ООО «Генезис АйТи»

СИСТЕМА УПРАВЛЕНИЯ СЛУЖБОЙ КАТАЛОГОВ DYNAMIC DIRECTORY

Версия 4.2

Описание программы

RU.69838320.02.06-07 31 01

Листов 18

2025

АННОТАЦИЯ

Описание программы является частью эксплуатационной документации на программное обеспечение системы управления службой каталогов Dynamic Directory (далее – Программа, Dynamic Directory).

Документ содержит описание общих сведений о Программе, функциональном назначении, описании логической структуры, используемых технических средствах, описании вызовов и загрузок, входных и выходных данных.

При разработке документа использованы ссылки на следующие стандарты:

– ГОСТ Р 2.105-2019 "Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам";

– ГОСТ 2.601 "Единая система программной документации. Виды программных документов";

– ГОСТ 19.101-77 "Единая система программной документации. Виды программ и программных документов";

– ГОСТ 19.105-78 "Единая система программной документации. Общие требования к программным документам";

– ГОСТ 19.402-78 "Единая система программной документации. Описание программы".

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Обозначение и наименование

Полное наименование Программы – Система управления службой каталогов Dynamic Directory (далее – Программа, Dynamic Directory).

Обозначение программного обеспечения – Dynamic Directory.

1.2 Программное обеспечение, необходимое для функционирования программы

Для функционирования Dynamic Directory необходимо предустановленное программное обеспечение, перечисленное в таблице 1.

Таблица 1 – ПО, необходимое для функционирования программы

Название программного обеспечения	Роль программного обеспечения	Место установки
Операционная система ROSA Enterprise Linux Server	Операционная система	Контроллеры домена, серверы управления.
Операционная система клиентских АРМ	Операционная система.	АРМ администратора Системы, АРМ администратора информационной безопасности, АРМ пользователя
Dynamic Directory (на базе FreeIPA)	Централизованная система по управлению идентификацией пользователей	Контроллеры домена
Служба управления конфигурациями ПК Puppet Server	Система централизованного управления конфигурацией ОС, программ и персональных компьютеров	Контроллеры домена/отдельный сервер
Набор манифестов для Puppet Server, включающий шлюзы ddpo_get и ddlap	Интерпретация групповых политик на клиентских АРМ.	Контроллеры домена/отдельный сервер. Манифесты распространяются на АРМ Системы через службу управления конфигурацией ПК
Клиент службы каталогов Dynamic Directory (dd-client)	Конфигурирование freeipa-client, sssd, puppet-agent.	Все АРМ, входящие в домен

Название программного обеспечения	Роль программного обеспечения	Место установки
puppet-agent, должен входить в состав ОС клиентских АРМ	Применение манифестов на клиентских АРМ, для реализации групповых политик.	Все АРМ, где требуется применение политик
freeipa-client, должен входить в состав ОС клиентских АРМ	Настройка конфигурации АРМ для работы в домене.	Все АРМ, входящие в домен
Программное обеспечение для управления службой каталогов Dynamic Directory (dd-admin)	ПО для управления службой каталогов	АРМ администратора Службы каталогов

1.3 Языки программирования

Для реализации функционала Программы используются следующие языки программирования:

– API Программы, интерфейс командной строки и визуальный графический интерфейс пользователя разрабатывается на высокоуровневом языке программирования общего назначения Python, ориентированном на повышение производительности разработчиков и улучшении читаемости кода.

– Описание политик в терминах создаваемой Программы или манифестов в терминах Puppet осуществляется на специальном декларативном предметно-ориентированном языке.

– Модуль связи системы оркестрации с базой LDAP службы каталогов FreeIPA разрабатывается на языке программирования Python.

2 ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1 Классы решаемых задач

Классы решаемых программой задач:

– Расширение функционала службы каталогов для возможности использования общих папок, общих принтеров, иерархической структуры организационных единиц.

– Реализация функционала групповых политик. Возможности создания, изменения, удаления, назначения подразделениям групповых политик. Определение статусов и значений параметров групповых политик.

– Предоставление удобного интерфейса командной строки и графического интерфейса пользователя.

– Возможность назначения и делегирования прав в иерархической структуре организационных единиц.

– Возможность сложения и применения результирующих групповых политик на АРМ пользователей.

2.2 Назначение Программы

2.2.1 Виды деятельности, для автоматизации которых предназначена Программа

Программа предназначена для управления записями службы каталогов, управления правами доступа к записям службы каталогов, реализации функционала управления групповыми политиками.

2.2.2 Перечень функций, реализуемых Программой

Программа реализует следующий набор функций:

– Управление записями службы каталогов:

- организационные единицы;
- учетные записи пользователей;
- учетные записи компьютеров;
- группы пользователей;
- группы компьютеров;
- общие папки;
- общие принтеры;
- права доступа к объектам службы каталогов;
- шаблоны параметров политик;

  - политики;
  - параметры политик;
  - зоны DNS;

- Управление групповыми политиками;
- Применение групповых политик на АРМ пользователей;
- Назначение прав доступа к записям службы каталогов;
- Аудит доступа;
- Автоматизация процессов экспорта и импорта данных.

2.2.3 Функциональные ограничения на применение Программы

Функциональные ограничения на применение Программы накладываются необходимостью наличия в ИТ-инфраструктуре поддерживаемых службы каталогов и системы оркестрации.

3 ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ ПРОГРАММЫ

3.1 Реализуемые алгоритмы

Программа обрабатывает данные, полученные из поддерживаемой службы каталогов.

Обработка осуществляется с учетом стандартов на используемые протоколы и настроек Программы.

По запросам администраторов осуществляется отображение и изменение данных, хранящихся в службе каталогов. Общий алгоритм работы Программы приведен на рисунке 1.

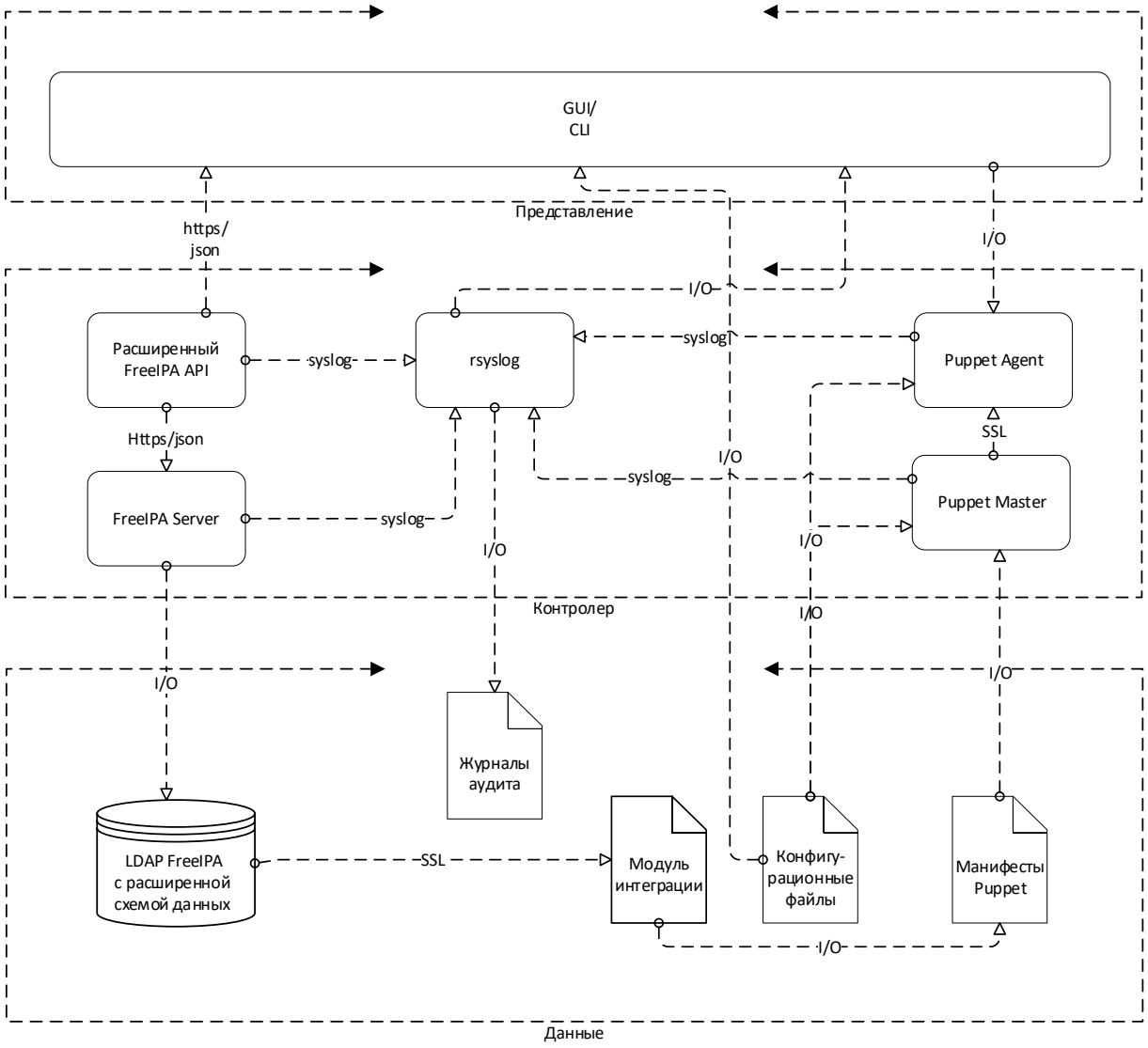

Рисунок 1 – Общий алгоритм работы Программы

В состав программы входят следующие модули:

– Пользовательский интерфейс:

– интерфейс командной строки;

– графический пользовательский интерфейс. Построен на отображении записей службы каталогов в иерархической структуре организационных единиц. Поддерживает диалоги по созданию, изменению, поиску и удалению записей службы каталогов, включая групповые политики. Назначение прав доступа реализовано в виде пошагового диалога. Определение статусов и значений групповых политик выполняется в отдельном окне, поддерживаются групповые политики для пользователей и компьютеров;

– Модуль управления записями службы каталогов. Предназначен для просмотра, создания, изменения, удаления, поиска объектов службы каталогов, а также для назначения/перемещения записей между организационными единицами и добавления/исключения из групп;

– Модуль управления групповыми политиками. Предназначен для просмотра, создания, изменения, удаления, поиска объектов службы каталогов, а также назначения групповых политик организационным подразделениям и группам;

– Модуль применения групповых политик. Предназначен для получения и сложения назначенных групповых политик, применения результирующих параметров политик на АРМ пользователей.

– Модуль управления правами администраторов. Предназначен для создания, изменения, удаления прав (ACL) для организационных единиц в их иерархии.

3.2 Используемые методы

На этапе инсталляции серверного компонента программы в соответствии с требованиями протокола LDAP v3:

– расширяется схема базы данных выбранной службы каталогов за счет добавления новых атрибутов и объектных классов, включая, но не ограничиваясь:

– атрибут ссылки на организационную единицу;

– расширенные атрибуты;

– классы общего принтера и общей папки;

– класс организационной единицы;

– класс групповой политики;

– класс параметра групповой политики;

– в выбранной службе каталогов формируются дополнительные контейнеры для дополнительных объектных классов;

– в выбранной службе каталогов формируются дополнительные права доступа к расширенной схеме базы данных;

– дополняются плагины выбранной службы каталогов для поддержки новых классов и атрибутов записей.

На этапе инсталляции клиентского компонента Программы:

– дополняются плагины клиентской части выбранной службы каталогов;

– устанавливается интеграционная часть Программы, позволяющая проводить сложение параметров групповых политик и предоставляющая выбранной системе оркестрации результирующие значения параметров групповых политик.

На этапе инсталляции административной части Программы на административные АРМ устанавливается визуальный интерфейс, дополнительные утилиты экспорта/импорта данных службы каталогов.

При работе Программы используются следующие методы:

– доступ к записям службы каталогов осуществляется по протоколам LDAP/LDAPS с использованием расширенного API выбранной службы каталогов;

– контроль доступа осуществляется с помощью списков контроля доступа (ACL);

– журналирование осуществляется по протоколу Syslog.

3.3 Структура Программы с описанием функций составных частей и связи между ними

3.3.1 Структура комплексов функций и назначение их частей

3.3.1.1 Перечень комплексов функций

Программа включает в себя следующие комплексы функций (далее – перспективы):

– Управление записями службы каталогов;

– Управление групповыми политиками;

– Применение групповых политик на АРМ пользователей;

– Управления доступом к записям службы каталогов.

Перспективы реализованы на единой технологической платформе (создание общего API) и обеспечивают унификацию реализации (функционал, внешний вид) комплексов.

Общая схема структуры перспектив приведена на рисунке 2.

Рисунок 2 – Общая структура перспектив Программы

3.3.1.2 Перспектива "Управление записями службы каталогов"

Перспектива предназначена для централизованного управления записями службы каталогов. Перспектива поддерживает иерархическую структуру представления ресурсов с упорядоченным по ряду признаков массивом информации о сетевых ресурсах (общие папки, серверы печати, принтеры, пользователи и т.д.), хранящимся в едином месте. Позволяет обеспечить централизованное управление как самими ресурсами, так и информацией о них.

3.3.1.3 Перспектива «Управление групповыми политиками»

Перспектива предназначена для создания и изменения наборов правил, которые будут применяться на АРМ пользователей домена. Для назначения правил и настроек ресурсам в домене перспектива интегрирована с комплексами "Управление записями службы каталогов" и "Управление правами доступа к записям службы каталогов" в части интерфейса взаимодействия с пользователем и с общим API для доступа к данным, хранящимся в службе каталогов.

Для штатного функционирования Программы в базу данных службы каталогов внесены изменения для возможности хранения контейнеров групповых политик.

3.3.1.4 Перспектива «Применение групповых политик на автоматизированном рабочем месте в домене»

Перспектива предназначена для безопасного получения данных о настройках групповых политик, хранящихся в службе каталогов, и их применения на конкретном АРМ.

Перспектива представляет собой интеграционный модуль, производящий сложение параметров политик и возврат результирующих параметров для выбранной системы оркестрации.

3.3.1.5 Перспектива "Управления доступом к записям службы каталогов"

Перспектива предназначена для контроля доступа к записям службы каталогов. Контроль доступа определяет: кто или что может получать доступ к конкретной записи службы каталогов, и какие именно операции разрешено или запрещено этому субъекту проводить над объектами.

Контроль доступа осуществляется над записями и атрибутами службы каталогов. Для назначения прав доступа к записям службы каталогов предусмотрена возможность выбора записей по DN и по фильтру, а также возможность делегирования полномочий для всех записей, принадлежащих подразделению. Когда объект службы каталогов назначается подразделению, происходит наследование прав, определенных для подразделения этому объекту. Уникальные права для объектов, назначенных подразделению, рекомендуется создавать, помещая объект в группу, для которой назначен набор прав, отличный от прав подразделения.

3.3.2 Описание взаимодействия Программы с другими системами

3.3.2.1 Перечень систем, с которыми связана Программа

Программа связана со следующим программным обеспечением:

– Служба каталогов – посредством протоколов LDAP/LDAPS;

– Система оркестрации – через интеграционный модуль;

– MS Active Directory – путем установления доверительных отношений, реализуемых штатными средствами службы каталогов.

3.3.2.2 Описание связей между системами

Все связи между системами осуществляются стандартными средствами этих систем. Взаимодействие между системами происходит следующим образом:

– с PAM LDAP – с помощью модуля libpam-ldap по протоколам LDAP/LDAPS;

– с конфигурациями программного обеспечения – через Puppet Agent;

– с другими службами LDAP – через протокол LDAP/LDAPS; настраивается штатными средствами службы каталогов.

3.3.2.3 Описание регламента связей

Особых регламентов связи между системами не используется.

4 ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

В качестве технических средств для работы Программы выступают:

– Контролер домена с техническими характеристиками, соответствующими требованиям, накладываемым используемыми компонентами службы каталогов и системы оркестрации;

– Реплика контроллера домена с характеристиками, соответствующими требованиям, накладываемым используемыми компонентами и службы каталогов и системы оркестрации;

– Рабочая станция администратора домена с техническими характеристиками: процессор x86-64, объем оперативной памяти не менее 4 ГБ, объем жесткого диска не менее 10 ГБ, разрешение монитора не менее 1024x786, клавиатура, манипулятор «мышь»;

– АРМ в домене с техническими характеристиками, достаточными для запуска и выполнения клиентских частей выбранной службы каталогов и системы оркестрации.

5 ОСОБЕННОСТИ РАБОТЫ С ПРОГРАММОЙ

5.1 Вызов и загрузка

5.1.1 Способы вызова Программы

Существует два способа вызова интерфейса Программы:

– через графический интерфейс пользователя запуском файла dynamicDirectory.py;

– через интерфейс командной строки с помощью конструкции вида:

```
# ipa <команда> <аргументы> <параметры>.
```

5.1.2 Входные точки Программы

Входными точками Программы является выполнение команд посредством графического интерфейса пользователя и команды, вводимые из интерфейса командной строки.

5.2 Входные и выходные данные

5.2.1 Входные данные

5.2.1.1 Характер, организация и предварительная подготовка данных

Программа использует несколько типов входных данных:

– Данные конфигурационных файлов Программы. При этом используются стандартные файлы конфигурации службы каталогов, системы оркестрации и графического интерфейса пользователя.

– Данные, вводимые администратором вручную. Данные могут вноситься через графический интерфейс пользователя или через интерфейс командной строки. Вводимые данные должны соответствовать требованиям:

– к данным служб каталогов;

– к параметрам групповых политик, хранящихся в базе данных LDAP службы каталогов;

– к синтаксисам системы оркестрации;

– Данные файлов журналов (log-файлов) – являются входными данными для служб журналирования.

5.2.1.2 Формат, описание и способ кодирования входных данных

Данные конфигурационных файлов, файлов журналов событий Программы формируются средствами Программы в кодировке UTF-8. Конфигурационные файлы, файлы журналов событий Программы формируются в текстовом виде.

Дополнительные требования к кодированию вводимых вручную данных не накладываются.

5.2.2 Выходные данные

5.2.2.1 Характер и организация выходных данных

Все выходные данные формируются Программой в автоматизированном режиме. Выходными данными являются данные, отображаемые по запросам администратора в интерфейсах Программы, формируемые Программой информационные сообщения для администраторов в графическом интерфейсе и интерфейсе командной строки, файлы журналов событий Программы и отчеты по журналам событий, формирующиеся Программой по запросам администратора.

5.2.2.2 Формат, описание и способ кодирования выходных данных

Журналы для компонентов, используемых Программой, формируются штатными способами. Способы аудита описаны в официальной документации на соответствующие компоненты.

Файлы журналов хранятся в кодировке UTF-8.

Специальных требований к способам кодирования выходных данных не предъявляется.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Dynamic Directory	–	Система управления службой каталогов
АРМ	–	Автоматизированное рабочее место
Веб-сервис (англ. web service)	–	Программная система, чьи общедоступные интерфейсы определены на языке XML. Описание этой программной системы может быть найдено другими программными системами, которые могут взаимодействовать с ней согласно этому описанию посредством сообщений, основанных на XML, и передаваемых с помощью интернет-протоколов
ОП	–	Организационные подразделение
ОС	–	Операционная система
ПО	–	Программное обеспечение
ПК	–	Персональный компьютер
СК	–	Служба каталогов
СПД	–	Сеть передачи данных
ЦОД	–	Центр обработки данных
AD	–	Active Directory, служба каталогов корпорации Microsoft для операционных систем семейства Windows Server