доверия и агенты доверия 21](#_Toc173683394)

[4.2.2 Доверительные отношения между двумя доменами (External Trust). 22](#_Toc173683395)

[4.3 Реализация доверительных отношений 22](#_Toc173683396)

[5 Инфраструктура развёртывания решения 23](#_Toc173683397)

[5.1 Необходимое программное обеспечение 23](#_Toc173683398)

[5.2 Варианты развёртывания компонентов решения 23](#_Toc173683399)

[5.3 Обеспечение связанности служб по протоколам и портам 23](#_Toc173683400)

[5.4 Обеспечение сетевой связанности между сервисами 23](#_Toc173683401)

[Приложение 1. Обеспечение связанности служб по протоколам и портам 24](#_Toc173683402)

[Приложение 2. Требования к сетевой связанности между сервисами 40](#_Toc173683403)

# Назначение документа

Данный документ содержит описание архитектуры решения и принципы построения инфраструктуры на базе продукта ALD Pro Группы Астра с применением перечня стандартных ролей из состава решения.

**Основные термины и определения, обозначения и сокращения.**

|  |  |
| --- | --- |
| Термин/сокращение | Определение |
| ALSE | Astra Linux Special Edition – сертифицированная ОС со встроенными средствами защиты информации для стабильной и безопасной работы ИТ–инфраструктур любого масштаба и обработки информации различной степени конфиденциальности |
| DHCP | Dynamic Host Configuration Protocol – протокол динамической настройки узла – сетевой протокол, позволяющий сетевым устройствам автоматически получать IP–адрес и другие параметры, необходимые для работы в сети TCP/IP |
| DNS | Domain Name System – система доменных имён – компьютерная распределённая система для получения информации о доменах |
| DNSSEC | Набор расширений IETF протокола DNS. Предоставляет DNS-клиентам гарантии достоверности и целостности данных |
| FTP | File Transfer Protocol - протокол передачи файлов по сети |
| KDC | Key Distribution Center - служба распространения ключей доверяющего домена |
| Kerberos | Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними |
| LDAP | Lightweight Directory Access Protocol - протокол прикладного уровня для доступа к службе каталогов |
| MS AD (AD) | Active Directory – службы каталогов корпорации Microsoft для операционных систем семейства Windows Server |
| NTP | Network Time Protocol - протокол сетевого времени |
| Samba suite | Пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB/CIFS |
| SID | Security Identifier (идентификатор безопасности) - структура данных, которая идентифицирует учётную запись пользователя, группы, службы, домена или компьютера |
| SMB | Server Message Block — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам |
| SSSD | System Security Services Daemon — это сервис для управления доступом к удалённым каталогам и механизмам проверки подлинности |
| Stratum2 | Сервер точного времени второго уровня, получает данные от серверов первого уровня |
| TFTP | Trivial File Transfer Protocol (Простой протокол передачи файлов) — это протокол прикладного уровня, предназначенный для передачи файлов |
| TGT | Ticket-Granting Ticket – технология Kerberos, содержит сеансовый ключ для засекречивания общения между клиентом и сервером выдачи билетов |
| АРМ | Автоматизированное рабочее место |
| АС, Система | Автоматизированная система |
| ИС | Информационная система |
| ИБ | Информационная безопасность |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| Серверная ОС | Система, на которую должна устанавливаться система управления, развертываться все необходимые подсистемы |
| СУБД | Система управления базами данных |

# Функциональные возможности решения ALD Pro

В качестве системы централизованного управления для операционных систем Astra Linux используется ALD Pro.

## Задачи, решаемые продуктом

Продукт ALD Pro предназначен для централизованного управления ресурсами (физическими и виртуальными рабочими местами), работающими под управлением операционной системы Astra Linux, и может использоваться в организациях различного масштаба. ALD Pro может применяться в информационных (автоматизированных) системах, обрабатывающих как общедоступную информацию, так и информацию с ограниченным доступом.

## Отказоустойчивость и высокая доступность

Предлагаемое решение обладает отказоустойчивостью и обеспечивает высокую доступность предоставляемых сервисов. Это обеспечивается такими мерами, как:

* использование нескольких контроллеров домена;
* возможность репликации данных между контроллерами домена.

## Функционал управления

Решение обладает широкими возможностями по управлению инфраструктурой и обеспечивает выполнение следующих функций:

* Настройка и конфигурация серверной группировки ALD Pro из портала управления;
* Настройка и конфигурация ОС и программного обеспечения клиентов ALD Pro из портала управления;
* Удаленное подключение к сессиям клиентов через портал управления;
* Управление конфигурацией ОС на АРМ и серверах (установка/удаление программных пакетов, профилей пользователей, внешнего вида графической оболочки ОС);
* Управление учетными записями пользователей и групп пользователей (создание, удаление, изменение параметров, изменение состава пользователей в группах);
* Управление компьютерами и группами компьютеров (включение/исключение из домена, управление параметрами; создание/удаление/изменение состава компьютеров в группах);
* Установка ОС по сети;
* Создание и управление файловыми сетевыми ресурсами общего доступа;
* Управление принтерами;
* Управление организационной структурой подразделений (создание и удаление подразделений, выстраивание иерархической структуры);
* Управление групповыми политиками (создание, удаление, изменение параметров, назначение на организационные подразделения).
* Автоматизация установки и настройки программного обеспечения.

## Мониторинг

Решение обеспечивает возможность мониторинга работы, которая реализуется посредством специального сервера мониторинга, который собирает все требуемые метрики и предоставляет возможность отображения статуса выполняемых задач на портале управления.

## Журналирование

В целях документирования работы системы предусмотрена возможность журналирования событий с использованием специального сервера ведения журналов, который выполняет:

* сбор журналов с серверов группировки ALD Pro;
* загрузку журналов с клиентов ALD Pro.

## Доверительные отношениями

Построение двусторонних доверительных отношений с каталогом объектов Microsoft Active Directory.

Доверительные отношения дают возможность пользователям одного домена выполнять прозрачную аутентификацию по протоколу Kerberos при обращении к ресурсам другого домена.

Двусторонние доверительные отношения, предоставляют возможность общаться доменам ALD Pro и MS AD, решая ряд важных задач:

* Авторизация пользователей доверенных доменов на рабочих станциях;
* Доступ к сетевым ресурсам пользователей доверенного домена (веб сервер, файловый сервер, базы данных и т.д.);
* Разграничение доступа к ресурсам доверенных доменов.

## Миграция

Перемещение объектов из каталога Microsoft Active Directory в каталог ALD Pro.

Следующие сущности доступны для миграции из домена Microsoft Active Directory в ALD Pro:

- пользователи (users);

- группы пользователей (groups);

- организационные подразделения (organizational units).

# Компонентный состав решения ALD Pro

## Описание подсистем ALD Pro

ALD Pro представляет собой совокупность подсистем, размещенных на нескольких серверах, объединённых в сеть.

Архитектура решения ALD Pro представлена следующими подсистемами:

* Подсистема «Пользователи и компьютеры»;
* Подсистема «Групповые политики»;
* Подсистема «Управление доменом»;
* Подсистема «Установка и обновление ПО»;
* Подсистема «Инвентаризация»;
* Подсистема «Автоматизация»;
* Подсистема «Роли и службы»;
* Серверная операционная система;
* Пользовательская операционная система.

Подсистема «Пользователи и компьютеры» предназначена для управления организационной структурой, пользователями и компьютерами. Данная функциональность обеспечивается следующими модулями:

* Модуль «Управление пользователями и компьютерами»;
* Модуль «Управление организационной структурой»;
* Модуль «Управление группами пользователей и компьютеров»;
* Модуль «Удаленный доступ».

Подсистема «Групповые политики» предназначена для настройки компьютеров и серверов, управления паролями, доступом к узлу и механизмом повышения привилегий. Данная функциональность обеспечивается следующими модулями:

* Модуль «Групповые политики»;
* Модуль «Политики доступа к узлу»;
* Модуль «Политики повышения привилегий»;
* Модуль «Политики паролей».

Подсистема «Управление доменом» предназначена для управления структурой и конфигурацией Системы. Данная функциональность обеспечивается следующими модулями:

* Модуль «Сайты и службы»;
* Модуль «Параметры групповой политики»;
* Модуль «Службы и параметры Kerberos»;
* Модуль «Интеграция с MS AD»;
* Модуль «Роли и права доступа».

Подсистема «Установка и обновление ПО» предназначена для управления журналом заданий, группировкой программного обеспечения и управления репозиториями. Данная функциональность обеспечивается следующими модулями:

* Модуль «Политики ПО»;
* Модуль «Перечень/каталог ПО»;
* Модуль «Репозитории ПО».

Подсистема «Автоматизация» предназначена для удаленного выполнения команд или скриптов на компьютере, группе компьютеров, или группе компьютеров, принадлежащих подразделению, а также для установки ОС по сети. Данная функциональность обеспечивается следующими модулями:

* Модуль «Установка ОС по сети»;
* Модуль «Автоматизация».

Подсистема «Роли и службы» предназначена для динамической настройки узла, управления механизмами синхронизации времени, системами печати а также системой доменных имён. Данная функциональность обеспечивается следующими модулями:

* Модуль «Управление разрешением имен (DNS)»;
* Модуль «Динамическая настройка узла»;
* Модуль «Управление/синхронизация времени»;
* Модуль «Печать».

Подсистема «Инвентаризация» предназначена для сбора информации о программно-аппаратных активах компании, входящих в домен. Данная функциональность обеспечивается следующим модулем:

* Модуль «Инвентаризация».

Серверная операционная система предназначена для развертывания и обеспечения функциональности АС ALD Pro.

Пользовательская операционная система предназначена для развёртывания ПО, обеспечивающего функциональность, которая необходима пользователю/клиенту для решения производственных задач.

## Общая схема архитектуры ALD Pro

Архитектура ALD Pro схематично изображена на диаграмме (Рисунок 1).

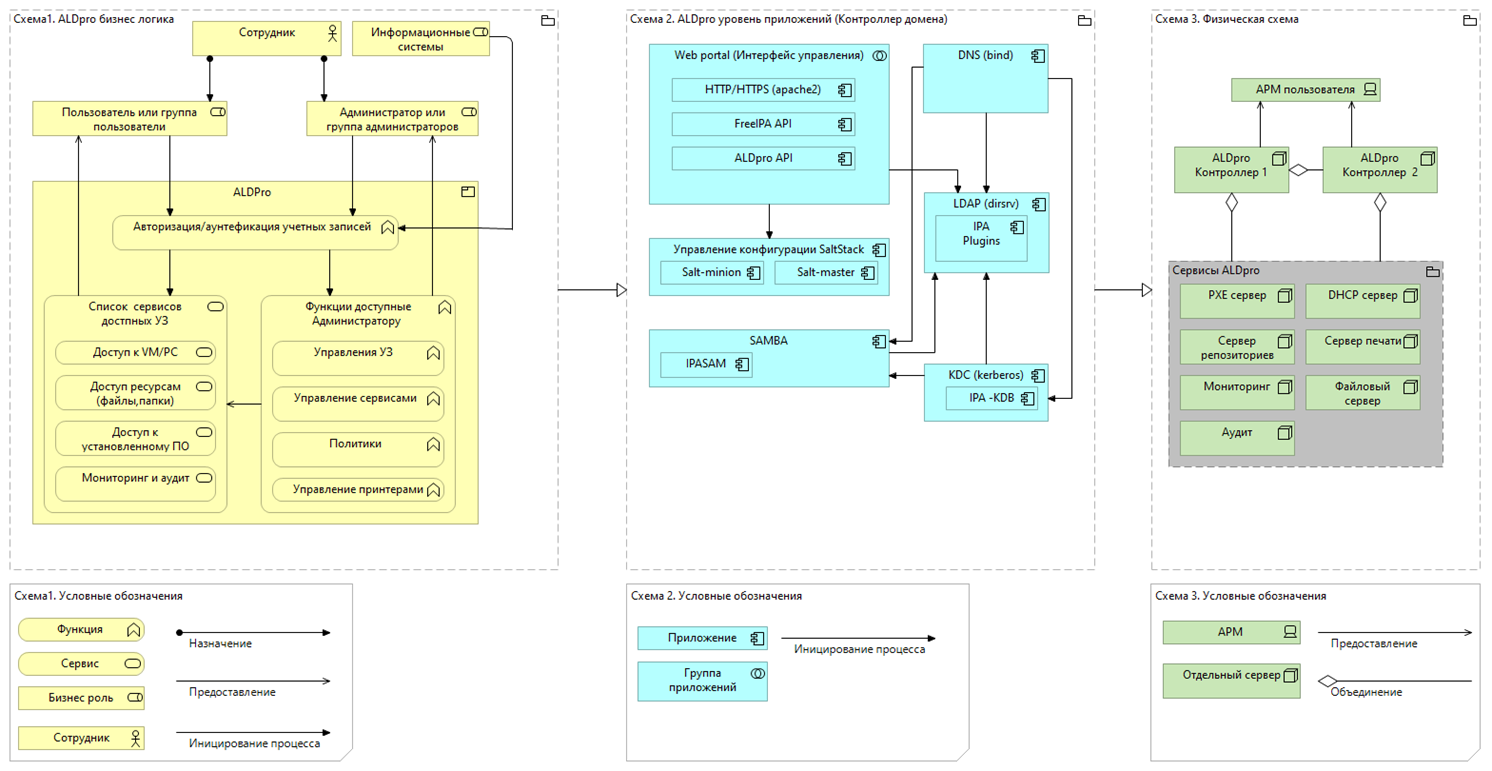


Рисунок 1. Архитектура ALD Pro

# Описание взаимодействия служб

## Общая схема взаимодействия служб ALD Pro

Общая схема взаимодействия служб ALD Pro представлена на диаграмме ниже (Рисунок 2)

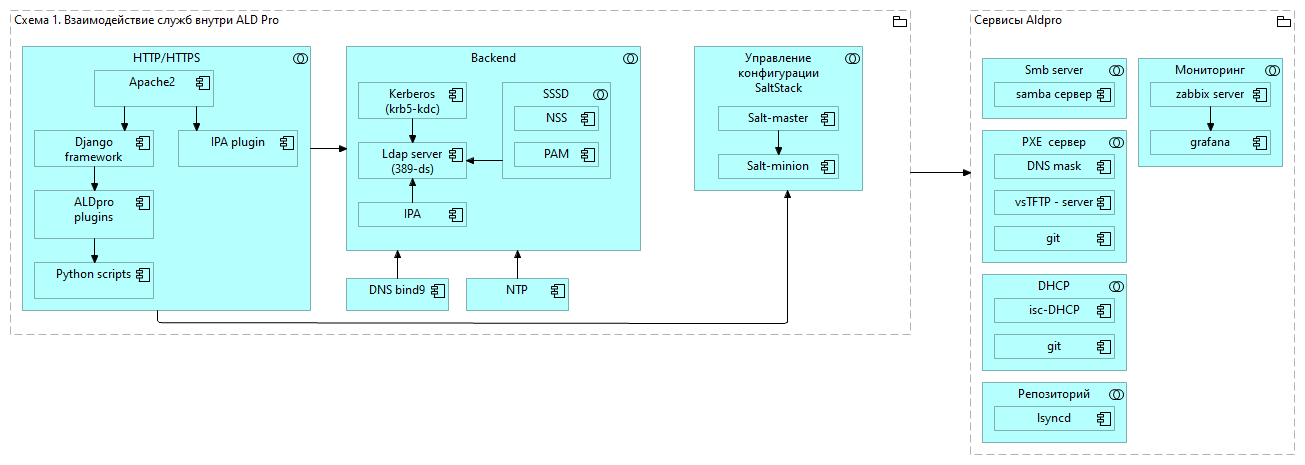


Рисунок 2. Схема взаимодействия служб ALD Pro

## Сервис службы динамической адресации (DHCP)

При использовании DHCP, не входящего в инфраструктуру ALD Pro, для подсистемы установки ОС по сети (PXE сервер) необходимо добавить следующие DHCP опции:

* Опция 66 - Определяет имя сервера TFTP.
* Опция 67 - Задает имя загрузочного файла. Может использоваться вместо ключевого слова bootfile, которое помещает файл в поле filename пакета.

## Сервис точного времени

Точное время необходимо для корректного формирования сертификатов, а также для работы таких сервисов, как Kerberos и система логирования.

Важную роль в функционировании ALD Pro выполняет служба точного времени, работа которой осуществляется по протоколу NTP. Источниками данных о времени для этой службы могут быть:

* серверы точного времени из сети Интернет;
* серверы точного времени Организации.

При выборе первичного источника времени для всех информационных систем, необходимо руководствоваться следующими условиями:

* поддержка протокола NTPv3;
* уровень доверия не ниже Stratum2.

В пуле серверов и клиентов ALD Pro, синхронизация контроллеров-реплик будет выполняться с основным источником пула (основной контроллер ALD Pro), который, в свою очередь, будет синхронизироваться с первичным источником времени всех информационных систем Организации. Все рабочие станции, входящие в состав комплекса, управляемого ALD Pro, синхронизируются по времени с ближайшим источником (контроллером ALD Pro) для корректной работы приложений.

## Сервис службы имен

DNSSEC - набор расширений IETF протокола DNS, позволяющих минимизировать атаки, связанные с подменой IP-адреса при разрешении доменных имён. Он направлен на предоставление DNS-клиентам (англ. термин resolver) гарантии достоверности и целостности данных.

Сервис DNSSEC - включен в состав ALD Pro по умолчанию.

При использовании глобальных перенаправителей с отключенным DNSSEC на них, необходимо отключить использование DNSSEC в ALD Pro.

В случае установки доверительных отношений с MS AD и включенным DNSSEC, необходимо его настроить и в ALD Pro. В противном случае доверительные отношения не будут установлены.

При необходимости, запись о домене (зоне) ALD Pro может быть размещена на внешнем сервисе имен (DNS/BIND) при условии отсутствия такой же записи о домене (зоне), принадлежащей другой системе.

Согласно международному стандарту RFC-2606 не допускается использование доменных имен, оканчивающихся на:

* *.test*
* *.local*
* *.example*
* *.invalid*
* *.localhost*

## Модуль синхронизации

Переименование подразделений, добавленных в «Сопоставление подразделений» недопустимо. Если возникла такая необходимость, корректным будет удалить сопоставление, произвести переименование и создать новое сопоставление подразделений.

Если для подразделения уже установлена синхронизация, то создавать сопоставления для его дочерних подразделений нельзя.

Атрибуты по умолчанию и соответствующие им сопоставления ограничены перечнем обязательных атрибутов для объектов ALD Pro:

* Пользователи: «Логин», «Пароль», «Фамилия», «Имя», «Подразделение»;
* Группы пользователей: «Название группы», «Подразделение»;
* Подразделения: «Наименование подразделения», «Родительское подразделение».

При этом, не все эти атрибуты явно указаны на карточке «Атрибуты AD», так как их синхронизация происходит при выполнении внутренних процессов Модуля синхронизации. Добавляя эти атрибуты в явном виде в карте сопоставления, можно нарушить логику работы модуля синхронизации.

Наименования подразделений, наименования групп и логины пользователей не должны содержать специальных символов, за исключением ".", "-", "\_".

Модуль синхронизации может быть установлен при первичной инсталляции или в процессе обновления контроллера домена. Ограничением настоящей версии является то, что модуль синхронизации устанавливается только на первый контроллер домена. В случае отключении первого контроллера домена, синхронизация новых данных, добавленных после отключения первого контроллера домена, выполняться не будет. Ранее синхронизированные данные сохранятся и будут реплицироваться между контроллерами домена, для которых созданы соглашения о репликации.

Для успешной синхронизации необходимо добавить в группу admins учетную запись администратора, которая используется для подключения к контроллеру домена.

### Рекомендации

Ввиду односторонних доверительных отношений и распространении групповых политик построенного решения на версии ALD Pro 1.4.1 предлагается переход на версию 2.3.0, провести следующие работы:

- Провести обследование развернутого решения;

- Скопировать действующие групповые политики;

- Скопировать дополнительные скрипты автоматизации;

- Развернуть и настроить серверную группировку ALD Pro 2.3.0;

- Доработать групповые политики под ALD Pro версии 2.3.0;

- Имплементировать доработанные групповые политики и дополнительные скрипты автоматизации в развернутую инфраструктуру ALD Pro версии 2.3.0;

- Перенести с серверов репозиториев кастомизированные рапозитории на ALD Pro версию 2.3.0;

- Настроить автоматизированную установку ОС версии 1.7.5uu1 по сети;

- Настроить доверительные отношения действующего MS AD и ALD Pro версии 2.3.0;

- Провести проверку возможности интеграции ИС в действующей инфраструктуре со службой каталогов ALD Pro версии 2.3.0;

### Схема построения инфраструктурных сервисов домена

Предлагаемая компонентная схема построения инфраструктурных сервисов домена приведена на диаграмме ниже (Рисунок 3)

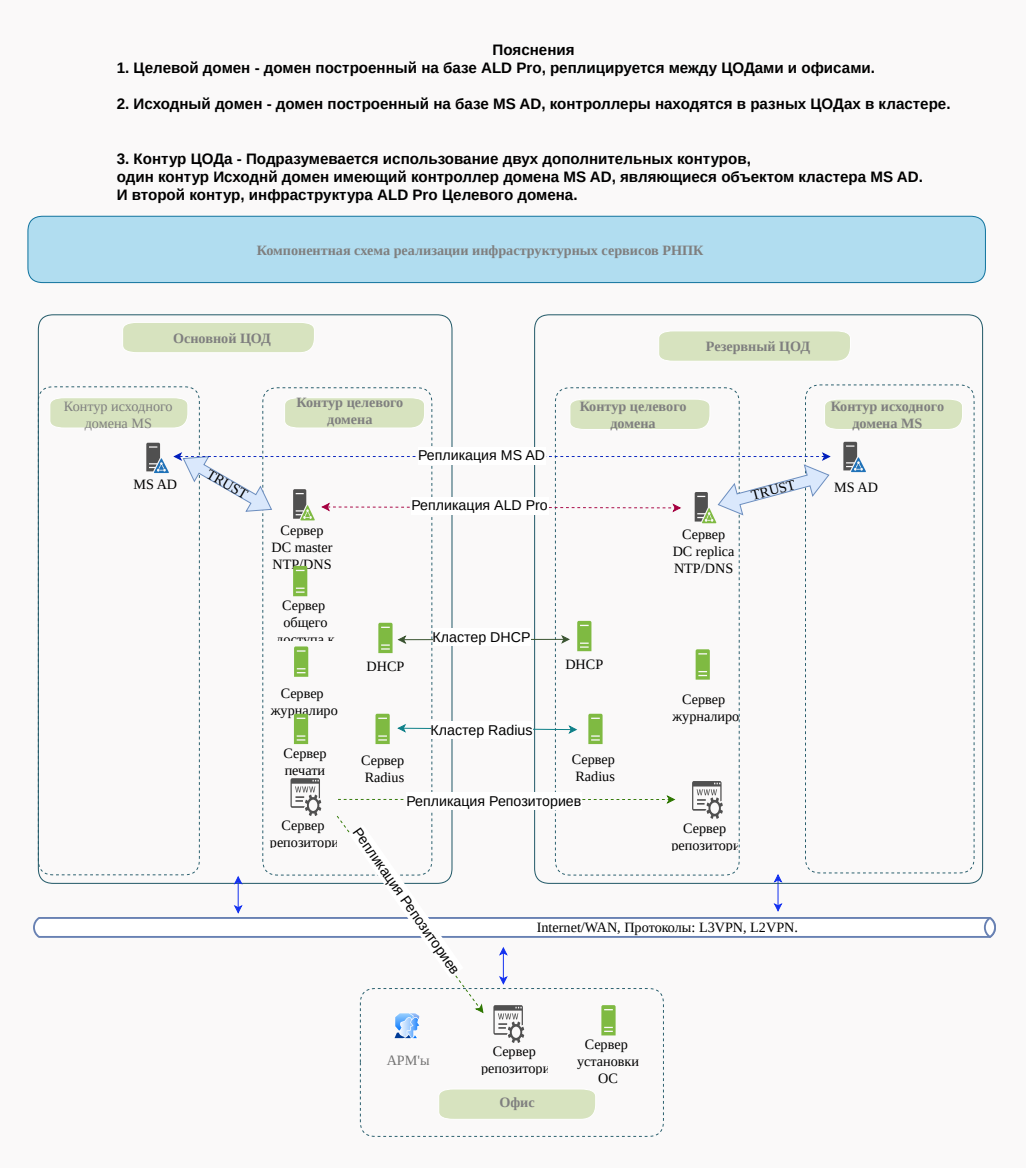


Рисунок 3. Схема построения инфраструктурных сервисов домена

# Интеграция ALD Pro c MS AD.

## Понятие доверительных отношений

Установление доверительных отношений между двумя доменами означает, что доверяющий домен (trusting domain) доверяет процесс аутентификации доверенному домену (trusted domain). Пользователь, аутентифицированный доверенным доменом, может получить доступ к ресурсам в доверяющем домене.

Доверительные отношения между доменами бывают двух типов:

* одностороннее доверие — позволяет пользователям и группам из домена A получать доступ к ресурсам в домене Б, но не наоборот. Домен A доверяет домену Б, но домен Б не доверяет домену A. При создании такого доверия нужно указать направление (входящее или исходящее);
* двустороннее доверие — позволяет пользователям и группам из домена A получать доступ к ресурсам в домене Б и наоборот. Запросы проверки подлинности могут передаваться между двумя доменами в обоих направлениях. Домен А доверяет домену Б, а домен Б доверяет домену А.

## Доверительные отношения между ALD Pro и MS AD.

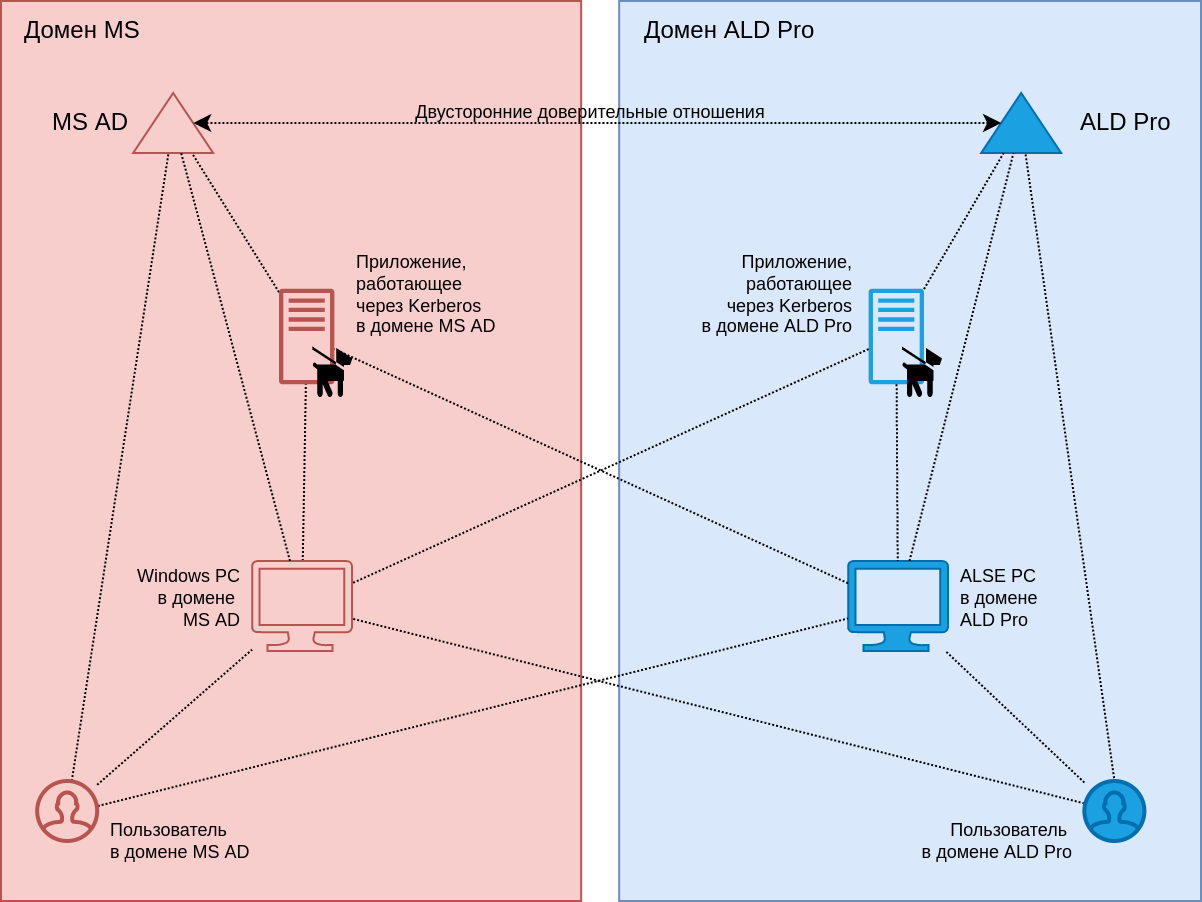
Алгоритм использования двусторонних доверительных отношений между ALD Pro и MS AD, представлен на рисунке ниже (Рисунок 4).

Рисунок 4. Алгоритм использования доверительных отношений между ALD Pro и AD

1. Пользователю доверенного домена ALD Pro нужно пройти аутентификацию в службе из доверяющего домена MS AD.
2. Пользователь ALD Pro успешно проходит аутентификацию на контроллере ALD Pro и получает от него TGT билет.
3. Пользователь ALD Pro обращается к своему контроллеру за сервисным билетом к службе из доверяющего домена MS AD. Контроллер ALD Pro видит, что служба находится в доверяющем домене MS AD, поэтому выписывает билет на выполнение рекурсивного Kerberos-запроса к контроллеру из доверяющего домена MS AD. Билет будет зашифрован паролем служебной учетной записи, соответствующей доверительному отношению. Таким образом, пользователь получает, как бы, сервисный билет на доступ к службе распространения ключей доверяющего домена (Key Distribution Center, KDC).
4. Пользователь ALD Pro обращается с полученным билетом к контроллеру доверяющего MS AD, совершая тем самым рекурсивный Kerberos-запрос. Контроллер MS AD расшифровывает билет, используя пароль учетной записи, соответствующей доверительному отношению и доверяя результатам проверки аутентичности пользователя, которая выполнялась контроллером ALD Pro, выписывает пользователю сервисный билет на доступ к своей службе.
5. Затем клиент обращается к службе из домена MS AD, используя сервисный билет, полученный от контроллера из этого же домена.

### Контроллеры доверия и агенты доверия

**Контроллеры доверия (Trust controllers)**

ALD Pro контроллеры могут выполнять поиск идентификационных данных на контроллерах домена AD. Они также запускают Samba suite, чтобы установить доверительные отношения с AD. Контроллеры домена AD связываются с контроллерами доверия при установлении и проверке доверия к AD. Компьютеры, зарегистрированные в AD, взаимодействуют с контроллерами доверия ALD Pro для запросов аутентификации Kerberos.

Первый контроллер доверия создается при настройке доверия. Контроллеры доверия управляют большим количеством сетевых служб, чем агенты доверия и таким образом, представляют большую площадь для атак потенциальных злоумышленников.

Контроллер доверия - это мастер FreeIPA, который запускает следующие службы:

* Сервер LDAP с плагинами sigden, extdom и ldap;
* KDC с драйвером IPA;
* Samba - сконфигурирована с помощью модуля ipasam PASSDB;
* SSSD с ipa\_server\_mode=True;
* Экземпляр глобального каталога (отдельный экземпляр LDAP с AD-совместимой схемой).

**Агенты доверия (Trust agents)**

Серверы ALD Pro, которые могут разрешать запросы идентификационных данных от клиентов ALSE к контроллерам домена AD, используя SSSD. В отличие от контроллеров доверия, агенты доверия не могут обрабатывать запросы на аутентификацию Kerberos.

Доверительный агент - это мастер FreeIPA, который запускает следующие сервисы:

* Сервер LDAP с подключаемыми модулями siding и ext dom
* KDC с драйвером IPA
* SSSD с ipa\_server\_mode=True.

Статус существующего контролера доверия не может быть понижен до статуса агента доверия.

### Доверительные отношения между двумя доменами (External Trust).

Внешнее доверие (External Trust) - это доверительные отношения между доменами MS AD, которые находятся в разных лесах MS AD. В то время как для обеспечения доверия к лесу всегда требуется установить доверие между корневыми доменами лесов MS AD, внешнее доверие может быть установлено к любому домену в лесу.

Внешнее доверие между доменами MS AD по определению является нетранзитивным и обеспечивает фильтрацию SID между границами домена. Это означает, что только пользователи и группы с SID из доверенного домена могут использовать ресурсы и быть видимыми в системах ALD Pro. Никому из других пользователей и групп из доменов, которым доверенный домен доверяет в своем собственном лесу MS AD, или других доменов, которым доверяют извне, не будет разрешен доступ к ресурсам ALD Pro.

## Реализация доверительных отношений

Функция внешнего доверия повторно использует существующую инфраструктуру «лесного» доверия.

Существует механизм, позволяющий поддерживать внешнее доверие:

* Нетранзитивность: поскольку внешнее доверие является нетранзитивным по определению, любая попытка установить функцию транзитивности доверительной ссылки с помощью команды *LSA SetInformationTrustedDomain()* завершится неудачей. Таким образом, нет необходимости устанавливать транзитивность для внешнего доверия;
* Атрибуты доверия: внешнее доверие может быть обнаружено путем проверки отсутствия атрибута *ipaNTTrustAttributes* LDAP объекта доверенного домена.

# Инфраструктура развёртывания решения

## Необходимое программное обеспечение

Программное обеспечение, необходимое для развёртывания решения представлено в таблице ниже (Таблица 3).

Таблица 3 Перечень программного обеспечения

| Тип | Наименование | Версия |
| --- | --- | --- |
| ОС | ALSE | 1.7.5uu1 |
| Программный комплекс | ALD Pro | 2.3.0 |

## Варианты развёртывания компонентов решения

Подсистемы ALD Pro могут быть развёрнуты в виде серверной группировки, которая размещается на:

* Физических серверных ресурсах;
* Виртуальных машинах;
* Любой комбинации физических и виртуальных ресурсов.

## Обеспечение связанности служб по протоколам и портам

В таблице ниже (Приложение 1, Таблица 4) представлены требования по обеспечению сетевой связанности служб ALD Pro.

## Обеспечение сетевой связанности между сервисами

В таблице ниже (Приложение 2, Таблица 5) представлены требования по обеспечению сетевой связанности между сервисами ALD Pro.

## Требования к предоставляемым сертификатам Вендора.

Сертификатом должен являться документ, предоставляющий право воспользоваться услугами производителя программного комплекса ALD Pro и ОС ALSE на оказание услуг по внедрению указанных продуктов. Документ должен иметь парт-номер производителя и зарегистрирован в системе учета ПАО Группа Астра.

Приложение 1. Обеспечение связанности служб по протоколам и портам

Таблица 4 Связанность служб

| доменный компьютер | IP адрес из локальной сети | контроллер домена | Apache (apache2) | IP адрес контроллера домена | 443 | TCP | HTTPS | доменный компьютер, контроллер домена | Администрирование домена через веб-портал, утилиту ipa, или прямые запросы к REST API |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | Apache (apache2) | IP адрес контроллера домена | 443 | TCP | HTTPS | доменный компьютер, контроллер домена | Самообслуживание пользователей через веб-портал |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | Daphne (python3) | IP адрес контроллера домена | 8008 | TCP | HTTPS | доменный компьютер, контроллер домена | Передача всплывающих уведомлений на портале управления |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | Apache (apache2) | IP адрес контроллера домена | 80 | TCP | HTTP | доменный компьютер, контроллер домена | Загрузка публичного корневого сертификата домена, может использоваться для настройки HTTPS, LDAPS http://адрес.контроллера/ipa/config/ca.crt |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | Bind9 (named-pkcs11) | IP адрес контроллера домена | 53 | TCP/UDP | DNS, GSS-TSIG | доменный компьютер, контроллер домена | Запрос DNS-записей. Большинство запросов будет обрабатываться с использованием протокола UDP, а переключение на TCP происходит, если ответы сервера будут превышать 512 байт на одно сообщение. По этому же порту происходит динамическое обновление DNS-записей со стороны клиентов по протоколу GSS-TSIG |
| - | - | контроллер домена | Bind9 (named-pkcs11) | 127.0.0.1 | 953 | TCP | DDNS | контроллер домена | Функция удаленного управления DNS сервером BIND через rndc не требуется, она необходима, например, при настройке динамического обновления DNS-записей с DHCP сервера. Порт слушается только на localhost. |
| - | - | доменный компьютер | Fly-dm (fly-dm) | 127.0.0.1 | 177 | UDP | XDMCP | доменный компьютер | Функция удаленного входа в систему автономным дисплеем по протоколу XDMCP не используется. Порт слушается только на localhost. |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | MIT Kerberos (krb5kdc) | IP адрес контроллера домена | 88 | TCP/UDP | KRB5 | доменный компьютер, контроллер домена | Аутентификация пользователей по протоколу Kerberos V5. При отправке сообщения в KDC библиотека попытается использовать TCP перед UDP, если размер сообщения превышает udp\_preference\_limit из настроек krb5.conf. По умолчанию на клиентах значение равно нулю, поэтому все запросы идут через TCP. |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | MIT Kerberos (krb5kdc) | IP адрес контроллера домена | 464, 749 | TCP/UDP | KRB5 | доменный компьютер, контроллер домена | Задачи администрирования, например, создание UPN чрез kadmin, или смена пароля через kpasswd |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | Chrony (chronyd) | IP адрес контроллера домена | 123 | UDP | NTP | доменный компьютер, контроллер домена | Синхронизация системного времени на доменных компьютерах с временем на контроллерах домена |
| - | - | доменный компьютер | Chrony (chronyd) | 127.0.0.1 | 323 | UDP | - | доменный компьютер | Функция удаленного управления службой chronyd не требуется |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | 389 Directory Server (ns-slapd) | IP адрес контроллера домена | 389 | TCP | LDAP | доменный компьютер, контроллер домена | Взаимодействие с LDAP-каталогом. Например, служба sssd получает так информацию об участии пользователя в группах, HBAC и SUDO правила. Служба sssd не использует LDAPS, но траффик шифруется с помощью SSL, т. к. в начале обмена данными всегда посылается StartTLS. |
| контроллер домена | IP адрес контроллера домена | контроллер домена | 389 Directory Server (ns-slapd) | IP адрес контроллера домена | 389,636 | TCP | LDAP+StartTLS, LDAPS | контроллер домена | Репликация данных каталога между контроллерами домена. |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | 389 Directory Server (ns-slapd) | IP адрес контроллера домена | 636 | TCP | LDAPS | доменный компьютер, контроллер домена | Взаимодействие с LDAP-каталогом. Например, с помощью ldapsearch, ldapmodify и др. Утилиты из пакета OpenLDAP по умолчанию используют LDAPS. |
| контроллер домена | IP адрес контроллера домена | доменный компьютер | Flask (python3) | IP адрес из локальной сети | 30000 | TCP | HTTP | контроллер домена, доменный компьютер | Обращение к REST API для получения информации о запущенных сессиях удаленного рабочего стола для подключения ассистента. Адрес интерфейса /aldpro/remote-mgr/sessions, в ответ приходит JSON со списком сессий. На хостах серверной группировки порт рекомендуется блокировать и оставлять только на рабочих станциях пользователей. |
| контроллер домена | IP адрес контроллера домена | доменный компьютер | VNC (x11vnc) через Websockify (python3) | IP адрес из локальной сети | 6080-608N | TCP | HTTPS | контроллер домена, доменный компьютер | Удаленное управление рабочим столом по протоколу VNC. Подключение выполняется к Python приложению Websokify через SSL, которое пересылает данные на порт 5900-590N в x11vnc |
| - | - | доменный компьютер | VNC (x11vnc) | 127.0.0.1 | 5900-590N | TCP | VNC | доменный компьютер | Удаленное управление рабочим столом по протоколу VNC. Порт слушается только на localhost. |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | SaltStack (python3) | IP адрес контроллера домена | 4505/4506 | TCP | ZMTP | доменный компьютер, контроллер домена | Минион удерживает постоянное подключение к мастеру на порту 4505 для получения заданий по модели push/pull и подключаются к нему время от времени на порт 4506 для информирования о результатах выполнения назначенных заданий. Через этот механизм происходит развертывание и менеджмент всех подсистем, работа групповых политик и заданий автоматизации. |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | SaltStack (python3) | IP адрес контроллера домена | 4505/4506 | TCP | ZMTP | доменный компьютер, контроллер домена | Минион удерживает постоянное подключение к мастеру на порту 4505 для получения заданий по модели push/pull и подключаются к нему время от времени на порт 4506 для информирования о результатах выполнения назначенных заданий. Через этот механизм происходит развертывание и менеджмент всех подсистем, работа групповых политик и заданий автоматизации. |
| - | - | контроллер домена | SaltStack (python3) | IP адрес контроллера домена | 8000 | TCP | HTTP/HTTPS | контроллер домена | Начиная с версии 2.0.0, функции REST API системы конфигурирования SaltStack продуктом не используются. В предыдущих версиях продукта интерфейс использовался бэкендом для передачи команд по localhost, поэтому для любых редакций продукта указанный порт рекомендуется блокировать. |
| доменный компьютер | IP адрес из локальной сети | контроллер домена | Flask (python3) | IP адрес контроллера домена | 5001 | TCP | HTTP | доменный компьютер, контроллер домена | В рамках процедуры конфигурирования подсистемы с доменного компьютера происходит обращение к REST API для выпуска сертификата, который далее передается на хост через шифрованный канал SaltStack. |
| - | - | доменный компьютер | SSH (sshd) | IP адрес из локальной сети | 22 | TCP | SSH | доменный компьютер | Протокол SSH в работе системы не используется. |
| - | - | контроллер домена | PostgreSQL (postgres) | 127.0.0.1 | 5432 | TCP | PostgreSQL | контроллер домена | Функция удаленного доступа к СУБД PostgreSQL не требуется. Скрипты портала управления подключаются к СУБД только локально. Порт слушается только на localhost. |
| - | - | контроллер домена | Redis (redis-server 12) | 127.0.0.1 | 6379 | TCP | RESP | контроллер домена | Функция удаленного доступа Redis не требуется. Доступ к данным заданий Celery выполняется только локально. Порт слушается только на localhost. |
| - | - | доменный компьютер | CUPS (cupsd) | 127.0.0.1 | 631 | TCP | IPP | доменный компьютер | Сервер печати CUPS входит в стандартные дистрибутивы Astra Linux и автоматически устанавливается и запускается при инсталляции ОС. Порт слушается только на localhost. |
| - | - | доменный компьютер | Avahi (avahi-daemon) | IP адрес из локальной сети | 5353, 40000-59999 | UDP | mDNS | доменный компьютер | Функции преобразования имен хостов в IP-адреса через mDNS в доменной инфраструктуре не используются. |
| - | - | сервер общего доступа к файлам | Bind9 (named) | 127.0.0.1 | 53 | TCP/UDP | DNS | сервер общего доступа к файлам | Функции Samba по обработке DNS-запросов на сервере общего доступа к файлам не используются. |
| - | - | сервер общего доступа к файлам | Bind9 (named) | 127.0.0.1 | 953 | TCP | DDNS | сервер общего доступа к файлам | Функции Samba по обработке DNS-запросов на сервере общего доступа к файлам не используются. Порт слушается только на localhost. |
| - | - | сервер общего доступа к файлам | Samba (smbd) | IP адрес сервера общего доступа к файлам | 135 | TCP | RPC | сервер общего доступа к файлам | Функции EPMAP на сервере общего доступа к файлам не используются |
| - | - | сервер общего доступа к файлам | Samba (smbd) | IP адрес сервера общего доступа к файлам | 1024-1300 | TCP | RPC | сервер общего доступа к файлам | Функции EPMAP на сервере общего доступа к файлам не используются |
| доменный компьютер | IP адрес из локальной сети | сервер общего доступа к файлам | Samba NMB Daemon (nmbd) | IP адрес сервера общего доступа к файлам | 137 | UDP | NBNS | доменный компьютер, сервер общего доступа к файлам | Работа NetBIOS network browsing (nmbd). |
| доменный компьютер | IP адрес из локальной сети | сервер общего доступа к файлам | Samba NMB Daemon (nmbd) | IP адрес сервера общего доступа к файлам | 138 | UDP | NBNS | доменный компьютер, сервер общего доступа к файлам | Работа NetBIOS name service (nmbd). |
| доменный компьютер | IP адрес из локальной сети | сервер общего доступа к файлам | Samba NMB Daemon (nmbd) | IP адрес сервера общего доступа к файлам | 139 | TCP | NBT | доменный компьютер, сервер общего доступа к файлам | Общий доступ к файлам |
| доменный компьютер | IP адрес из локальной сети | сервер общего доступа к файлам | Samba NMB Daemon (nmbd) | IP адрес сервера общего доступа к файлам | 445 | TCP | SMB | доменный компьютер, сервер общего доступа к файлам | Общий доступ к файлам без NetBIOS |
| - | - | сервер общего доступа к файлам | Samba (smbd) | IP адрес сервера общего доступа к файлам | 80, 443 | TCP | HTTP, HTTPS | сервер общего доступа к файлам | Функции сервера Apache не используются, устанавливается как зависимость |
| доменный компьютер | 0.0.0.0 | сервер DHCP | DHCP (dhcpd) | 255.255.255.255 | 67 | UDP | DHCP | доменный компьютер, сервер DHCP | Клиенты отправляют серверу широковещательные запросы для получения сетевых настроек (discover, request) |
| сервер DHCP | IP адрес DHCP сервера | доменный компьютер | DHCP Client (dhclient) | 255.255.255.255, IP адрес доменного компьютера | 68 | UDP | DHCP | сервер DHCP, доменный компьютер | Сервер отправляет клиентам широковещательные ответы, Ack уходит на IP адрес хоста |
| компьютер локальной сети | IP адрес из локальной сети | сервер PXE | Dnsmasq (dnsmasq) | IP адрес сервера PXE | 69 | UDP | TFTP | компьютер локальной сети, сервер PXE | Клиенты скачивают загрузчик с сервера PXE |
| компьютер локальной сети | IP адрес из локальной сети | сервер PXE | vsFTP (vsftpd) | IP адрес сервера PXE | 21 | TCP | FTP | компьютер локальной сети, сервер PXE | Устанавливается, как зависимость |
| компьютер локальной сети | IP адрес из локальной сети | сервер PXE | Apache (apache2) | IP адрес сервера PXE | 80 | TCP | HTTP | компьютер локальной сети, сервер PXE | Клиенты получают установочные файлы с сервера PXE. Используется нешифрованный HTTP протокол |
| компьютер локальной сети | IP адрес из локальной сети | сервер PXE | Apache (apache2) | IP адрес сервера PXE | 443 | TCP | HTTPS | компьютер локальной сети, сервер PXE | Порт открывается Apache, но загрузка файлов с PXE сервера осуществляется по обычному HTTP |
| - | - | сервер PXE | Dnsmasq (dnsmasq) | IP адрес сервера PXE | 53 | TCP/UDP | DNS | сервер PXE | Функции Dnsmasq по обработке DNS-запросов на сервере PXE не используются. |
| - | - | сервер PXE | Redis (redis-server 12) | 127.0.0.1 | 6379 | TCP | RESP | сервер PXE | Функция удаленного доступа Redis не требуется. Порт слушается только на localhost. |
| - | - | сервер PXE | PostgreSQL (postgres) | 127.0.0.1 | 5432 | TCP | PostgreSQL | сервер PXE | Функция удаленного доступа к СУБД PostgreSQL не требуется. Скрипты подключается к СУБД только локально. Порт слушается только на localhost. |
| доменный компьютер | IP адрес из локальной сети | - | - | Любой IP адрес глобальной сети | 80, 443 | TCP | HTTP, HTTPS | доменный компьютер | Доступ к публичным репозиториям для загрузки пакетов по протоколам HTTP и HTTPS |
| доменный компьютер | IP адрес из локальной сети | сервер репозитория | Apache (apache2) | IP адрес сервера репозитория | 80, 443 | TCP | HTTP, HTTPS | доменный компьютер, сервер репозитория | Доступ к корпоративным репозиториям для загрузки пакетов по протоколам HTTP и HTTPS |
| сервер репозитория | IP адрес сервера репозитория | сервер репозитория | PostgreSQL (postgres) | IP адрес сервера репозитория | 5432 | TCP | PostgreSQL | сервер репозитория | Между серверами репозиториев происходит репликация СУБД средствами PostgreSQL. |
| - | - | сервер репозитория | Redis (redis-server 12) | 127.0.0.1 | 6379 | TCP | RESP | сервер репозитория | Функция удаленного доступа Redis не требуется. Порт слушается только на localhost. |
| контроллер домена | IP адрес контроллера домена | сервер печати | CUPS (cupsd) | IP адрес сервера печати | 631 | TCP | HTTP, HTTPS | контроллер домена, сервер печати | Администрирование CUPS через веб-интерфейс: управление принтерами, заданиями печати, драйверами и т. п. |
| доменный компьютер | IP адрес из локальной сети | сервер печати | CUPS (cupsd) | IP адрес сервера печати | 631 | TCP | HTTP, HTTPS | доменный компьютер, сервер печати | Самообслуживание пользователей через веб-интерфейс CUPS. При просмотре заданий доступен только их номер, название принтера и размер файла (название или содержимое недоступно ни пользователю, ни администратору). |
| доменный компьютер | IP адрес из локальной сети | сервер печати | CUPS (cupsd) | IP адрес сервера печати | 631 | TCP | IPP | доменный компьютер, сервер печати | Взаимодействие клиента с сервером для получения списка доступных принтеров, отправки заданий на печать, получение статуса заданий. |
| контроллер домена | IP адрес из локальной сети | сервер печати |  | IP адрес сервера печати | 80 | TCP | HTTP | контроллер домена, сервер печати | Обращение к REST API для загрузки драйверов \*.ppd в каталог /usr/share/cups/model/ На уровне сети доступ нужно разрешить только для контроллеров домена |
| сервер мониторинга | IP адрес сервера мониторинга | хост серверной группировки | Zabbix (zabbix\_agentd) | IP адрес серверной группировки | 10050 | TCP | Zabbix/JSON | сервер мониторинга, хост серверной группировки | Получение подсистемой мониторинга данных с хостов при пассивном режиме работы. Обращение происходит только к хостам серверной группировки. |
| хост серверной группировки | IP адрес серверной группировки | сервер мониторинга | Zabbix (zabbix\_server) | IP адрес сервера мониторинга | 10051 | TCP | Zabbix/JSON | хост серверной группировки, сервер мониторинга | Передача хостами данных в подсистему мониторинга в активном режиме работы. Обращение происходит только с хостов серверной группировки. |
| контроллер домена | IP адрес контроллера домена | сервер мониторинга | Apache (apache2) | IP адрес сервера мониторинга | 80, 443 | TCP | HTTP, HTTPS | контроллер домена, сервер мониторинга | Администрирование Zabbix через веб-портал и прямые запросы к REST API |
| - | - | сервер мониторинга | SNMP (snmpd) | IP адрес сервера мониторинга | 161 | UDP | SNMP | сервер мониторинга | Функция мониторинга через SNMP не используется. Порт слушается только на localhost. |
| доменный компьютер | IP адрес из локальной сети | сервер журналирования | Fluentd (ruby) | IP адрес сервера журналирования | 24222 | TCP/UDP | Fluent | доменный компьютер, сервер журналирования | Правило устарело, fluent заменен на syslog-ng  Агенты подключаются к серверу для передачи событий. |
| доменный компьютер | IP адрес из локальной сети | сервер журналирования | Syslog-NG (syslog-ng) | IP адрес сервера журналирования | 514 | TCP | Syslog-NG (syslog-ng) | доменный компьютер, сервер журналирования | Агенты подключаются к серверу для передачи событий. |
| доменный компьютер | IP адрес доменного компьютера | сервер мониторинга | Apache (apache2) | IP адрес сервера мониторинга | 3000 | TCP | HTTPS | доменный компьютер, сервер мониторинга | Просмотр панелей мониторинга Grafana из портала управления, прямой вход в веб-интрерфейс Grafana |
| контроллер домена | IP адрес доменного компьютера | контроллер домена | RabbitMQ | IP адрес контроллера домена | 4369 | TCP | AMQP | контроллер домена | Служба обнаружения одноранговых узлов, используемая узлами RabbitMQ и инструментами CLI |
| контроллер домена | IP адрес доменного компьютера | контроллер домена | RabbitMQ | IP адрес контроллера домена | 5672, 5671 | TCP | AMQP | контроллер домена | Клиенты AMQP 1.0 |
| контроллер домена | IP адрес доменного компьютера | контроллер домена | RabbitMQ | IP адрес контроллера домена | 5552, 5551 | TCP | AMQP | контроллер домена | Клиенты протокола RabbitMQ Stream |
| контроллер домена | IP адрес доменного компьютера | контроллер домена | RabbitMQ | IP адрес контроллера домена | 6000 | TCP | AMQP | контроллер домена | Потоковая репликация |
| контроллер домена | IP адрес доменного компьютера | контроллер домена | RabbitMQ | IP адрес контроллера домена | 25672 | TCP | AMQP | контроллер домена | Связь между узлами и инструментами CLI (порт сервера распространения Erlang), выделяется из динамического диапазона (по умолчанию ограничен одним портом, вычисляемым как порт AMQP + 20000). |
| контроллер домена | IP адрес доменного компьютера | контроллер домена | RabbitMQ | IP адрес контроллера домена | 35672-35682 | TCP | AMQP | контроллер домена | Инструменты CLI (клиентские порты распределения Erlang) для связи с узлами, выделяется из динамического диапазона (рассчитывается как порт распределения сервера + 10000 через порт распределения сервера + 10010). |
| контроллер домена | IP адрес доменного компьютера | контроллер домена | RabbitMQ | IP адрес контроллера домена | 15672, 15671 | TCP | AMQP | контроллер домена | Клиенты HTTP API, пользовательский интерфейс управления и Rabbitmqadmin (когда включен плагин управления) |

Приложение 2. Требования к сетевой связанности между сервисами

Таблица 5 Связанность между сервисами

| № п/п | Источник | Назначение | Порт, протокол | Регламент | Описание |
| --- | --- | --- | --- | --- | --- |
| 1 | Контроллер домена | Контроллер домена | TCP:53,80,88,135,139,389,  443,445,464,631,636,749,953,4505,4506,5001,  5432,6379, 8000,8008,9789,24224,  49152-65535.  UDP:53,88,123,323,464,631,15000. | Регулярно | Репликация данных службы каталогов. |
| 2 | Все в пределах сайта | Контроллер домена | TCP:53,80,88,135,139,389,  443,445,464,631,636,749,4505,4506,5001,  5432,6379,8000,8008,9789,24224,30000.  UDP:53,88,123,137,138,323,464,631. | Регулярно | Запрос к контроллерам домена и серверам DNS для аутентификации пользователя. Запрос на наличие изменение в описании конфигураций, чтение описания конфигураций. |
| 3 | Все в пределах сайта | Сервер мониторинга | TCP:80,443,3000,10050,10051. | Регулярно | Данные метрик мониторинга |
| 4 | Серверы репозиториев ПО | Серверы репозиториев ПО | TCP: 22, 5432 | Регулярно | Репликация репозиториев ПО |
| 5 | Все в пределах сайта | Серверы:  Установка ОС по сети Репозитории ПО | TCP:21,80,443,5432.  UDP:21,67,68,69 | По запросу | Запрос параметров установки ОС. Получение установочных пакетов. |
| 6 | Все в пределах сайта | Сервер аудита | TCP:80,443,5432,24224 | По запросу | Сбор логов в центральное хранилище. |
| 7 | Сервер мониторинга | Сервер аудита | TCP:22. | Регулярно | Сбор логов мониторинга в центральное хранилище |
| 8 | Контроллер домена | Подсистемы ALD Pro | TCP:22,8000,8008,10050,30000. | Регулярно | Обеспечение функционирования ALD Pro |
| 9 | Все в пределах сайта | Подсистема общих файлов | TCP:53,135,139,445,49152-65535 | Регулярно | Доступ к общим файлам; интеграция с AD |