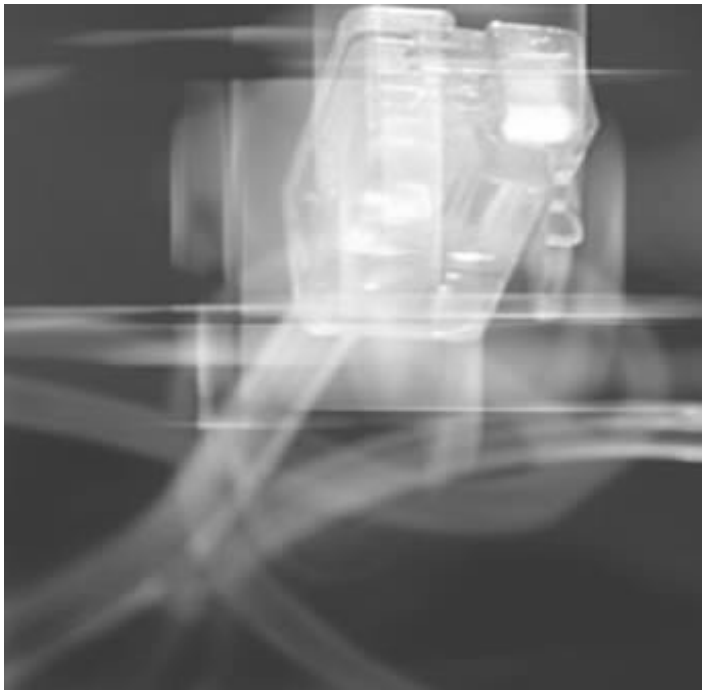
Configuração LDAP SSL

Documento Técnico

Revisão 1



ÍNDICE

Público Alvo

O presente documento é direccionado a Administradores de Domínio Windows.

Resumo

O presente documento pretende fazer uma abordagem sobre as configurações de Active Directory para possibilitar comunicações SSL por forma a proteger algumas comunicações entre a AD e o SIGES.

Objectivos

O objectivo do presente documento é fornecer todos os passos necessários para que possa ser estabelecido um certificado de confiança entre o servidor da Active Directory e a Java Virtual Machine onde está o sistema SIGES. Desta forma serão descritos todos os passos necessários para atingir esta configuração.

Revisões

Historial de revisões ao documento desde a sua criação:

v.1	22 Janeiro 2007	João Silva	Criação do documento

Documentos Relacionados

Para informações adicionais poderão ser consultados os seguintes documentos:

Documento1	Descrição Resumida do conteúdo do documento...

Envie-nos a sua opinião

A sua opinião é muito importante para nós. Todos os comentários que possa fazer sobre a qualidade e utilidade do presente documento servirá para continuamente podermos melhorar a qualidade deste e futuros documentos.

Esta informação será principalmente utilizada para futuras revisões deste mesmo documento.

Os seguintes tópicos são os mais relevantes sobre os quais gostaríamos de saber a sua opinião:

- Encontrou erros quer ortográficos, quer em termos do conteúdo?
- A informação está apresentada de uma forma clara?
- A informação é suficiente?
- Os exemplos apresentados estão correctos? São suficientes?
- O que mais gostou no presente documento

Estes e outros comentários ou sugestões que nos queira enviar poderão ser enviados para a nossa sede pelos seguintes meios:

- eMail: suporte@digitalis.pt
- Telefone: +351 21 440 89 90
- FAX: +351 21 440 89 99
- Correio: Digitalis Informática
  Estrada de Paço de Arcos nº9 Piso -1
  2780-666 Paço de Arcos
  Portugal

Pré-requisitos

Para realizar a configuração necessita verificar os seguintes pré-requisitos:

1. Active Directory em Windows 2000 ou 2003
2. Java Virual Machine(JVM) >= 1.5 instalada no servidor que irá hospedar o **SIGES** e variável de ambiente **JAVA_HOME** a apontar para o sitio onde a JVM esta instalada. Será também necessário ter **JAVA_HOME/bin** na variável de ambiente **$PATH**.
3. Certicate Authority Web Enrollment tool configurado no Servidor da Active Directory. Caso não tenha pode seguir esta documentação:

   http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/webenroll.mspx

Descrição do Processo

- Partindo do pressuposto que estão cumpridos todos os pré-requisitos e o servidor onde esta a Active Directory é servidor.dominio.pt, deverá o administrador executar os seguintes passos:
  - ① A partir do servidor que irá correr o SIGES, aceder via Browser a http://computador.dominio.pt/certsrv/certcarc.asp e nesta página, fornecer o login e passoword de acesso à Active Directory. Na página inicial clicar em **Download a CA Certificate** deixando a opção **DER encoded** seleccionada. Grave de seguida o ficheiro **certnew.cer** em qualquer pasta do servidor.
  - ① Posicione-se em **linha de comando** na pasta onde esta o certificado **certnew.cer** e executar os seguintes passos:
    - Existe o ficheiro **JAVA_HOME/jre/lib/security/cacerts** que contem a **client certificate authority** para a java virtual machine em causa. Uma boa prática será mudar a password **changeit** que este traz por defeito para uma definida por nós. Para o fazer, deve-se executar o seguinte comando:
      - Em windows:

        keytool -storepasswd -new novapassword -storepass changeit -keystore "%JAVA_HOME%/jre/lib/security/cacerts"

- Em Linux:

  keytool -storepasswd -new novapassword -storepass changeit -keystore $JAVA_HOME/jre/lib/security/cacerts

- De seguida devemos então importar o certificado para o ficheiro cliente **cacerts.** Parte-se do principio que o servidor onde se fez download do certificado tem o seguinte **DNS *servidor.dominio.pt.*** Com esta informação deve-se executar o seguinte comando:
  - Em windows:

    keytool -import -alias dominio -file certnew.cer -keystore "%JAVA_HOME%/jre/lib/security/cacerts"
  - Em Linux:

    keytool -import -alias dominio -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts

  Irá entao obter alguma informação sobre o certificado e deverá responder **yes** para que seja estabelecido o certificado de confiança entre cacerts e o servidor da Active Directory.
- Após o passo anterior, podemos testar se obtivemos o resultado previsto adicionando um utilizador à Active Directory através do **SIGES**.

Nota: O certificado tem a duração de um ano, pelo que antes de terminar este prazo ter-se-á de voltar a registar o certificado. Para o fazer, deverá seguir os seguintes passos(aconselhado a fazer no dia anterior à expiração do certificado de um ano):

- *Posicione-se na directoria onde tinha o **certnew.cer** e execute o comando abaixo com a password que deu ao certificado:*
  - *Em Windows:*

    keytool -delete -alias dominio -file certnew.cer -keystore "%JAVA_HOME%/jre/lib/security/cacerts"
  - *Em Linux:*

    keytool -delete -alias dominio -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts
- *Importe novamente o certificado fornecendo a mesma **password** do passo anterior:*
  - Em Windows:

    keytool -import -alias dominio -file certnew.cer -keystore "%JAVA_HOME%/jre/lib/security/cacerts"
  - Em Linux:

    keytool -import -alias dominio -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts

Erros/questões comuns

:: Descrição do primeiro possível problema

E se eu quiser apagar o certificado?

Deverá executar o comando ***keytool -delete -alias digitalis -file certnew.cer -keystore $JAVA_HOME/jre/lib/security/cacerts.*** Se pôr em prática esta opção, deve ter em conta que o certificado de confiança foi apagado e deixará de poder executar algumas operações que exigem SSL, tais como mudar a password de um utilizador da Active Directory. Deve então importar novamente o certificado com o comando descrito nos passos de configuração.

Ao importar o certificado obtive o seguinte erro *keytool error: java.io.IOException: Keystore was tampered with, or password was incorrect*. O que aconteceu?

Não forneceu a password que têm o cliente **cacerts.** Lembre-se que inicialmente esta era changeit e depois a alterou para uma password definida por si.

Erros que podem acontecer em stack trace:

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 525, v893
HEX: 0x525 - user not found
DEC: 1317 - ERROR_NO_SUCH_USER (The specified account does not exist.)
CAUSA: Acontece quando um utilizador é inválido

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 52e, v893
HEX: 0x52e - invalid credentials
DEC: 1326 - ERROR_LOGON_FAILURE (Logon failure: unknown user name or bad password.)
CAUSA: Acontece quando um utilizador é válido mas a password/credencial é inválida.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 530, v893
HEX: 0x530 - not permitted to logon at this time
DEC: 1328 - ERROR_INVALID_LOGON_HOURS (Logon failure: account logon time restriction violation.)
CAUSA: O utilizador está restrito de se autenticar na altura em que o está a tentar fazer.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 531, v893
HEX: 0x531 - not permitted to logon from this workstation
DEC: 1329 - ERROR_INVALID_WORKSTATION (Logon failure: user not allowed to log on to this computer.)
LDAP[userWorkstations: <multivalued list of workstation names>]
CAUSA: O utilizador não tem permissão para se autenticar no computador em causa.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error,Documento com configuracao ldap ssl (Source) data 532, v893

HEX: 0x532 - password expired

DEC: 1330 - ERROR_PASSWORD_EXPIRED (Logon failure: the specified account password has expired.)

LDAP[userAccountControl: <bitmask=0x00800000>] - PASSWORDEXPIRED

CAUSA: A password de utilizador expirou na Active Directory.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 533, v893

HEX: 0x533 - account disabled

DEC: 1331 - ERROR_ACCOUNT_DISABLED (Logon failure: account currently disabled.)

LDAP[userAccountControl: <bitmask=0x00000002>] - ACCOUNTDISABLE

CAUSA: A conta do utilizador foi desactivada na Active Directory.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 701, v893

HEX: 0x701 - account expired

DEC: 1793 - ERROR_ACCOUNT_EXPIRED (The user's account has expired.)

LDAP[accountExpires: <value of -1, 0, or extemely large value indicates account will not expire>] - ACCOUNTEXPIRED

CAUSA: A conta de utilizador expirou na Active Directory

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 773, v893

HEX: 0x773 - user must reset password

DEC: 1907 - ERROR_PASSWORD_MUST_CHANGE (The user's password must be changed before logging on the first time.)

LDAP[pwdLastSet: <value of 0 indicates admin-required password change>] - MUST_CHANGE_PASSWD

CAUSA: O utilizador tem de fazer reset à password da Active Directory

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 775, v893

HEX: 0x775 - account locked out

DEC: 1909 - ERROR_ACCOUNT_LOCKED_OUT (The referenced account is currently locked out and may not be logged on to.)

LDAP[userAccountControl: <bitmask=0x00000010>] - LOCKOUT

CAUSA: A conta de utilizador da Active Directory foi bloqueada.

`[LDAP: error code 50 - 00000005: SecErr: DSID-031A0F40, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0`

CAUSA: O utilizador do ficheiro dif-ldap.properties utilizado para estabelecer comunicação entre o SIGES e a Active Directory não pertence ao grupo Administradores