ФАСТ ЛЕЙН
УЧЕБНЫЙ ЦЕНТР

Длительность: 5 дней

Установка, настройка и использование ПК ALD Pro 3.0.0 (AP-301)

Аудитория

- Системные администраторы Linux и Astra Linux
- Администраторы доменной инфраструктуры и служб каталогов
- Специалисты, отвечающие за внедрение и сопровождение ALD Pro
- Инженеры по миграции с Microsoft Active Directory на ALD Pro
- Специалисты по информационной безопасности и управлению доступом
- Инженеры технической поддержки и эксплуатации ИТ-инфраструктуры
- Архитекторы и специалисты по проектированию централизованной инфраструктуры управления

Требования

- **Базовые навыки работы с Linux**: работа в терминале, навигация по файловой системе, файловые операции, права доступа; знание основных команд командной строки (CLI); опыт редактирования файлов в консольных редакторах (nano, vim или аналоги); понимание организации процессов в Linux.
- **Навыки администрирования:** владение основами администрирования учетных записей пользователей и разграничения прав доступа; понимание базовых инструментов безопасности ОС Astra Linux; понимание принципов работы служб каталога (Active Directory, FreeIPA или аналоги): аутентификация, авторизация, учетные записи, группы, организационные единицы.
- **Сетевые знания и навыки:** понимание сетевых основ: IP-адресация, маски подсетей, маршрутизация, DNS; базовые навыки настройки сетевых интерфейсов.

Цели

Уметь:

- объяснять архитектуру ALD Pro, назначение контроллеров домена, FreeIPA, 389 Directory Server, MIT Kerberos, Samba, портала управления и дополнительных подсистем,
- планировать и выполнять развертывание ALD Pro: подготавливать виртуальную среду, устанавливать операционную систему, настраивать сеть, репозитории, DNS и первый контроллер домена,
- проверять работоспособность доменных служб, Kerberos-аутентификации и портала управления, присоединять Linux- и Windows-компьютеры к домену,
- управлять пользователями, компьютерами, группами и организационной структурой через портал ALD Pro, веб-интерфейс FreeIPA и консольные утилиты,
- администрировать службу каталога: создавать, изменять, удалять и искать объекты, управлять диапазонами идентификаторов, выполнять резервное копирование и восстановление данных,
- настраивать SSSD, LDAP, Kerberos и NTLM, защищать соединения с помощью StartTLS и LDAPS, управлять Kerberos-билетами и обеспечивать автономную работу доменных компьютеров,
- диагностировать проблемы аутентификации, смены паролей и контроля доступа с помощью журналов SSSD и других средств отладки,
- настраивать DNS-зоны и записи, динамическое обновление DNS, службу синхронизации времени chrony и автоматическое обнаружение доменных сервисов,
- создавать и применять групповые политики, политики паролей, HBAC- и SUDO-правила, учитывать наследование и репликацию параметров,
- настраивать LAPS и разрабатывать дополнительные параметры групповых политик с использованием Salt и Jinja с учетом идемпотентности и производительности,
- развертывать и администрировать подсистему общего доступа к файлам, настраивать Samba, Kerberos- и NTLM-аутентификацию, права доступа и модели ACL XATTR и NFS4ACLs,
- проектировать и настраивать топологию домена, добавлять контроллеры, управлять репликацией, анализировать конфликты и выполнять повторную инициализацию серверов,
- контролировать и диагностировать репликацию с помощью dsconf, ds replcheck, checkipaconsistency, журналов изменений и средств мониторинга,
- планировать миграцию и гибридное развертывание с Microsoft Active Directory, выбирать подходящий сценарий интеграции и настраивать доверительные отношения между доменами,
- настраивать взаимное перенаправление DNS-зон, глобальный каталог ALD Pro, службу samba dcerpcd и проверять работоспособность трастов и механизмов синхронизации,

- организовывать резервное копирование контроллеров домена и дополнительных подсистем, выбирать способ резервирования дисков и данных, настраивать регулярное выполнение заданий через CRON,
- развертывать и администрировать репозитории программного обеспечения, создавать их из ISO-образов, обновлять версии и управлять установкой ПО через групповые политики,
- настраивать службы печати, мониторинга, аудита и журналирования, а также интегрировать ALD Pro с внешними приложениями,
- развертывать и настраивать DHCP- и PXE-серверы, подготавливать файловую структуру и загрузочное меню, адаптировать GRUB для BIOS и UEFI,
- автоматизировать сетевую установку операционных систем с помощью Preseed, Postinstall и Firstinstall и управлять загрузкой различных дистрибутивов Linux,
- настраивать мандатное разграничение доступа и контроль целостности, назначать уровни и категории конфиденциальности, мандатные атрибуты и ограничения для пользователей, процессов и объектов,
- создавать защищенные каталоги и файловые ресурсы, ограничивать подключение внешних носителей, регистрировать устройства и управлять засекречиванием и рассекречиванием документов.

Программа

Модуль 1. Введение в ALD Pro и планирование развертывания

Система ALD Pro: общее представление:
назначение и ключевые функции
возможности службы каталога
Архитектура и компоненты ALD Pro:
контроллер домена
служба синхронизации времени (chrony)
портал управления
подсистемы:
репозиторий программного обеспечения
общий доступ к файлам
служба печати
динамическая настройка узлов (DHCP)
установка ОС по сети (PXE)
мониторинг
аудит
клиентская часть
Сравнение механизмов каталогов FreeIPA и Samba AD:
особенности реализации Samba AD
преимущества FreeIPA и обоснование ее выбора в ALD Pro
Практическое сопоставление MS AD и ALD Pro

Подготовка к развертыванию:
минимальные требования к инфраструктуре
планирование ресурсов (оперативная память, CPU, пропускная способность сети)
модуль синхронизации и прочие службы
Масштабирование и организация инфраструктуры:
методики горизонтального масштабирования
рекомендации по именованию доменов

Модуль 2. Развертывание первого контроллера домена

Подготовка инфраструктуры: требования к тестовой среде, создание и настройка виртуальной машины:
проверка ОС: build_version
проверка (установка) уровня «Смоленск»
отключение NetworkManager
настройка статического IP в /etc/network/interfaces
Развертывание контроллера домена:
настройка репозиториев ALD Pro: создание /etc/apt/sources.list.d/aldpro.list
присвоение имени контроллера
установка пакетов: aldpro-mp, aldpro-gc, aldpro-syncer, aldpro-syncer-pwdsync
повышение роли сервера до контроллера домена
проверка базовых функций: доменных служб, Kerberos-аутентификации, портала управления
ввод компьютера в домен
Практическая работа: развертывание первого контроллера домена

Модуль 3. Архитектура службы каталога ALD Pro

Архитектура службы каталога ALD Pro:
обзор компонентов и их взаимодействия
сравнительный анализ с MS AD: служба каталога — FreeIPA, LDAP — 389 Directory Server, Kerberos — MIT Kerberos
Сервер FreeIPA:
веб-интерфейс управления
утилиты управления: ipactl, ipa, ipa-getkeytab, ipa-backup, ipa-restore
конфигурационные файлы: /etc/ipa/default.conf, /etc/krb5.conf
Сервер LDAP 389 Directory Server:
структура каталога
утилиты: ldapsearch, ldapmodify, dsctl, dsconf
расположение БД
Сервер MIT Kerberos:
служба KDC: krb5-kdc
утилиты: kinit, klist, kdestroy
файлы ключей: /etc/krb5.keytab
Сервер Samba:
интеграция с Windows
службы: smb, winbind

конфигурация: /etc/samba/smb.conf
Идентификаторы безопасности:
диапазоны UID/GID: ipa config-show
SID (Security Identifier)
Управление объектами службы каталога:
управление организационной структурой
управление пользователями
управление компьютерами
удаленный доступ для оказания поддержки
управление группами
Практическая работа: администрирование службы каталога с помощью утилит командной строки FreeIPA и LDAP

Модуль 4. Настройка базовых служб

Назначение базовых служб в домене ALD Pro:
DNS: разрешение имен, SRV-записи для автоматического обнаружения служб
синхронизация времени (NTP): критична для работы Kerberos
сравнительный анализ с MS AD: DNS Manager — BIND в ALD Pro, W32Time — chrony
DNS-служба в ALD Pro:
использование BIND 9 (bind9-pkcs11)
конфигурационные файлы:
/etc/bind/named.conf (основной конфиг)
/etc/bind/ipa-options-ext.conf (дополнительные настройки)
/etc/bind/ipa-ext.conf (зоны)
автоматическое создание зон при установке домена
отключение DNSSEC для работы в закрытом контуре
настройка рекурсивных запросов
Синхронизация времени:
служба chrony (альтернатива ntpd)
конфигурационный файл: /etc/chrony/chrony.conf
синхронизация сервера времени контроллера домена с внешними источниками
синхронизация клиентов с контроллерами домена
Практическая работа: настройка DNS и NTP, проверка SRV-записей

Модуль 5. Работа Linux-компьютера в домене

Архитектура клиентской части ALD Pro:
основные клиентские пакеты: aldpro-client, freeipa-client, sssd, krb5-user
сравнение с Windows: присоединение к домену Windows — ввод в домен ALD Pro
Служба SSSD (System Security Services Daemon):
архитектура: монитор, бэкенды, ответчики
механизм кеширования: автономная работа
конфигурационные файлы: /etc/sssd/sssd.conf, /etc/sssd/conf.d/
Способы аутентификации в домене:
LDAP: ldap:// или ldaps://
Kerberos: билеты TGT и сервисные билеты

NTLM: для совместимости с Windows
Безопасный обмен данными:
SSL/TLS для LDAP (LDAPS)
StartTLS для защиты LDAP-сессий
сертификаты домена: /etc/ipa/ca.crt
Учетная запись компьютера в домене:
автоматическое создание при вводе в домен
пароль компьютера: /etc/krb5.keytab
проверка: klist -k
Работа в автономном режиме:
кеширование учетных данных
ограниченная функциональность
автоматическая синхронизация при подключении
Практическая работа: ввод компьютера в домен, диагностика аутентификации

Модуль 6. Управление политиками ALD Pro

Концепция управления политиками в ALD Pro:
централизованное управление настройками пользователей и компьютеров
Сравнение с MS AD:
Group Policy Objects (GPO) — групповые политики ALD Pro
иерархия применения: домен — сайт — подразделение — группа — пользователь/компьютер
Типы политик в ALD Pro:
политики паролей (аналог Windows Password Policy)
HBAC-правила (Host-Based Access Control)
SUDO-правила (повышение привилегий)
групповые политики (настройки ОС и приложений)
политики ПО (установка и управление программным обеспечением)
LAPS (Local Administrator Password Solution)
Политики паролей FreeIPA:
настройки сложности, истории, срока действия
группы с автоматическим участием (встроенные группы)
HBAC-правила (доступ к узлам):
контроль доступа пользователей к хостам и сервисам
компоненты правила: кто (пользователь/группа) — куда (хост/группа хостов) — к чему (сервис), по умолчанию правило allow_all
SUDO-правила:
делегирование прав выполнения команд
аналогия с /etc/sudoers, но централизованно
поддержка групп пользователей, хостов, команд
Групповые политики ALD Pro:
настройка через портал управления
категории: параметры компьютеров, параметры пользователей
дополнительные параметры (кастомизация через Salt-скрипты)
Практическая работа: создание и применение политик безопасности

Модуль 7. Дополнительные подсистемы: общий доступ к файлам

Процедура развертывания подсистем:
установка ролей в Windows Server
установка подсистем в ALD Pro
Универсальный двухэтапный процесс для всех подсистем:
ввод сервера в домен как обычной рабочей станции с помощью aldpro-client-installer
назначение серверу роли через портал управления (раздел «Роли и службы сайта»)
автоматическая установка и настройка подсистемы (через ~30 минут)
форсирование установки: sudo aldpro-roles --iud на целевом хосте
Архитектура подсистемы в ALD Pro: Samba-сервер, интеграция с доменной аутентификацией
Аутентификация: Kerberos vs NTLM в контексте ALD Pro
Управление доступом: портал vs файловая система, модели безопасности Samba (стандартная, ACL XATTR, NFS4 ACLs)
Интеграция с Windows-клиентами
Практическая работа: развертывание файлового сервера, настройка общих ресурсов

Модуль 8. Управление топологией в домене

Архитектура топологии домена ALD Pro:
мультимастерная репликация (все контроллеры равноправны)
Сравнение с MS AD: AD Sites and Services — сайты в ALD Pro
Механизмы репликации:
репликация изменений (incremental replication)
полная репликация при инициализации
конфликты репликации и их разрешение
журнал изменений (change log)
Сайты (Sites):
группировка контроллеров по физическому местоположению
балансировка нагрузки и отказоустойчивость
DNS SRV-записи для автоматического обнаружения сайта
Автоматическое обнаружение сервисов:
через DNS SRV-записи
в SSSD-клиентах
в библиотеке libkrb5
Диагностика репликации
Практическая работа: создание сайта, настройка репликации, диагностика

Модуль 9. Миграция и гибридное развертывание с MS AD

Стратегии миграции с Active Directory: доверительные отношения (Trusts), глобальный каталог, модуль синхронизации
Сравнение с Windows: Forest Trust/External Trust — Trust в ALD Pro
Типы доверительных отношений: Forest Trust (между лесами AD и FreeIPA), External Trust (между отдельными доменами), односторонние/двусторонние

Компоненты интеграции: Samba DCERPC (для работы трастов), Global Catalog (для поиска в доверенных доменах), SSSD с поддержкой нескольких доменов
Модуль синхронизации (aldpro-syncer): установка только на первый контроллер, синхронизация пользователей, групп и паролей, ключ --setup_syncer при установке
Настройка доверительных отношений: подготовка DNS, проверка времени, создание траста через портал
Настройка глобального каталога: установка пакета aldpro-gc, назначение роли через портал
Присоединение Windows-машин к домену ALD Pro (утилита aldpro join.exe)
Практическая работа: настройка доверительных отношений с тестовым AD

Модуль 10. Резервное копирование и восстановление ALD Pro

Стратегия резервного копирования в ALD Pro: полные бэкапы, инкрементальные, резервное копирование дисков, резервное копирование данных
Критически важные данные: контроллеры домена (LDAP-база, Kerberos-база, сертификаты), подсистемы (конфигурации служб, данные приложений), журналы (аудит, мониторинг, логи безопасности)
Инструменты резервного копирования: ipa-backup — для данных FreeIPA; tar, CRON — автоматизация регулярных бэкапов
Практическая работа: создание и проверка резервных копий

Модуль 11. Дополнительные подсистемы: репозитории, печать, мониторинг

Архитектура дополнительных подсистем: репозитории ПО (централизованное хранение пакетов), служба печати (CUPS), мониторинг (Zabbix), аудит (Syslog-NG)
Принципы работы: роли серверов, автоматизация установки через aldpro-roles --iud, управление через портал, интеграция с доменом
Единый процесс развертывания (как в модуле 7):
подготовка сервера (ОС, сеть, имя)
ввод в домен как клиента
назначение роли через портал управления
автоматическая установка (~30 минут)
Подсистема «Репозитории ПО»: создание репозитория из ISO-образа, управление версиями
Подсистема «Печать»: добавление сетевых и локальных принтеров, управление очередями
Подсистема «Мониторинг»: установка Zabbix-сервера, базовые шаблоны мониторинга
Подсистема «Аудит»: настройка централизованного сбора логов через Syslog-NG
Практическая работа: развертывание подсистемы на выбор

Модуль 12. Подсистемы DHCP и PXE

Архитектура сетевых служб:
DHCP (Dynamic Host Configuration Protocol): автоматическая выдача сетевых настроек
PXE (Preboot Execution Environment): сетевая загрузка и установка ОС
Интеграция с доменом:

привязка к домену (автоматический ввод в домен при установке)
Компоненты PXE-сервера:
TFTP-сервер: передача файлов загрузки
HTTP-сервер: предоставление установочных образов
конфигурационные файлы: меню загрузки, параметры установки
Preseed/Postinstall-скрипты: автоматизация установки
Сценарии использования:
массовая установка ОС на новые компьютеры
развертывание однотипных конфигураций
централизованное управление загрузкой
Практическая работа: настройка DHCP и PXE для автоматической установки

Модуль 13. Мандатное управление доступом и контроль целостности

Модели безопасности в ALD Pro: МРД (мандатное управление доступом), МКЦ (мандатный контроль целостности), дискреционное управление доступом
Принципы работы: уровни конфиденциальности (иерархические 0–255), категории конфиденциальности (битовая маска), контейнеры объектов (файлы, процессы, сокеты)
Интеграция с доменом: хранение мандатных атрибутов в LDAP, применение политик через PAM и ядро ОС, централизованное управление через портал FreeIPA
Настройка мандатных атрибутов пользователей через портал управления
Создание защищенной структуры каталогов с учетом мандатных меток
Работа с внешними носителями: перенос мандатных меток
Интеграция с файловым сервером Samba: настройка мандатного доступа к общим ресурсам
Практическая работа: настройка МРД для пользователей и каталогов

Модуль 14. Диагностика и мониторинг ALD Pro

Методики поиска проблем: системный подход к диагностике
Комплексный чек-лист диагностики:
проверка служб: aldproctl, krb5-kdc dirsrv@... bind9-pkcs11 sssd
диагностика аутентификации: логи SSSD (/var/log/sssd/), kinit admin, sssctl user-checks
проверка репликации: dsconf ldap://dc-1 repl-agmt list, ds-replcheck, checkipaconsistency (см. модуль 8)
проверка DNS: nslookup dc-1, dig -t SRV _ldap._tcp.ald.company.lan
сеть: доступность портов (nc -zv dc-1 389 636 88 53)
Типовые ошибки и их решения: проблемы с аутентификацией, репликацией, DNS
Ключевые утилиты диагностики:
sssctl — диагностика SSSD (см. модуль 5)
dsconf, ipa-replica-manage — диагностика репликации
checkipaconsistency — проверка целостности данных
aldproctl — управление службами ALD Pro
Инструменты мониторинга: Zabbix (метрики, триггеры, уведомления), системные метрики
Сравнение с Windows: Event Viewer — логи ALD Pro + Zabbix

Практическая работа: диагностика искусственно созданных проблем в тестовой среде

Модуль 15. Итоговое тестирование

Практическая работа: 90 мин.