## ASIST – PL3

## Na máquina virtual Linux instale o necessário para autenticação centralizada com recurso a LDAP. Pretende-se que os utilizadores registados no LDAP do DEI possam autenticar-se na VM com as credenciais do DEI. Para tal deve utilizar o comando apt install libnss-ldapd (a ferramenta apt será explorada posteriormente) tendo em atenção as caraterísticas do LDAP:

Configurar a autenticação centralizada usando LDAP em uma máquina virtual Linux.

Primeiro procedemos à instalação do libnss-ldapd:

**sudo apt update**

**sudo apt install libnss-ldapd**

Durante a instalação configuramos o libnss-ldapd atendendo às seguintes informações:

**SERVIDOR: vsrv0.dei.isep.ipp.pt**

**URL: ldap://vsrv0.dei.isep.ipp.pt**

**Versão LDAP: 3**

**O administrador local não vai gerir a base de dados LDAP**

**Não é necessário efetuar o login no servidor LDAP**

**Configure o NSS para utilizar como segunda opção de autenticação o servidor LDAP indicado.**

Seguidamente, procedemos à verificação de autenticação, tendo, previamente, reiniciado o serviço NSS para aplicar as configurações acima descritas através do comando.

**sudo systemctl restart nscd**

Só depois tentamos fazer login com o utilizador:

**su - <nome\_de\_utilizador>**

Respondendo agora às perguntas referentes a este ponto:

1. Onde residem os ficheiros de configuração do LDAP?

Os ficheiros de configuração do LDAP estão localizados principalmente no diretório **/etc/ldap/**.

1. Qual o seu formato?

Os ficheiros de configuração do LDAP geralmente têm formato de texto simples, como arquivos de configuração padrão do Linux. O arquivo principal de configuração é o **/etc/ldap/ldap.conf**.

1. Como consegue corrigir um eventual engano na instalação do libnss-ldapd?

Se, eventualmente, cometermos algum erro durante a instalação, podemos corrigi-lo recorrendo ao comando **sudo dpkg-reconfigure libnss-ldapd** para reconfigurar as opções de autenticação LDAP.

1. Que alternativas tem para validar a autenticação com os seus dados do DEI na máquina virtual?

Além do **libnss-ldapd**, podemos considerar outras alternativas, como o uso do **PAM (Pluggable Authentication Module)** para configurar a autenticação LDAP. Existem ferramentas como a **ldapsearch** para verificar a conexão com o servidor LDAP e as informações do diretório LDAP. Além disso, a configuração do **SSSD (System Security Services Daemon)** é outra alternativa para autenticação LDAP.

## Na máquina virtual Windows Server vamos promovê-la a controlador de domínio (DC). Por omissão o Windows Server é instalado com um mínimo de serviços (Features) e funções (Roles). Para instalar/remover um serviço e/ou função podemos aceder ao Server Manager e escolher o que pretendemos:

1. Instale a função do **Active Directory Domain Services**:
2. Abrir o "**Server Manager**".
3. Clicar em "**Add roles and features**".
4. Selecionar "**Role-based or feature-based installation**" e clicar em "Next".
5. Selecione o seu servidor na lista e clicar em "**Next**".
6. Na lista de funções, selecione "**Active Directory Domain Services**" e clicar em "**Next**".
7. Seguir as instruções para concluir a instalação da função.
8. Criar uma nova floresta:

Após a instalação do **Active Directory Domain Services**, será solicitado a configuração do **AD**. Selecionamos, então, “**Add a new forest**".

Digitamos o nome da floresta no formato **wvdomXXX.dei.isep.ipp.pt**, onde **XXX** é o número da sua máquina virtual.

Seguimos as instruções para a configuração do domínio, definimos a senha do modo de restauração do Diretório de Serviços (DSRM) e continuamos com a configuração.

1. Por omissão, alguns serviços serão selecionados:
   1. Quais?

Por padrão, o serviço **DNS** é selecionado junto com o **Active Directory Domain Services** durante a instalação, pois o **DNS** é essencial para o funcionamento do **Active Directory**.

* 1. Porquê?

O **Active Directory Domain Services** depende do **DNS** para a resolução de nomes e para localizar controladores de domínio na rede. Portanto, o **DNS** é automaticamente instalado e configurado para dar suporte ao **Active Directory Domain Services**.

1. Deverá indicar o nível da floresta e do domínio:
2. Quais as implicações?

A escolha do nível da floresta e do domínio define a funcionalidade disponível no ambiente do **Active** **Directory**. Níveis mais altos permitem funcionalidades mais avançadas, mas podem ser incompatíveis com versões mais antigas do Windows Server. Deve prevalecer o nível que melhor atenda às necessidades da infraestrutura e que garanta que todas as máquinas no ambiente sejam compatíveis.

1. Por omissão, algumas características serão adotadas:
2. Quais?

As características padrão incluem **configurações de segurança**, **políticas de grupo** padrão e outras configurações do **Active** **Directory**.

1. Quais as implicações?

As configurações padrão são projetadas para um ambiente de segurança e funcionamento razoáveis. Podemos personalizá-las posteriormente de acordo com necessidades específicas.

1. Como pode agora aceder remotamente (via RDP) ao servidor?

Primeiramente, certificamo-nos de que a função "**Serviços de Área de Trabalho Remota**" está instalada no servidor.

No servidor, abrimos o "**Server Manager**".

Clicamos em "**Local Server**" no painel esquerdo.

Em "**Remote Desktop**," escolhemos a opção "**Disabled**" ao lado de "**Remote Desktop**."

Na janela de propriedades, selecionamos "**Allow remote connections to this computer**".

Agora temos tudo configurado para pode usar o **RDP** para conectar ao servidor remotamente.

1. O que sucedeu aos utilizadores criados na aula anterior?

Os utilizadores criados anteriormente **não fazem parte do domínio AD** que acabamos de criar no Windows Server. Eles não serão afetados e continuarão a existir como contas locais no sistema.

1. Criar os utilizadores wuser1, wuser2 e wuser3:

Primeiramente, abrimos o "**Active Directory Users and Computers**" no servidor.

Clicamos com o botão direito do mouse em "**Users**" e selecionamos "**New" -> "User**".

Agora, basta apenas seguir as instruções para criar cada utilizador, definindo os seus nomes e senhas.

1. Criar os grupos wgrupo1 e wasistgrupo:

No "**Active Directory Users and Computers**," clicamos com o botão direito do mouse em "**Users**" e selecione "**New" -> "Group**."

Tal como os utilizadores, basta apenas seguir as instruções para criar os grupos com os nomes desejados.

1. Associe o utilizador wuser1 ao grupo wasistgrupo e atribua a este grupo permissão para fazer login na consola:

Abrimos as propriedades do grupo "**wasistgrupo**."

Na guia "**Members**," adicionamos o utilizador "**wuser1**" ao **grupo**.

Para atribuir permissões de login, podemos optar por meio de políticas de grupo. Para isso, criamos uma **GPO** (**Group Policy Object**) e configuramos as permissões de login conforme necessário.

1. Criar as Organizational Units (OUs) ouasist1 e ouasist2:

No "Active Directory Users and Computers," clicamos com o botão direito do mouse no domínio e selecione "**New" -> "Organizational Unit**."

Aí, podemos criar as **OUs** com os nomes desejados.

Por fim, movemos os utilizadores "**wuser2**" e "**wuser3**" para suas respectivas **OUs** usando a opção "**Move**" no menu de contexto.