

# Настройка доменного контроллера Samba

Владимир Базлов

## Начало выступления

Добрый день, уважаемые слушатели!

Сегодня мы поговорим о мощном инструменте для интеграции разнородных ИТ-сред – доменном контроллере на базе Samba. В мире, где часто существуют операционные системы Windows и Linux, необходимость в их бесшовном взаимодействии становится критически важной. И именно Samba выступает в роли такого «переводчика» и «организатора».

### Слайд 2: Что такое Samba AD?

#### 1. Что такое Samba и зачем ему быть доменным контроллером?

- Samba — это набор открытых программ, которые позволяют компьютерам под управлением Linux и Unix «говорить» на сетевом протоколе Microsoft SMB/CIFS.
- Роль доменного контроллера (Domain Controller, DC) — сложная и мощная функция Samba, позволяющая Linux-серверу управлять доменом Windows.
- Домен Windows — логическая группа компьютеров с централизованной базой данных для управления учетными записями и политиками безопасности.
- Samba 4 — реализует полный функционал контроллера домена, совместимого с Windows Server, начиная с версии 2008 R2.

### Слайд 3: Зачем это нужно? Цели внедрения

#### 2. Какие задачи решает доменный контроллер Samba?

- Централизованное управление учетными записями — единый логин и пароль для всех компьютеров домена.
- Единая политика безопасности — применение групповых политик (GPO) для настроек и параметров безопасности и рабочей среды.
- Упрощенный доступ к ресурсам — авторизация через контроллер для доступа к файлам и принтерам.
- Снижение затрат — функционал корпоративного уровня без лицензий Windows Server.
- Интеграция разнородных систем — объединение Linux-серверов и Windows-клиентов в единое пространство.

### Слайд 4: Ключевые концепции и компоненты

#### 3. Основные теоретические концепции

- Active Directory (AD) — реализация служб каталогов Microsoft. Samba 4 — совместимая реализация AD.

- LDAP (Lightweight Directory Access Protocol) — открытый протокол для доступа к службам каталогов. Samba использует LDAP для хранения данных домена.
- Kerberos — протокол аутентификации, основа безопасности в AD. Обеспечивает надежную проверку подлинности.
- DNS (Domain Name System) — критически важный компонент. DNS-сервер интегрирован с AD для поиска контроллера домена в сети.

## Слайд 5: Этапы настройки (теоретический взгляд)

### 4. Теоретические этапы настройки

#### 1. Подготовка инфраструктуры

- Статический IP-адрес и FQDN (например, `dc1.company.local`).

#### 2. Установка и настройка зависимостей

- DNS-сервер (BIND9) в режиме интеграции с Samba AD.

#### 3. Установка Samba

- Пакеты Samba 4.x и выше с компонентами для доменного контроллера.

#### 4. Настройка Kerberos

- Базовая настройка клиента Kerberos для работы с доменом.

#### 5. Provisioning (инициализация домена)

- Создание структуры базы данных LDAP.
- Генерация схем Active Directory.
- Настройка интеграции с DNS и Kerberos.
- Создание учетной записи администратора.

## Слайд 6: Безопасность и управление

### 5. Безопасность и управление

- Инструменты управления — RSAT (Remote Server Administration Tools) для удаленного управления пользователями, группами и политиками.
- Безопасность — аутентификация Kerberos, шифрование трафика, централизованные политики паролей через GPO.

## Слайд 7: Заключение

### Заключение

Samba — полноценное, надежное и экономически эффективное решение для корпоративной сети.

Преимущества:

- Стабильность и открытость Linux-платформы.
- Привычный инструментарий управления доменом Windows.
- Гибкость, контроль и снижение затрат на IT-инфраструктуру.

Спасибо за внимание! Готов ответить на ваши вопросы.