Administração de Sistemas (ASIST)

Aula Teórico Prática 07 - 2018/2019

Utilizadores e grupos no *Active Directory*
Políticas no *Active Directory*
Relações de confiança no *Active Directory*

Active Directory - LDAP

A estrutura lógica de domínios *Active Directory (domains, domain trees, forests)* é sustentada em bases de dados residentes em cada domínio (replicada entre os vários DC do mesmo domínio).

O serviço de diretoria usado no acesso a essas bases designa-se *Active Directory*, usa como base o protocolo LDAP. Cada domínio AD é identificado por um nome DNS, correspondendo ao **root-DN** da DIT do domínio. Tratando-se de uma DIT LDAP, o domínio está organizado em ramos.

Objetos como utilizadores e grupos estão alojados em ramos da DIT, alguns ramos são definidos pelo sistema, tais como **Buildin**, **Computers** e **Users** (são da classe *Container*). O administrador pode definir novos ramos criando objetos da classe ***Organizational Unit***.

Muitas das ferramentas de gestão do *Active Directory* protegem o utilizador de interagir diretamente com o LDAP, nomeadamente não identificando os objetos através do *distinguished name* (DN).

Num domínio AD, dois objetos podem ter o mesmo RDN desde que o DN seja diferente, ou seja, dois objetos podem ter o mesmo nome desde que estejam em ramos diferentes.

Sob o ponto de vista de administração, a divisão do domínio em ramos tem várias vantagens, mas a necessidade de referir a localização de cada objeto dentro do domínio acaba por ser um inconveniente.

AD – identificação de utilizadores e grupos

Os domínios Windows anteriores ao AD, sob o ponto de vista de nomeação de objetos eram completamente rasos.

Os utilizadores e grupos são identificados na forma **DOMAINNAME\USERNAME** e **DOMAINNAME\GROUPNAME**, onde DOMAINNAME é o nome *NetBIOS* do domínio (nome não qualificado do domínio AD).

Esta forma continua a ser suportada nos domínios AD, tanto para grupos como utilizadores, no caso dos utilizadores é mesmo a forma mais usada para identificação no início de sessão (***Down-Level Logon Name***).

No entanto, esta forma de identificar utilizadores e grupos não é suficiente no AD porque dentro do domínio podem existir vários grupos e utilizadores com o mesmo nome.

Para resolver este problema, no AD cada conta de grupo possui um nome **Pre-Windows 2000** para ser usado na forma **DOMAINNAME\nome-grupo**. Normalmente este nome é igual ao nome da conta de grupo, no entanto tem de ser único em todo o domínio.

O mesmo se passa no caso das contas dos utilizadores, o nome **Pre-Windows 2000** é habitualmente usado no login na forma **DOMAIN\username** (*Down-Level Logon Name*), por omissão é igual ao nome da conta. Dois utilizadores podem ter contas com o mesmo nome no AD do domínio, mas o *Down-Level Logon Name* de cada um deles terá de ser diferente.

AD – *User principal name* (UPN)

A forma mais atual de identificar um utilizador no AD é na forma UPN, também designado *User Logon Name*, porque é usado no *logon*:

username@AD-DNS-DOMAIN

Por omissão o UPN está definido com o nome da conta do utilizador (RDN do objeto) e o nome DNS do domínio AD. Num domínio não podem existir dois UPN iguais, se existirem duas contas de utilizadores com o mesmo nome, um deles terá de usar um UPN diferente do nome da conta.

Uma conta de utilizador num domínio é um objeto LDAP identificado por um DN, o atributo **cn** (*Common Name*) é usado no RDN, o seu valor é o nome da conta, por exemplo **cn=specialuser**.

Neste exemplo o UPN será **specialuser@AD-DNS-DOMAIN** e o nome Pre-Windows 2000 será **DOMAIN\specialuser**. Estes serão os valores por omissão, podem ser alterados pelo administrador se for necessário ou conveniente.

Também as contas de grupo são identificadas pelo atributo **cn** (*Common Name*) correspondendo ao nome da conta. Por isso, uma conta de utilizador e uma conta de grupo podem ter o mesmo nome apenas se tiverem em ramos diferentes, mas os nomes Pre-Windows 2000 terão de ser necessariamente diferentes.

AD – grupos

As contas de grupo num domínio AD são bastante diferentes das contas de **grupos locais** que apenas existem na máquina local. Num domínio as contas de grupo são armazenadas na base AD do domínio e são válidas em todo o domínio.

No AD os grupos são objetos LDAP identificados por um DN, dentro da base de dados do domínio (DIT) podem estar localizadas num qualquer ramos, o atributo **nome Pre-Windows 2000** (DOMAIN\group) permite identificar o grupo no domínio sem a necessidade de identificar o ramo. Ao contrário do que acontece com um grupo local, os grupos do AD podem ter como membros outros grupos (group *nesting*).

As máquinas que são membros de um domínio podem continuar a trabalhar com utilizadores e grupos locais, no entanto nos *domain controllers* não existem contas locais.

Existem dois tipos de grupo no AD:

Security group – são objetos de segurança, podem ser utilizados para atribuir direitos aos seus membros e podem ser incluídos em ACLs.

Distribution group – destinam-se a criar grupos lógicos de utilizadores e grupos, com outros objetivos. Não permite atribuir diretos aos membros nem podem ser usados em ACLs. Podem servir por exemplo para criar listas de distribuição de correio eletrónico. Note-se que um *security group* também pode ser usado para distribuir correio.

AD – *group scope*

O scope do grupo define a sua abrangência: em termos de membros que pode ter, grupos de que pode ser membro, e permissões ou direitos que lhe podem ser associados.

Local groups (Local scope) – existem apenas localmente na máquina (não estão no AD). Podem incluir membros de toda a floresta e outros domínios de confiança (*trusted domains*). Os direitos atribuídos ao grupo apenas podem ser relacionados com os recursos locais da máquina onde são definidos. Um *local group* não pode ser membro de outros grupos.

Domain local groups (Domain local scope) – existem no domínio AD. Podem incluir como **membros:** utilizadores e grupos globais de toda a floresta e outros domínios de confiança (*trusted domains*), grupos universais da floresta e grupos *domain local* do mesmo domínio. **Podem ser membros de:** grupos *domain local* do mesmo domínio e grupos locais de máquinas do mesmo domínio (excluindo grupos *build-in*). Os direitos atribuídos ao grupo podem dizer respeito a qualquer objeto ou recurso existente no domínio, mas não recursos de outros domínios.

AD – *Global and Universal groups*

Global groups (Global scope) – existem no domínio AD. **Membros possíveis:** utilizadores do mesmo domínio e grupos globais do mesmo domínio. No entanto um *global group* pode ser **membro de** grupos universais da mesma floresta, grupos globais do mesmo domínio e grupos locais definidos em máquinas de domínios de confiança. É possível atribuir a um *global group* permissões sobre qualquer domínio da floresta ou outros de confiança.

Universal groups (Universal scope) – existem no domínio AD. **Membros possíveis:** utilizadores da floresta, grupos globais e universais da mesma floresta. **Podem ser membros de:** grupos universais da floresta, grupos *domain local* de domínios de confiança (inclui todos os domínios da floresta) e grupos locais de máquinas de domínios de confiança. Os direitos atribuídos ao grupo podem dizer respeito a qualquer objeto ou recurso existente na floresta e outros *trusted domains*.

Um grupo **universal** pode ser convertido para ***domain local*** ou **global**.

Um grupo **global** pode ser convertido para **universal**.

Um grupo ***domain local*** pode ser convertido para **universal**.

Estas conversões apenas são válidas se não violarem as regras anteriormente enunciadas.

Organizational Units (OUs)

No contexto de um domínio AD, objetos como utilizadores, computadores e grupos encontram-se em ramos do LDAP, embora existam inicialmente definidos no AD alguns ramos como **Builtin**, **Users** e **Computers** que são do tipo ***Container***, podem ser definidos novos ramos através de objetos do tipo ***Organizational Unit (OU)***.

As OU permitem subdividir um domínio em áreas lógicas numa estrutura em árvore (uma OU pode conter outras OUs). Os objetos como utilizadores e grupos podem ser movidos de uma OU para outra OU dentro do mesmo domínio.

Existem várias vantagem em definir OUs. Sob o ponto de vista de organização tornam-se mais evidente para os administradores relações de afinidade entre subconjuntos de utilizadores e grupos estando organizados em OUs. Inicialmente está definida por exemplo a OU **Domain Controllers** que contém objetos do tipo **Computer** correspondentes aos vários DCs do domínio

As OUs permitem:

- **Delegar poderes de administração** – para uma dada OU, o administrador pode delegar a respetiva gestão a determinados utilizadores e grupos, definindo exatamente que poderes são delegados.
- **Definir políticas de grupo** (GPO – *Group Policy Objects*) a aplicar à OU e consequentemente a todos os objetos que estão na OU, como por exemplo contas de utilizadores.

Nomeação de gestores de grupos e OUs

No caso de uma OU, a forma recomendada para atribuir poderes de gestão a utilizadores ou grupos sobre a OU e objetos nela residentes é através da delegação (***Delegate Control***).

No entanto objetos das classes **Group**, **Computer** e **Organizational Unit** possuem o atributo **managedBy** que identifica o utilizador ou grupo que é responsável pela sua gestão. Esta constitui uma via alternativa de atribuir direitos de administração sobre uma OU, que no entanto parece apresentar alguns problemas em situações específicas.

Políticas

Uma política é um **conjunto de elementos de configuração**, inclui elementos de configuração relativos ao utilizador e relativos ao computador. Os elementos de configuração podem ser tão diversos como entradas no **Start Menu** e **Desktop**, chaves no **registry** (do utilizador e do computador), configurações de firewall e permissões (***user rights***) a atribuir ao utilizador.

Um elemento de configuração pode ou não estar definido numa política:

- Se estiver definido é aplicado ao utilizador/computador **eliminando definições anteriores** (originais, ou resultantes de aplicações anteriores de outras políticas).
- Se não tiver definido não afeta o valor corrente desse elemento.

Aplicação de políticas - Local Policy

As políticas são aplicadas no momento em que o utilizador realiza o login (quando de torna membro do grupo **Authenticated Users**).

No entanto, as políticas afetam não apenas o utilizador, mas também a configuração do computador onde ele efetua o login.

No caso de um login local, usando uma conta local do computador, existe uma única política aplicada designada **Local Policy** que está armazenada localmente no computador e pode ser gerida com a ferramenta **Local Security Policy**.

No caso de um login num domínio, a **Local Policy** definida no computador utilizado é aplicada em primeiro lugar, mas segue-se a aplicação de políticas definidas no *Active Directory* que consequentemente se vão sobrepor à **Local Policy**.

No contexto de um domínio *Active Directory* as políticas estão armazenadas em **Group Policy Objects** (GPO) existem alguns GPO definidos, mas podem ser criados outros.

Num domínio, os GPO podem ser geridos através da ferramenta **Group Policy Management**. Um GPO é um conjunto de elementos de configuração, para que seja aplicado durante o login dos utilizadores é necessário estabelecer ligações entre objetos apropriados do domínio e o GPO.

Aplicação dos GPO (*Group Policy Objects*)

Quando um utilizador efetua o login no domínio são inicialmente aplicadas as Local Policies, seguem-se as políticas definidas nos GPO do *Active Directory*.

Uma vez definidos os GPO, três tipos de objetos do AD podem ser ligados (*linked*) a eles: **Site**, **Domínio** e **OUs**.

Diferentes Sites, Domínios ou OUs podem ser ligadas ao mesmo GPO, também, um Site, Domínio ou OU pode ser ligado a vários GPO.

A ordem de aplicação dos GPO é notoriamente relevante porque um GPO sobrepõe-se aos GPO aplicados anteriormente (apenas para os elementos de configuração que define).

A ordem de aplicação segue a hierarquia do *Active Directory*: primeiro são aplicados os GPO aos quais o **Site** está ligado, depois os GPO aos quais o **domínio** está ligado e finalmente os GPO aos quais **cada OU** está ligada (seguindo a hierarquia entre diferentes OUs).

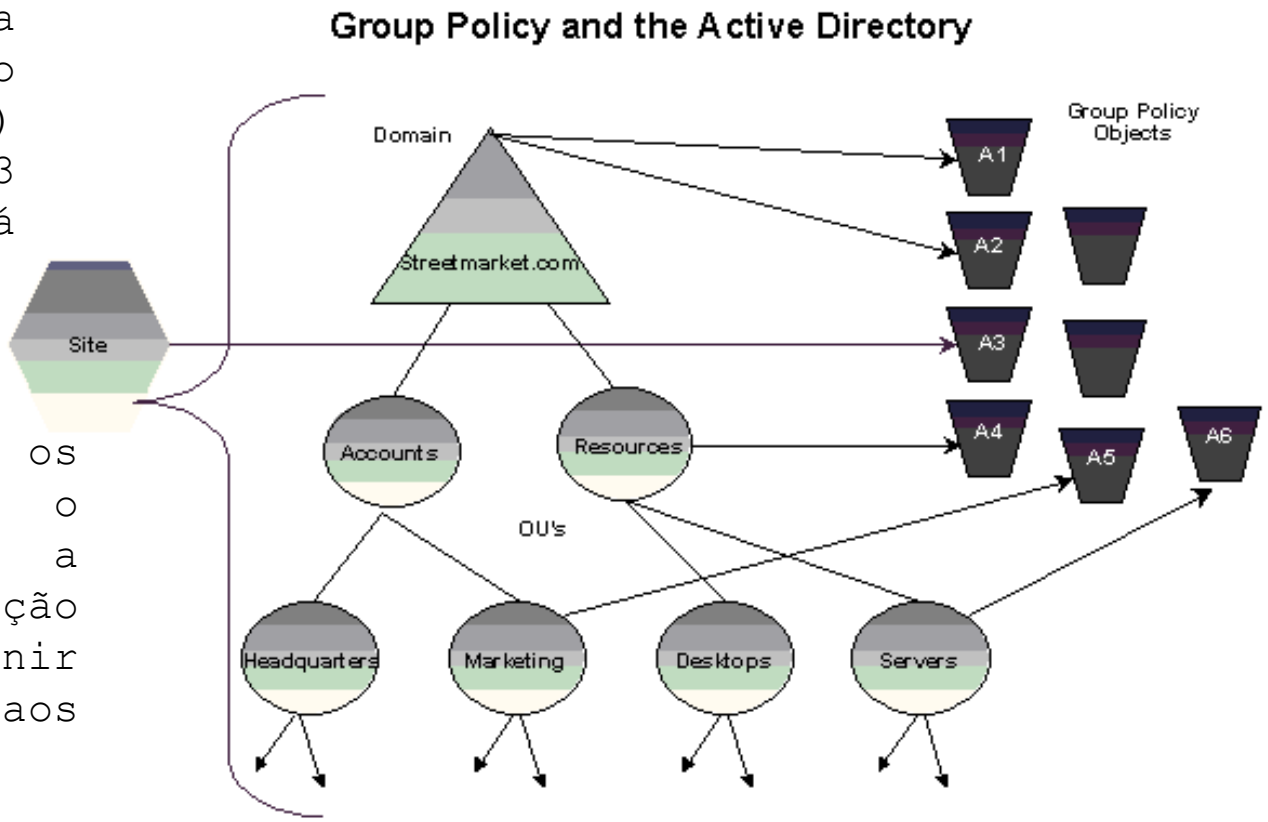
Quando um Site, domínio ou OU está ligado a vários GPO podemos definir exatamente a ordem de aplicação do vários GPO (***link order***).

Aplicação dos GPO - (*Group Policy Objects*)

A figura abaixo (*https://technet.microsoft.com*) apresenta um exemplo de aplicação de políticas no *Active Directory*.

Depois de aplicada a *Local Policy* (não representada na imagem) é aplicado o GPO A3 porque o Site está ligado a ele.

A seguir são aplicadas os GPO A1 e A3 porque o domínio está ligado a eles, a ordem de aplicação é estabelecida ao definir as ligações do domínio aos GPO (*link order*).



Aplicação dos GPO - (*Group Policy Objects*)

Os GPO são aplicadas a objetos do tipo **User** e **Computer**, não a objetos do tipo **Group**. Por outras palavras, os GPO aplicados a um utilizador são estabelecidos apenas pela conta de utilizador (nomeadamente a OU em que está definida) e **não pelos grupos de que ele é membro**.

Concretamente, se um utilizador é membro de um grupo e esse grupo está definido numa OU que está ligada a um GPO, então isso não é motivo para que esse GPO será aplicado ao utilizador durante o login.

Um cenário diferente é aquele em que o utilizador se encontra definido numa OU ligada a um GPO e esse GPO atribui a um grupo determinadas permissões (*user rights*). Neste caso o GPO será aplicado ao utilizador durante o login. Consequentemente, se o utilizador é membro do referido grupo terá as permissões que foram atribuídas ao grupo.

Active Directory Trust Relationships

As relações de confiança entre domínios podem ser estabelecidas nos dois sentidos (***two-way trust***) ou apenas num sentido (***one-way trust***).

Uma relação de confiança *one-way trust* pode ser usada quando temos interesse que um domínio possa aceder aos recursos de outro domínio, mas não o inverso.

As relações de confiança podem ser transitivas (***transitive trust***) ou não transitivas (**non*transitive trust***). Ser transitiva significa que a confiança se estende entre domínios, por exemplo: se o domínio A confia no domínio B (A-->B) e B confia em C (B-->C) então A confia em C (A-->C):

A-->B-->C => A-->C

Numa floresta existe implicitamente uma relação de confiança ***two-way transitive trust*** entre um domínio e o domínio hierarquicamente superior (pai). Por ser transitiva a confiança estende-se a todos os domínios da floresta, assim entre quaisquer dois domínios de uma mesma floresta existe sempre uma ***two-way trust***.

Para além das relações de confiança estabelecidas desta forma entre domínios da mesma floresta podemos definir outras relações de confiança, desde que se possuam as permissões de administração necessárias nos domínios e florestas envolvidos.

Active Directory – External Trust and Forest Trust

Uma **external trust** pode ser estabelecida entre um domínio de uma floresta e outro domínio de outra floresta. Pode ser **one-way** ou **two-way**, mas é **non*transitive***. Pelo facto de ser não transitiva não se propaga a outros domínios das florestas e fica confinada aos dois domínios entre os quais é estabelecida. De acordo com os sentidos em que é estabelecida permite aos utilizadores de um domínio aceder aos recursos do outro domínio.

Uma ***forest trust*** é de certa forma equivalente, mas ao nível de florestas. Pode ser **one-way** ou **two-way**, mas é sempre ***transitive***. Ao ser estabelecida aplica-se a toda a floresta, ou seja todos os domínios da floresta. De acordo com os sentidos em que é estabelecida permite aos utilizadores de qualquer domínio de uma floresta aceder aos recursos de qualquer domínio da outra floresta.

Active Directory – Realm Trust and Shortcut Trust

Uma ***realm trust*** é usada para estabelecer uma relação de confiança entre um domínio *Windows Active Directory* e um ***realm Kerberos*** versão 5 de sistemas não Windows, por exemplo Linux.

A *realm trust* pode ser **one-way** ou **two-way** e pode ser ***transitive*** ou **non*transitive***.

Uma ***shortcut trust*** é sempre ***transitive***, mas pode ser **one-way** ou **two-way**. Esta relação de confiança pode ser definida no seio de uma floresta para melhorar a performance das operações entre árvores diferentes da mesma floresta. A validação da relação de confiança entre dois domínios de árvores distintas é estabelecida recorrendo às relações de confiança através da hierarquia do AD até ao nível da floresta.

Sob o posto de vista de eficiência isso pode ser penalizador, por exemplo quando um utilizador de um domínio de uma árvore efetua o login num domínio de outra árvore. As ***shortcut trusts*** permitem evitar ir ao nível da floresta para este tipo de operações.