# ВОЗМОЖНОСТЬ УДАЛЕННОГО УПРАВЛЕНИЯ ПО НА КЛИЕНТАХ

Чинкова Полина Геннадьевна, студентка 3-го курса РГУ нефти и газа (НИУ) имени И.М. Губкина

Лужнов Александр Олегович, студент 3-го курса РГУ нефти и газа (НИУ) имени И.М. Губкина

***Аннотация***

***В данной статье рассмотрен способ удаленного управления на клиентах с помощью Samba AD DC на операционной системе Linux, приведена методика настройки контроллера домена на базе Samba, изучены различные виды групповых политик с применением их на практике.***

# Введение

В современном мире информационных технологий удаленное управление становится все более актуальной и важной темой для предприятий и организаций.

Удаленное управление программным обеспечением позволяет компаниям обеспечить доступ к необходимым программам и ресурсам для удаленных сотрудников, обеспечивая таким образом непрерывную работу и высокую производительность даже при отсутствии физического присутствия в офисе, а также обеспечивать необходимую безопасность информационно й системы.

Одним из ключевых аспектов удаленного управления программным обеспечением является выбор правильных инструментов и технологий, которые позволят обеспечить быстрый и надежный доступ к необходимым инструментам. В данной статье мы рассмотрим основные принципы удаленного управления с помощью Samba AD.

# Удаленное управление с помощью samba ad

Удаленное управление на клиентах с помощью Samba AD является одним из ключевых способов управления IT-системами.

Samba Active Directory (Samba AD) - это программное обеспечение с открытым исходным кодом, представляющее собой реализацию служб доменной директории, совместимых с протоколами Microsoft Active Directory. Данное програмное обеспечение обладает множеством функциональных возможностей, которые позволяют предоставлять полный интегрированный набор инструментов для управления сетью.

Так, Samba AD позволяет создавать и управлять доменными средами, включающими контроллеры домена, пользователей, группы, политики безопасности, а также обеспечивает централизованное управление ресурсами на сервере систем Linux, Unix и других UNIX-подобных операционных системах.

Одной из основных задач удаленного управления на клиентах с помощью Samba AD является обеспечение безопасности данных и сетей организации. Централизованное управление пользователями и группами позволяет администраторам быстро и эффективно назначать права доступа к файлам и папкам, устанавливать политики безопасности и мониторить активность пользователей.

Для того, чтобы samba функционировал в качестве AD DC, понадобиться установить пакеты, представленные в таблице 1:

|  |  |  |
| --- | --- | --- |
| Название пакета | Версия пакета | Описание пакета |
| Winbind | 2:4.17.12 | Предоставляет службы для интеграции с Windows AD |
| libpam-winbind | 2:4.17.12 | Обеспечивает модуль для PAM (Pluggable Authentication Modules) для аутентификации пользователей с помощью AD |
| libnss-winbind | 2:4.17.12 | Предоставляет службы NSS (Name Service Switch) для разрешения имен пользователей и групп из AD |
| bind9 | 1:9.18.24 | Обеспечивает DNS-сервер (Domain Name System) |
| libpam-krb5 | 4.11-1+b1 | Обеспечивает модуль для PAM для аутентификации пользователей с помощью Kerberos |
| krb5-config | 2.7 | Обеспечивает конфигурацию Kerberos |
| krb5-user |  1.20.1 | Предоставляет инструменты для управления учетными записями пользователей в Kerberos |

Таблица 1 Перечень и описание необходимых пакетов

# Назначение samba ad на роль ad dc

Реализация назначения samba на роль AD DC происходит посредством следующей команды:

samba-tool domain provision [options]

В результате выполнения которой был развернут домен со следующими параметрами:

1. --use-rfc2307 - флаг, который указывает, что Samba будет использовать RFC 2307 для аутентификации с Active Directory
2. --realm=SAMBADC.AU.TEAM - домен DNS Active Directory
3. --domain=SAMBADC - имя домена
4. ---server-role=dc - роль Samba-сервера
5. --dns-backend=BIND9\_DLZ- способ взаимодействия Samba с DNS
6. --adminpass=somepass - пароль администратора Active Directory

Пример выполнения команды:

sudo samba-tool domain provision --server-role=dc --use-rfc2307 --dns-backend=BIND9\_DLZ --realm=SAMBADC.AU.TEAM --domain=SAMBADC --adminpass=somepass

# Групповые политики и их виды

Далее перейдем к разбору групповых политик.

Групповые политики (Group Policy) представляют собой мощный инструмент, используемый в среде Active Directory (AD) для централизованного управления настройками и конфигурациями компьютеров и пользователей в сети. В общем смысле групповые политики можно разделить на два направления: групповые политики для компьютеров и групповые политики для пользователей.

Групповые политики компьютеров подразумевают настройку отдельных узлов в сети, его программного обеспечения и операционной системы. В то время как групповые политики пользователей влияют на настройки пользователя, его доступ к ресурсам и его взаимодействие с системой

Однако, технически групповые политики можно классифицировать следующим образом:

1. политики, применяемые при входе пользователя – в Plugable Authentification Modules (PAM) на этапе аутентификации (PAM auth), смены пароля (PAM password), создания сессии (PAM session) и назначении групп (NSS initgroups);
2. пользовательские политики, требующие административных привилегий (подключение сетевых каталогов, настройка сервера печати CUPS и любых других локальных сервисов);
3. политики, требующие контекст графической сессии, выполняемые с пользовательскими привилегиями (настройка фона рабочего стола, дополнительные ярлыки на рабочем столе и т.п.).

Для непосредственного применения групповых политик, на контроллер домена необходимо заблаговременно установить административные шаблоны.

Административные шаблоны представляют собой механизм, который позволяет администраторам управлять настройками пользователей и компьютеров в домене. В шаблонах описываются изменения, которые требуется выполнить для применения настроек, предусмотренных определенной групповой политикой.

Сам административный шаблон состоит из двух файлов формата XML - admx и adml файлов. Admx файл представляет собой сам шаблон, так называемую инструкцию, а файл adml является языковым дополнением. В admx файле содержится область применения параметра, ключ реестра, отвечающий за его настройку, а также ссылки на описание, которое находится в соответствующем языковом файле adlm и отображается при редактировании политики.

Существует несколько типов административных шаблонов в рамках групповых политик, которые позволяют управлять настройками компьютеров и пользователей в сети. Условно административные шаблоны можно разделить на несколько категорий:

1. Шаблоны реестра: позволяют изменять настройки операционной системы и приложений, хранящиеся в реестре Windows. Например, можно установить правила для паролей пользователей или ограничить доступ к определенным приложениям.
2. Шаблоны файлов: позволяют управлять правами доступа к файлам и папкам на компьютерах в сети. Например, можно ограничить доступ к конфиденциальным документам только определенным пользователям или группам.
3. Шаблоны программ: позволяют управлять установленными программами на компьютерах и настраивать их параметры. Например, можно запретить использование определенных программ или установить ограничения на их использование.
4. Шаблоны безопасности: позволяют установить правила безопасности для компьютеров и пользователей в сети. Например, можно настроить политику безопасности паролей или установить правила для брандмауэра.

После установки необходимых шаблонов можно приступать к применению политик на клиентах.

# Применение групповых политик в samba ad

Применение политик на клиентах осуществляется с помощью команды samba-gpupdate. Данная команда имеет различные ключи, влияющие на ее выполнение. Например, принудительное применение групповой политики на клиенте осуществляется с помощью следующей команды:

samba-gpupdate --force --target=User -U<username>

Базовые операции над клиентами групповых политик проводятся с помощью команды samba-tool gpo. Функционал данной комманды позволяет:

1. получать список всех GPO в домене;

samba-tool gpo listall -H ldap://192.168.50.24 -U administrator



Рис.1 Список всех GPO в домене

1. получать список GPO, назначенных учетной записи;

samba-tool gpo list User -H ldap://192.168.50.24 -U administrator



Рис.2 Список GPO назначенных учетной записи

1. получать информацию о GPO;

samba-tool gpo show \ {{31B2F340-016D-11D2-945F-00C04FB984F9} -H ldap://192.168.50.24 -U administrator



Рис 3. Информация о GPO

1. Создавать GPO

samba-tool gpo create "Server GPO" -H ldap://192.168.50.24 -U administrator



Рис.4 Создание GPO

5. Удалять GPO

samba-tool gpo del {2E8AACC8-A7A6-4FB3-8FF9-C6EE859A2625} -U administrator



Рис.5 Удаление GPO

# Заключение

В данной статье была рассмотрена возможность осуществления удаленного управления с помощью контроллера домена Samba. Удаленное управление с помощью Samba и групповые политики в Samba ad предоставляют администраторам эффективные инструменты для управления сетевой инфраструктурой, обеспечивая безопасность, гибкость и удобство в работе. Благодаря возможности удаленного управления с помощью Samba и внедрению групповых политик в Samba ad, администраторы могут эффективно контролировать доступ пользователей к ресурсам, устанавливать настройки безопасности, управлять профилями и многое другое в централизованном виде. Такие инструменты позволяют значительно упростить управление сетью, повысить безопасность данных и обеспечить более эффективную работу компьютерной инфраструктуры в целом.

**Список использованных источников**

1. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование : Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург : Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.
2. Администрирование объектов групповых политик [электронный ресурс]. URL: [https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362929#SambaкакконтроллердоменаAD-НазначениеSambaнарольADDC](https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362929" \l "SambaкакконтроллердоменаAD-НазначениеSambaнарольADDC)
3. Реализация групповых политик [электронный ресурс]. URL: <https://samag.ru/archive/article/3733>
4. Samba как контроллер домена AD [электронный ресурс]. URL: [https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362929#SambaкакконтроллердоменаAD-НазначениеSambaнарольADDC](https://wiki.astralinux.ru/pages/viewpage.action?pageId=27362929" \l "SambaкакконтроллердоменаAD-НазначениеSambaнарольADDC)
5. Samba AD [электронный ресурс]. URL: <https://www.altlinux.org/SambaAD_start>