Pràctiques de laboratori

Serveis de domini d'Active Directory AD DS (2 sessions)

Concurrència i Sistemes Distribuïts

Presentació

Els serveis de domini d'Active Directory (AD DS) són un sistema distribuït la principal funció del qual és la de proporcionar identitats als usuaris d'una organització, encarregant-se d'autenticar-los i proporcionar així la base per poder autoritzar què podrán fer amb els recursos informàtics de l'empresa.

Aquesta pràctica té com a objetius que pugui descriure les principals característiques de ADDS, utilitzar les seves eines i procediments administratius associats, així com identificar algunes característiques dels sistemes distribuïts en un sistema concret.

Esperem que li resulti útil.

El professorat de CSD.

Material de suport i recomanacions

Abans d'assistir al laboratori es necessari veure els tres següentes vídeos que trobarà en el lloc PoliformaT de l'assignatura, en "Recursos / Materiales para el laboratorio / Práctica 4: Servicios de dominio de AD DS"

- Vídeo 1: Introducció als Serveis de Domini d'Active Directory (Conceptes Generals: dominis, controladors de domini, boscos i arbres, protocols)
- Vídeo 2: Creació de boscos i arbres
    - Activar rol de l'administrador
    - Crear un bosc
    - Crear un bosc i primer domini del bosc
    - Afegir controlador de domini
    - Crear nou arbre
    - Afegir membre al domini
- Vídeo 3: Directori d'Active Directory: gestió del directori i els seus elements (usuaris, equips, grups, contenidors, unitats organitzatives)

Suggeriments a l'hora de fer la pràctica:

- Tenir a ma les presentacions dels tres vídeos anteriors, també disponibles en PoliformaT, on es mosten els diferents procediments a realitzar.
- Al llarg de la pràctica veurà que hi ha una sèrie d'exercicis a realitzar. Es recomana resoldre'ls i anotar els seus resultats en els requadres que s'adjunten, per facilitar l'estudi posterior del contingut de la pràctica.
- Mantenir a la vista de forma constant l'última fulla d'aquest butlletí que conté un resum esquemàtic de la configuració a obtenir.

Utilització de l'entorn de màquines virtuals

Per realitzar aquesta pràctica utilitzarà cinc ordinadors conectats entre si mitjançant una xarxa privada i un enrutador que connecta la xarxa privada a Internet. Tots aquets ordinadors estan completament instal·lats, configurats i llests per al seu ús. Les seves dades son les següents:

Nom	Sistema Operatiu	Compte d'administració	Contrasenya
adc1	Windows 2008 R2	Administrador	Csd.Adc.1
am1	Windows 7 Professional	AdminW7	Csd.Am.1
edc1	Windows 2008 R2	Administrador	Csd.Edc.1
edc2	Windows 2008 R2	Administrador	Csd.Edc.2
em1	Windows 7 Professional	AdminW7	Csd.Em.1

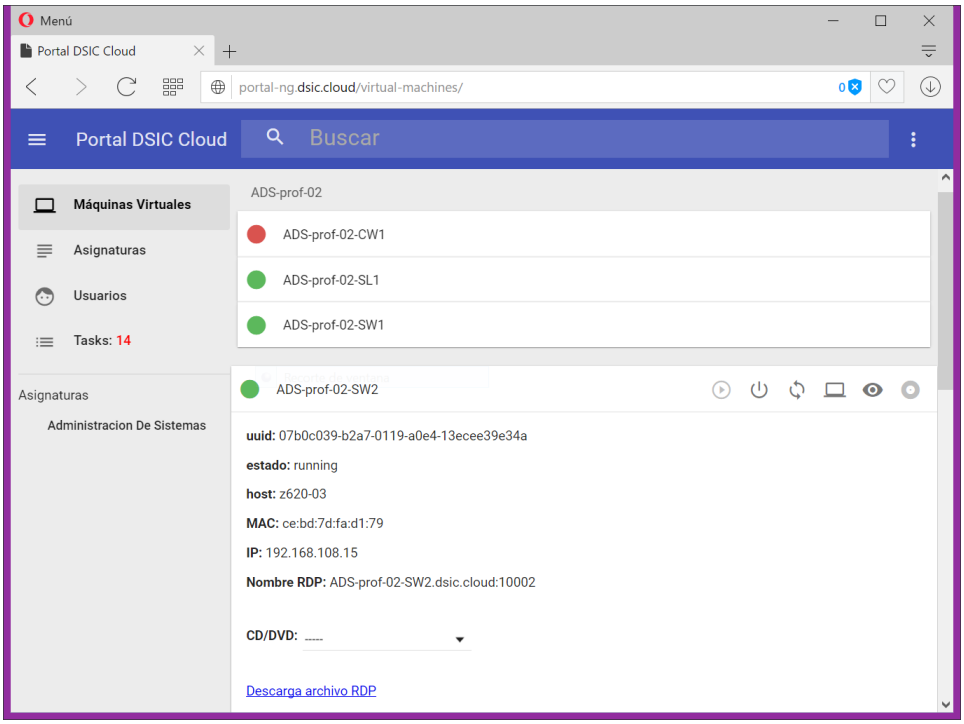
IMPORTANT: És probable que en algun moment les contrasenyes caduquen i el sistema sol·licite introducir-ne una nova. En eixe cas, la nova contrasenya deurà ser igual que la original però incrementant en un el seu valor numeric.

Per accedir a aquests ordinadors, des dels laboratoris del DSIC obri qualsevol navegador web, i connecti's a la següent URL:

https://portal-ng.dsic.cloud

Si el navegador alerta sobre la seguretat, ignori els advertiments i continuï.

La pàgina sol·licitarà les seves credencials del DSIC (usuari i contrasenya), i una vegada acreditat, mostrarà un panell amb les seves màquines virtuals, como es veu en la següent captura.



En cada màquina virtual es poden dur a terme les següents accions:

- Encender la màquina virtual
- Apagar la màquina virtual
- Refrescar la informació de la màquina virtual
- Accedir a la consola VNC

A més, prement sobre una màquina concreta es desplega una fitxa amb informació addicional.

Com a regla general hauria d'arrencar les màquines servidores primer i les màquines client a continuació. L'ordre d'arrencada adequada serà per tant:

edc1, edc2, adc1, em1, am1

Per favor, apagui sempre les màquines quan acabi d'utilitzar-les. Qualsevol màquina virtual que romangui en execució després de la sessió continuarà consumint (innecessàriament) recursos en el servidor que allotja aquesta màquina.

IMPORTANT: Apagui les màquines en l'ordre invers a la seva arrencada.

La primera vegada que encengui les seves màquines, és possible que se li demane seleccionar la ubicació de xarxa. En aquest cas, seleccioni "Xarxa de Treball"

Una vegada enceses des del panell, pot iniciar sessió en els seus sistemes utilitzant dos mètodes d'accés diferents:

1. El mètode recomanat perquè utilitzi la seva màquina remota és mitjançant una connexió a escriptori remot (RDP). Per a això, descarregui l'arxiu RDP associat a la seva màquina utilitzant l'enllaç que apareix al final de la fitxa de cada màquina virtual i obri-ho a continuació. Aquesta acció iniciarà l'aplicació "Connexió a escriptori remot" de Windows. Per entrar a cada màquina ha d'indicar el domini i usuari amb el qual connectar-se. Per exemple, al principi per connectar-se a l'equip adc1 haurà d'indicar: adc1\Administrador i la contrasenya Csd.Adc.1 (que és la indicada en la taula anterior).

2. Un mètode alternatiu consisteix a realitzar la connexió des del propi navegador, prement la icona amb forma de pantalla. Això obrirà una nova pestanya, i en ella un visor de tipus VNC. Aquest tipus de connexió presenta els desavantatges de tenir uns temps de resposta molt més alts respecte a RDP i diversos problemes amb l'ús del teclat que afecten als caràcters de puntuació i a les combinacions amb la tecla AltGr, fent necessari l'ús del teclat en pantalla en certes ocasions. No obstant això, resulta imprescindible per poder interactuar amb la màquina mentre s'inicialitza el sistema operatiu, la qual cosa no és possible amb el mètode anterior.

IMPORTANT: tot el descrit en aquesta secció funciona accedint des dels laboratoris del DSIC tal com s'ha explicat o, indistintament, des dels escriptoris virtuals del DSIC (http://www.upv.es/entidades/DSIC/infoweb/dsic/info/896580normalc.html).

Activitat 1 - Bosc de dominis

En aquest document els sol·licitem que construïsquen un bosc de dominis Active Directory adaptat a les característiques de la nostra empresa. Actualment disposem de dues seus. La seu principal està localitzada a València i es dedica a la comercialització i desenvolupament de productes d'alta tecnologia. La seu secundària està localitzada a Amsterdam i la seua funció principal és el desenvolupament de prototips del que poden ser els nostres futurs productes a comercialitzar.

Ambdues seus disposen en l'actualitat d'un espai de noms DNS ja existent, el qual no ha de canviar. Cada seu tindrà autonomia administrativa però és necessari que qualsevol usuari puga ser autoritzat a utilitzar qualsevol recurs informàtic de l'empresa, amb independència de les seus de l'usuari i del recurs. Donats aquests requisits, una estructura de bosc amb dos dominis sembla ser l'adequada en el nostre cas. Els detalls dels dominis i els ordinadors que formaran part d'aquests són els següents:

Domini Principal	
Nom DNS	`eovic.csd`
Primer controlador de domini	`edc1.eovic.csd`
Segon controlador de domini	`edc2.eovic.csd`
Membre del domini	`em1.eovic.csd`

Domini Secundari	
Nom DNS	`amsterdam.eovic.csd`
Primer controlador de domini	`adc1.amsterdam.eovic.csd`
Membre del domini	`am1.amsterdam.eovic.csd`

Guia de configuració

1. Cree el domini `eovic.csd`, configurant `edc1` com el primer controlador d'aquest domini

IMPORTANT: Configuri en `edc2`, `em1` i `adc1` el "servidor DNS preferido"[1] com `10.0.0.1` i el "servidor DNS alternativo" com `10.0.0.2` abans de realitzar cadascun dels passos 2 al 4

2. Configuri `edc2` com el segon controlador d'aquest domini

NOTA: En configurar el segon controlador mitjançant **DCPromo** cal deixar les opcions per defecte en el pas "Opciones adicionales del controlador del dominio".

3. Agregui a `em1` com a membre del domini `eovic.csd`
4. Cree el domini `amsterdam.eovic.csd`, configurant `adc1` com el primer controlador d'aquest domini

IMPORTANT: Configuri en `am1` el "servidor DNS preferido" com `10.0.0.4` i el "servidor DNS alternativo" com `10.0.0.1` abans de realitzar el pas 5

[1] En Panel de Control --> Redes e Internet --> Conexión área local --> Propiedades --> Protocolo de Internet versión 4 (TCP/IPv4) --> Propiedades --> direcciones de servidor DNS

5. Agregui a `am1` com a membre del domini `amsterdam.eovic.csd`

IMPORTANT: A partir d'aquest moment totes les validacions i activitats es realitzaran utilitzant els usuaris del domini (eovic\Administrador i amsterdam\Administrador) i no els administradors locals indicats a la pàgina 4 del butlletí.

Validació

Faça el següent conjunt de proves iniciant la sessió com l'usuari indicat en la columna "Usuari".

	Usuari	Prova
1	`eovic\Administrador`	Ha de poder iniciar sessió en `edc1`, `edc2` y `em1`, una vegada s'haja configurat el paper que cada ordinador exercirà en el bosc de dominis
2	`amsterdam\Administrador`	Ha de poder iniciar sessió en `adc1` y `am1`, una vegada s'haja configurat el paper que cada ordinador exercirà en el bosc de dominis.

Qüestions

1. Indiqui els quatre tipus de DC que se poden crear en funció de la seua relació amb el bosc, arbre i domini. Després indiqui els tres tipus utilitzats en aquesta activitat i el nom del DC de cadascun d'ells.

Activitat 2 - Usuaris i unitats organitzatives

La seu principal de l'empresa EOVIC i la seua seu a Amsterdam estan organitzades en departaments, estant cada treballador de l'empresa assignat a un i només un d'aquests departaments. En aquest document se li proposa plasmar com a elements d'Active Directory part de l'estructura departamental d'ambdues seus, així com un petit conjunt dels treballadors associats a aquests departaments. Cada departament serà representat en Active Directory com una unitat organitzativa, i a cada treballador se li crearà un compte d'usuari en la unitat organitzativa que correspon al departament al que pertany. Aquests departaments, així com alguns dels treballadors, es detallen en la taula següent:

Seu principal **Departament**	**Domini eovic.csd** **Treballadors**
Desenvolupament	dídac
Supervisió	samuel
Executius	enric

Seu a Amsterdam **Departament**	**Domini amsterdam.eovic.csd** **Treballadors**
Desenvolupament	delia
Supervisió	sara
Executius	eduard

Instruccions addicionals

- Encara que el domini `eovic.csd` pot gestionar-se tant des de `edc1` com des de `edc2`, no utilitzi de moment `edc2`. Treballarà amb aquest ordinador en una activitat posterior.
- Quan cree una unitat organitzativa, desactive l'opció "Proteger contra el borrado accidental"
- Quan cree un usuari, desactive l'opció "El usuario debe cambiar la contraseña en el siguiente inicio de sesión"
- Cree en el contenidor arrel de cada domini una unitat organitzativa anomenada `deptos`. En cada domini, cree les unitates organitzativas requerides en aquest document dins d'aquesta unitat `deptos`.
- Assigne la contrasenya "Eovic.1234" a tots els comptes d'usuari del domini `eovic.csd` i "Amsterdam.1234" a tots els comptes d'usuari del domini `amsterdam.eovic.csd`.

Validació

	Usuari	**Prova**
1	`eovic\dídac`	Ha de poder iniciar la sessió en l'ordinador `em1`
2	`amsterdam\delia`	Ha de poder iniciar la sessió en l'ordinador `am1`

Activitat 3: Escalabilitat administrativa

En AD DS, encara que cada domini dins d'un bosc és una entitat totalment autònoma des del punt de vista administratiu, els serveis d'identitat que es proporcionen són globals a tot el bosc. A aquesta característica la hi coneix com a escalabilitat administrativa, ja que el sistema distribuït pot construir-se a partir de diversos sistemes que operen amb autonomia, però malgrat això exerceix la seva funció com un únic tot. Gràcies a això, si per exemple es crea un usuari en un domini d'un bosc, aquest usuari serà conegut també en els altres dominis del mateix bosc, i per tant podrà ser, o no, autoritzat a usar els recursos de qualsevol domini del bosc. En aquesta activitat anem a explorar aquesta característica de AD DS.

Comenci realitzant les dos següents accions i contestant si l'acció ha estat o no possible:

	Usuari	Acció	Sí / No
1	`eovic\dídac`	Inicia la sessió en l'ordinador `am1`	
2	`amsterdam\delia`	Inicia la sessió en l'ordinador `em1`	

Si tot ha anat be, tant `dídac` com `delia` hauran pogut iniciar sessió, encara que ho hagin fet en un ordinador que no és del seu domini respectiu.

Intenti realitzar ara aquestes altres dues accions:

	Usuari	Acció	Sí / No
1	`eovic\administrador`	Inicia la sessió en l'ordenador `am1`	
2	`amsterdam\administrador`	Inicia la sessió en l'ordenador `em1`	

Hauria d'haver succeït el mateix que abans, és a dir, els administradors dels dominis també poden iniciar sessió en dominis que no són els seus.

Anem ara a intentar alguna cosa semblant una vegada més, però ara els inicis de sessió seran en els DCs de cada domini:

	Usuario	Acción	Sí / No
1	`eovic\administrador`	Inicia la sessió en l'ordenador `adc1`	
2	`amsterdam\administrador`	Inicia la sessió en l'ordenador `edc1`	
3	`eovic\dídac`	Inicia la sessió en l'ordenador `edc1`	
4	`eovic\dídac`	Inicia la sessió en l'ordenador `adc1`	
5	`amsterdam\delia`	Inicia la sessió en l'ordenador `adc1`	
6	`amsterdam\delia`	Inicia la sessió en l'ordenador `edc1`	

Ara haurà succeït alguna cosa diferent.

D'una banda, els usuaris normals del domini no hauran pogut iniciar sessió en els DCs. Això resulta raonable, ja que els DCs són ordinadors amb un accés bastant restringit donades les seves funcions. Només els usuaris que pertanyin a uns grups molt determinats, i en particular al grup de domini local Administradors, poden iniciar sessió.

D'altra banda, l'administrador del domini Eovic haurà pogut iniciar sessió en el DC d'Amsterdam, però no així l'administrador d'Amsterdam en el DC de Eovic. Això es deu al fet que quan es creen els dominis en un bosc, l'administrador del domini arrel s'inclou per defecte en el grup Administradors dels dominis secundaris, la qual cosa li concedeix el dret d'iniciar sessió en els DCs d'aquests dominis. El contrari en canvi no succeeix, els administradors de dominis secundaris no s'inclouen en el grup Administradors del domini arrel.

En qualsevol cas, l'administrador d'un domini secundari pot decidir en qualsevol moment eliminar a l'administrador del domini arrel del grup Administradors, recuperant així l'autonomia completa en el seu domini. Provi-ho, per a això:

- Com `amsterdam\administrador` inicie sessió en `adc1`
- Localitzi el grup Administradors que està en el contenidor "Builtin"
- Mostri les propietats d'aquest grup
- En la pestanya Membres, elimini al grupo Administradors d'empreses (al que pertany l'administrador del domini arrel)

I ara provi de nou:

	Usuari	**Acció**	**Sí / No**
1	`eovic\administrador`	Inicia la sessió en l'ordenador `adc1`	

Ara l'administrador de Eovic no haurà pogut accedir a `adc1`, i per tant haurà deixat de poder administrar el domini Amsterdam.

Activitat 4: Replicació

La replicació és un mecanisme essencial que permet que un sistema distribuït sigui escalable en grandària i ofereixi transparència de fallades.

En AD DS els controladors d'un mateix domini mantenen una rèplica del directori del domini. D'aquesta forma poden repartir-se la càrrega de treball i, el més important, si un controlador falla, la resta pot seguir prestant el servei d'identificació i autenticació d'usuaris sense interrupció.

En el bosc que va configurar en l'activitat 1, el domini Eovic disposa de dos controladors replicats, `edc1` i `edc2`. En aquesta activitat els va a utilitzar per observar com es comporta la replicació del directori en AD DS, realitzant una sèrie de proves i prenent nota de com es comporta el sistema.

Pot resultar convenient que utilitzi els dos ordinadors físics del laboratori, connectant-se en cadascun d'ells a un ordinador virtual diferent.

Prova 1

Inicïi sessió en `edc1` i en `edc2` i obri en tots dos ordinadors l'eina "Usuarios y Equipos de Active Directory"

- Observa els mateixos objectes (Unitats organitzatives i usuaris) en tots dos ordinadors? Per què?

Prova 2

En `edc1` cree l'usuari `diana` en la unitat de Desenvolupament i en `edc2` cree l'usuari `debora` en la unitat Desenvolupament. A continuació, actualitzi la vista de la unitat Desenvolupament en tots dos ordinadors (pot usar la tecla F5, l'entrada Actualitzar en el menú Acció i Contextual o el botó Actualitzar).

- Apareixen tant `diana` com `debora` en la unitat Desenvolupament tant en `edc1` com en `edc2`? Què pensa que ha succeït?

Prova 3

Cree alhora en `edc1` i en `edc2` l'usuari `sergi` en la unitat Supervisió. Perquè el més "alhora" possible, premi al mateix temps el botó "Finalitzar" del asistent de creació d'usuaris en tots dos ordinadors.

- S'han creat dos usuaris o un? Què pensa que ha succeït?

Prova 4

Va a comprovar ara com reacciona el sistema davant una fallada.

Comenci apagant l'ordinador `edc1`. Esperi al fet que estigui totalment apagat i a continuació realitzi el següent:

1. En `edc2` cree l'usuari `eva` en la unitat Executius i l'usuari `david` en la unitadt Desenvolupament.
2. Inicie sessió com a `eva` en em1
3. Inicie sessió com a `david` en em1
4. Inicie sessió com a `dídac` en em1

- Descrigui si ha anat tot be o ha sorgit algun problema amb les accions anteriors.

Prova 5

Com a última prova, torni a encender `edc1`.

- Indiqui si els usuaris `eva` y `david`, creats en l'anterior prova, apareixen en `edc1` en les seves respectives unitats organitzatives i quin creu que és el motiu.

Glossari de termes

En aquesta secció es proporciona un glossari dels principals termes necessaris per a la realització de la pràctica.

- *Domini de Active Directory* - És un conjunt d'ordinadors i usuaris, on usuaris i ordinadors són autenticats i identificats pels serveis del domini.
- *AD DS* – Solució que emmagatzema tota la informació rellevant dels elements que constitueixen el domini (usuaris, ordinadors, grups,…). Aquesta informació s'utilitza en els processos d'autenticació i autorització que succeeixen en el domini.
- *Controlador de Domini (DC)* - Ordinador (Windows Server) on s'han instal·lat els AD DS encarregats de la gestió del domini. Tot domini ha de tindre com a mínim un DC, si bé és recomanable tindre més d'un per replicar serveis.
- *Boscos i arbres* – A la xarxa interna d'una organització poden existir un o diversos dominis. El conjunt de dominis conforma un bosc i aquests dominis al seu torn s'organitzen en arbres en funció de la jerarquia establerta a través del nomenat DNS (Domain Name System) dels mateixos. Al primer domini creat a la xarxa se li denomina Domini Arrel del bosc.
- *Protocols estàndard* – AD DS es basa en una sèrie de protocols estàndard per al seu funcionament entre els quals ha de destacar-se: LDAP (Lightweight Directory Access Protocol), Kerberos i DNS (Domain Name System).
- *Serveis de directori* – Dins dels serveis que proporciona AD DS a un controlador de domini ha de destacar-se els serveis de directori doncs aquests permeten, entre uns altres, la gestió dels usuaris i equips. Aquesta gestió es realitza mitjançant objectes de tipus Usuari, Equip, Grup, Contenidor i Unitat Organitzativa. Els directoris de tots els dominis d'un bosc conformen un directori comú.
- *Unitat Organitzativa* – Un directori s'estructura com una jerarquia de contenidors. Un contenidor és un objecte que pot mantenir dins d'ell a altres objectes sent les unitats organitzatives un tipus particular de contenidor.
- *Usuaris* – Els objectes usuari representen als usuaris de la xarxa empresarial en els serveis de directori d'un domini, proporcionant a cada usuari una identitat única en el bosc al que pertany aquest domini.

Resum

Màquines virtuales

Nom	Sistema Operatiu	Compte d'administració	Contrasenya
adc1	Windows 2008 R2	Administrador	Csd.Adc.1
am1	Windows 7 Professional	AdminW7	Csd.Am.1
edc1	Windows 2008 R2	Administrador	Csd.Edc.1
edc2	Windows 2008 R2	Administrador	Csd.Edc.2
em1	Windows 7 Professional	AdminW7	Csd.Em.1

Dominis a crear

	Nom DNS	Controladors de dominio	Membres del domini
Principal	eovic.csd	edc1.eovic.csd edc1.eovic.csd	em1.eovic.csd
Secundari	amsterdam.eovic.csd	adc1.amsterdam.eovic.csd	am1.amsterdam.eovic.csd

Estructura i treballadors de Eovic (Example of a Very Important Company)

Seu principal **Departament**	**Domini eovic.csd** **Treballadors**
Desenvolupament	dídac, diana, debora, david
Supervisió	samuel, sergi
Executius	enric, eva

Seu a Amsterdam **Departament**	**Domini amsterdam.eovic.csd** **Treballadors**
Desenvolupament	delia
Supervisió	sara
Executius	eduard