”

+ Р

”

”Е

4 = Т

4 = Л

Планирование Active Directory

Что необходимо понимать под таким мудреным определением как «**Планирование Active Directory**»?

Проектирование систем на базе Windows Server требует больших ресурсов, как временных, так и людских.

Успех проекта зависит во многом от того, насколько корректно управляется проект, как распределены ресурсы, от подготовленности специалистов и персонала.

Процесс проектирования инфраструктуры Active Directory состоит из четырех этапов:

- Создание плана лесов.
- Создание плана доменов.
- Создание плана подразделений.
- Создание топологического плана сайтов.

Роли в проекте

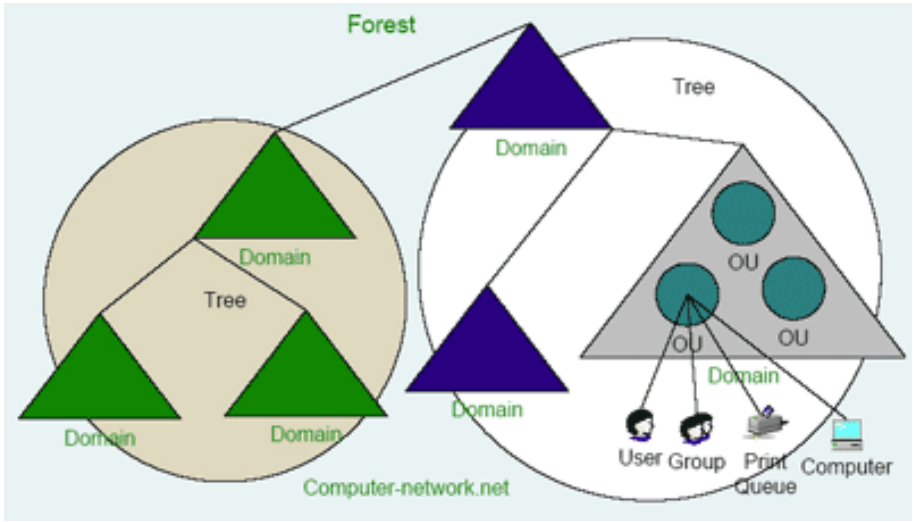
Руководитель службы IT

Руководитель проекта

Разработчик и тестировщик

Первый этап. Создание плана лесов.

Лес Active Directory предназначен для того, чтобы быть отдельным самодостаточным модулем. Внутри леса легко совместно использовать информацию и сотрудничать с другими пользователями из того же самого подразделения.



- Проектируя самый высокий уровень инфраст руктуры Active Directory, вы должны решить, нужно ли вам развертывать **один лес** или **несколько**.
- **Один –** в одном лесу пользователи работают с единым каталогом, задействуют все преимущества транзитивных доверительных отношений, а администраторы легко управляют всеми доменами.
- **Несколько – о**днако существуют ситуаций, когда необходимо и мы вынуждены использовать несколько лесов. Примером может служить объединение нескольких предприятий партнеров

Ситуации, в которых введение нескольких лесов оправдано

- Задачи сетевого администрирования **выполняются несколькими самостоятельными группами, между которых нет абсолютного доверия.**
- **Организационные единицы** в силу «политических» **причин разделены на самостоятельные группы.**

- Существует **необходимость в разделенном ведении организационных единиц**.

- **Леса содержат различные схемы каталога, контейнеров конфигурации и глобального каталога (GC).** В этом случае требуется через создание лесов изолировать их друг от друга.

- **Требуется в целях безопасности ограничить область доверительных отношений между доменами и деревьями доменов**.

- Создав два или больше леса, **Вы не сможете объединить их в один**. Можно клонировать лишь отдельные объекты, но перенос доменов и слияние лесов невозможны.
- На данном этапе **определяется владелец леса и создается так называемая «политика изменений леса** – документ который определяет круг лиц обладающих полномочиями управлением схемой и регулируют механизмы администрирования изменений, воздействующие на лес в целом.

В технических терминах просто определить, кто является владельцем леса. Группы **Schema Admins (Администраторы схемы), Enterprise Admins (Администраторы предприятия) и Domain Admins (Администраторы домена)** в корневом домене могут быть определены как владельцы леса, потому что они управ ляют теми изменениями, которые могут быть сделаны в лесу.

Политика управления изменениями леса определяет процедуры тестирования, одобрения и реализации любых изменений леса.

Два типа изменений леса:

- изменения схемы
- изменения раздела конфигурации каталога

Документ «политика управления изменениями леса» должна быть сформирована прежде, чем вы начнете развертывать Active Directory. Она так же должна быть прописана в документе более высокого ранга такой как «Политика IT безопасности предприятия» в целом.

Создание плана доменов

- Процесс планирования доменов, как и при планирования леса, начинается так же с анализа компании, фирмы или предприятия, и выявления или скажем формулирования требований целесообразности именно построения такого плана доменов.
- Всегда стремитесь свести количество доменов к **минимуму** насколько это возможно.

Чем хорош один домен? Перечислим преимущества:

- Отпадает необходимость планирования доверительных отношений
- Становится проще управлять пользователями и группами.
- При необходимости предоставления прав на администрировании или как говорится при делегирование прав, это делается на уровне организационных подразделений (OU).
- Единая политика безопасности.

Ситуации когда создание нескольких доменов необходимо и оправдано:

- В случае когда **необходимо привязать различные политики безопасности.** Так как политики безопасности могут содержать различные требования то создаются дополнительные домены и к каждому из них привязывается необходимая политика, или более жесткая.
- **Обеспечению соответствию административным требованиям, связными с правовыми соображениями или конфиденциальностью**.

- При **большом трафике репликации в целях его оптимизации проводят деление доменов или добавление доменов** или изначально зная что трафик будет большим и сразу создают больше доменов в зависимости от реальной ситуации.
- **При наличие в сети старых доменов** которых нужно сохранить под управлением Windows NT.
- **Необходимость создания отдельного пространства имен.**

Шаги деления доменов

Определение **Количества доменов:**

- Составить физическую и логическую топологию сети
- Определить количество пользователей
- Определить скорость передачи линии
- Определить надежность связи
- Все основные используемые протоколы.
- Программные приложения производящий обмен данными по сети.
- Тип связи (выделенные, коммутируемые).
- Загрузку каждого сегмента.

Шаги деления доменов

Выбор корневого домена.

- В этой роли может выступить **любой из существующих доменов в нашем лесу** доменов. Однако мы можем создать и **специальный домен.**
- Создавая специализированный корневой домен мы в конечном итоге получим некоторые **преимущества** по части администрирования системы защиты, оптимизации трафика репликации, и еще этим специализированным корневым доменом мы получим возможность более гибкого управления или лучше сказать маштабируемости нашего леса.

Шаги деления доменов

Определение иерархии доменов (или объединение доменов в деревья).

Алгоритм создания иерархии доменов.

- Определить количество деревьев в лесу.
- Назначить каждому дереву свой корневой домен.
- Расположить оставшиеся дочерние домены на более низких чем корневые домены уровнях иерархии.

Создание плана подразделений (OU)

- На этом этапе как и на предыдущих этапах проводится анализ выставляемых предприятием или фирмой требований, или требований вами разработанными. Затем определяется структура подразделений.

Три основных цели, побуждающих к созданию подразделений, заключаются в следующем:

- Делегирование административных полномочий
- Сокрытие объектов
- Администрирование групповой политики.

Создание топологического плана сайтов

- **Основное значение сайтов** – это физическая группировка компьютеров с целью оптимизации сетевого трафика.
- Структура сайтов Active Directory показывает нам размещение пользовательских сообществ.

Отдельный сайт нужно создать для следующих объектов:

- Для каждой локальной сети или набора локальных сетей, подключенных к высокоскоростным линиям связи.

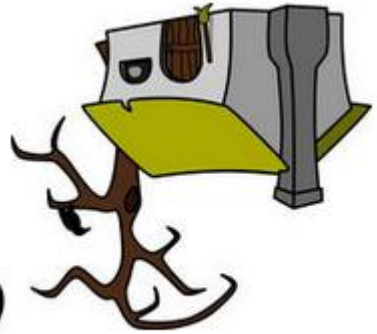
- Для каждой области, которая не связана с остальными нашими сайтами напрямую, и обмен информации доступен только по протоколу SMTP.

Д

2 = М

Л 

3

Я,, 

Т,  ’К

Д,  ,,, 

4 = О

1 = В

Е

, # ’ 

1 = Р

СВЕТА

2