

Дополнительные возможности использования Active Directory в корпоративной сети



Active Directory

Управление сетевыми ресурсами

Управление пользователями

Управление приложениями

Обеспечение функционирования сети

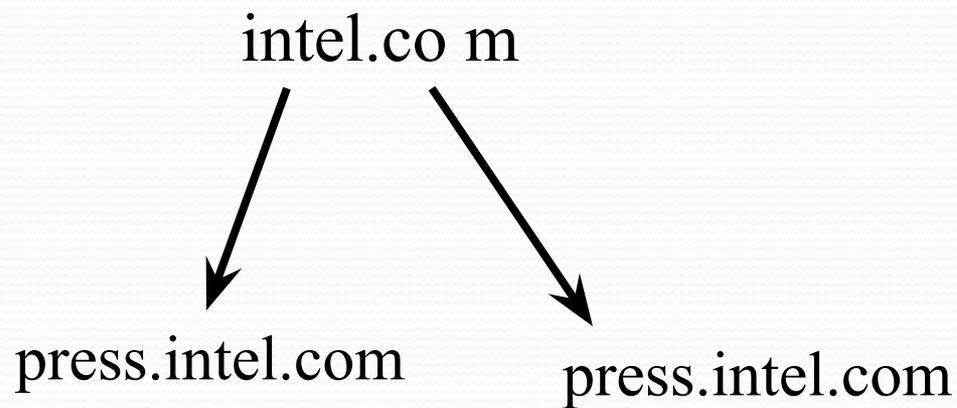
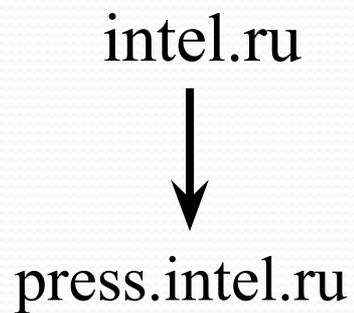
- *Службы Active Directory (службы активного каталога)* представляют собой распределённую базу данных, которая содержит все объекты домена. Доменная среда Active Directory является единой точкой аутентификации и авторизации пользователей и приложений в масштабах предприятия. Именно с организации домена и развёртывания служб Active Directory начинается построение ИТ-инфраструктуры предприятия.

- Основные понятия:
- Каталог – иерархическая структура, используемая для логического упорядочения объектов, ассоциированных с ресурсами сети
- Схема - структура, содержащая определения всех типов объектов, которые допустимо размещать в каталоге, а также совокупность правил, позволяющих управлять структурой каталога и его содержимым.

- Домены:
- Домен - совокупность компьютеров, характеризующаяся общей базой учетных записей пользователей и единой политикой безопасности. Контроллер домена - сервер, являющийся носителем глобальной копии каталога.

- Доменная модель:
- Дерево доменов - способ организации доменов, при котором они образуют непрерывное пространство имен.
- Лес доменов - способ организации доменов, при котором они не образуют непрерывное пространство имен.

● Пример:





● Режим:

Windows 2000 (смешанный)

Windows Server 2003



● Роли контроллеров домена:

Владелец доменных имен

Владелец схемы

Владелец идентификаторов

Эмулятор основного контроллера домена

Владелец инфраструктуры каталога

- 
- Иерархия объектов каталога:
 - Организационная единица - объект каталога, позволяющий группировать другие объекты, относящиеся к одной административной области
 - Сайт - совокупность подсетей, соединенных между собой высокоскоростными линиями связи



- Делегирование полномочий:

- На уровне узла

- На уровне домена

- На уровне организационной единицы

- Использование служб Active Directory значительно повышает уровень безопасности сети. Во-первых – это единое и защищённое хранилище учётных записей. В доменной среде все пароли доменных пользователей хранятся на выделенных серверах контроллерах домена, которые, как правило, защищены от внешнего доступа. Во-вторых, при использовании доменной среды для аутентификации используется протокол Kerberos, который значительно безопаснее, чем NTLM, использующийся в рабочих группах.

Обозначения:

- **SRV-1** и **SRV-2** – серверы
- **WS-1** и **WS-2** – рабочие станции
- **SAM-1**, **SAM2**, **SAM-3** и **SAM-4** – базы данных
- **USER-1** и **USER-2** - учетные записи пользователей, существующие в каждой из баз **SAM**
- Компьютер **SRV-1** ничего «не знает» об учетных записях компьютеров **SRV-2**, **WS-1**, **WS-2**, а так же всех остальных компьютеров сети.

Домен предоставляет ряд преимуществ:

- Упорядочение объектов
- Публикация ресурсов и сведений об объектах домена
- Применение объекта групповой политики к домену объединяет управление ресурсами и безопасностью
- Делегирование полномочий устраняет необходимость большого числа администраторов с широкими административными полномочиями
- Политики и параметры безопасности (такие как политики прав и пароля пользователя) не переходят от одного домена к другому
- Каждый домен хранит только сведения об объектах, расположенных в данном домене

- 
- Выполнил: Бушуев Артем. 13-09 КС