Основы Active Directory: 2 Часть.

telegra.ph/Osnovy-Active-Directory-2-CHast-07-30

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint July 30, 2024

Продолжаем разбираться с базовыми понятиями и элементами Active Directory:

- **Идентификатор безопасности (Security Identifier)** или **SID** используется как уникальный идентификатор участника безопасности или группы безопасности. Каждая учетная запись, группа или процесс имеет свой собственный уникальный SID, который в среде AD выдается контроллером домена и хранится в защищенной базе данных. SID можно использовать только один раз. Даже если принцип безопасности будет удален, его больше никогда нельзя будет использовать в этой среде для идентификации другого пользователя или группы. Когда пользователь входит в систему, система создает для него токен доступа, который содержит SID пользователя, предоставленные ему права и SID для любых групп, членом которых является пользователь. Этот токен используется для проверки прав всякий раз, когда пользователь выполняет какое-либо действие на компьютере. Существуют также хорошо известные SID, которые используются для идентификации общих пользователей и групп. Они одинаковы во всех операционных системах. Примером может служить группа «Everyone».
- **Отличительное имя (Distinguished Name) (DN)** — описывает полный путь к объекту в AD (например, cn=bjones, ou=IT, ou=Employees, dc=inlanefreight, dc=local). В этом примере пользователь bjones работает в ИТ-отделе компании Inlanefreight, а его учетная запись создана в организационном подразделении (OU), в котором хранятся учетные записи сотрудников компании. Общее имя (CN) bjones — это лишь один из способов поиска пользовательского объекта или доступа к нему в домене.

- **Relative Distinguished Name (RDN)** или **Относительное отличительное имя** — это отдельный компонент отличительного имени, который идентифицирует объект как уникальный среди других объектов на текущем уровне иерархии именования. В нашем примере bjones — это относительное отличительное имя объекта. AD не допускает двух объектов с одинаковым именем в одном родительском контейнере, но могут существовать два объекта с одинаковыми RDN, которые по-прежнему уникальны в домене, поскольку у них разные DN. Например, объект cn=bjones,dc=dev,dc=inlanefreight,dc=local будет распознан как отличный от cn=bjones,dc=inlanefreight,dc=local.
- **sAMAccountName** — это имя для входа пользователя. Это должно быть уникальное значение и содержать не более 20 символов.
- Атрибут **userPrincipalName** — это еще один способ идентификации пользователей в AD. Этот атрибут состоит из префикса (имя учетной записи пользователя) и суффикса (имя домена) в формате bjones@inlanefreight.local. Этот атрибут не является обязательным.
- **Контроллер домена только для чтения** или **Read-Only Domain Controller (RODC)** — имеет базу данных Active Directory, доступную только для чтения. Никакие пароли учетных записей AD не кэшируются на RODC (кроме учетной записи компьютера RODC и паролей RODC KRBTGT). Никакие изменения не передаются через базу данных AD RODC, SYSVOL или DNS.
- **Репликация (Replication)** — происходит в AD, когда объекты AD обновляются и передаются с одного контроллера домена на другой. При каждом добавлении контроллера домена создаются объекты подключения для управления репликацией между ними. Эти подключения устанавливаются службой проверки согласованности знаний Knowledge Consistency Checker (KCC), которая присутствует на всех контроллерах домена. Репликация обеспечивает синхронизацию изменений со всеми другими контроллерами домена в лесу, помогая создать резервную копию на случай сбоя одного контроллера домена.
- **Имя участника службы** или **Service Principal Name (SPN)** — однозначно идентифицирует экземпляр службы. Они используются в Kerberos для связывания экземпляра службы с учетной записью входа, позволяя клиентскому приложению запрашивать у службы проверку подлинности учетной записи без необходимости знать имя учетной записи.
- **Групповые политики (GPO)** — позволяют администраторам настраивать параметры компьютеров и пользователей в сети с использованием централизованных политик
- **Список управления доступом** или **Access Control List (ACL)** — это упорядоченный набор записей контроля доступа (ACE), которые применяются к объекту.
- Каждая **запись контроля доступа** или **Access Control Entries (ACE)** в ACL идентифицирует доверенное лицо (учетную запись пользователя, учетную запись группы или сеанс входа в систему) и перечисляет права доступа, которые разрешены, запрещены или проверяются для данного доверенного лица.

- Списки **DACL (Discretionary Access Control List)** определяют, каким принципам безопасности предоставляется или запрещается доступ к объекту; он содержит список ACE. Когда процесс пытается получить доступ к защищаемому объекту, система проверяет записи ACE в списке DACL объекта, чтобы определить, следует ли предоставлять доступ. Если у объекта нет DACL, система предоставит полный доступ всем, но если в DACL нет записей ACE, система будет отклонять все попытки доступа. Элементы ACE в списке DACL проверяются последовательно до тех пор, пока не будет найдено совпадение, которое разрешает запрошенные права, или пока доступ не будет запрещен.
- **System Access Control Lists** или **Списки управления доступом к системе (SACL)** — позволяет администраторам регистрировать попытки доступа к защищенным объектам. ACE определяют типы попыток доступа, которые заставляют систему создавать запись в журнале событий безопасности.
- **Полное доменное имя (Fully Qualified Domain Name)** — это полное имя конкретного компьютера или хоста. Он записывается с именем хоста и именем домена в формате [имя хоста].[имя домена].[TLD]. Это используется для указания местоположения объекта в древовидной иерархии DNS. Полное доменное имя можно использовать для поиска хостов в Active Directory без знания IP-адреса, как при просмотре веб-сайта, такого как google.com, вместо ввода связанного IP-адреса. Примером может служить хост DC01 в домене INLANEFREIGHT.LOCAL. Полное доменное имя здесь будет DC01.INLANEFREIGHT.LOCAL.