opensuse sanda

Eduardo Adolfo Sotomayor G.

Copyright (c) 2014 Eduardo Adolfo Sotomayor G. Se concede permiso para copiar, distribuir y/o modificar este documento bajo los términos de la Licencia de Documentación Libre de GNU, Versión 1.3 o cualquier otra versión posterior publicada por la Free Software Foundation; siendo las Secciones Invariantes openSUSE 11.2 con Samba Guía Ilustrada, siendo los Textos de Cubierta Delantera Eduardo Adolfo Sotomayor G. Una copia de la licencia puede ser encontrada en la página Web de la FSF.

SUSE®, openSUSE®, el logo openSUSE®, son marcas registradas de Novell, Inc. En los Estados Unidos y otros países. Linux es marca registrada de Linus Torvalds. Todas las otras marcas son propiedad de sus respectivos dueños.

Configuración inicial del SO

Configuración de la red.	7
Desinstalar los paquetes samba que vienen con la distribución.	8
Instalar los paquetes necesarios.	9
Instalación de samba 4.x	
Descargar samba 4.x.	10
Instalar samba.	10
Editar los PATH.	10
Provisionamiento de samba 4.x	
Provisionar samba.	10
Iniciar samba.	11
Reiniciar samba.	12
Volver a leer la configuración de smb.conf.	12
Probar conectividad.	12
Configuración de DNS	
Configurar Bind.	13
Probando DNS.	17
Configuración de Kerberos	
Configurar Kerberos.	18
Probando kerberos.	18
Configuración de ntp	
Configurar ntp.	19
Habilitar y arrancar el servicio ntp.	19
Ajustes de seguridad	
Cambiar políticas de complejidad de password.	20
Para ver las políticas actuales.	20

Cambiar la clave de Administrator.	21
Agregar permisos administrativos varios al grupo Domain Admins.	21
Cuenta administradora de dominio alterna.	21
Configurando el servicio samba	
Configurando el servicio samba	22
Compartiendo Archivos	
Compartir archivos	23
Modificar los permisos del recurso compartido.	25
Configurando el Firewall	
Abrir los puertos correspondientes en el firewall	26
Uniendo estaciones de trabajo al dominio	
Unir las estaciones de trabajo al nuevo dominio.	28
Usando las RSAT (Remote Server Administration Tools)	
Herramientas de administración remota del servidor para Windows	34
Creando cuenta administradora de dominio alterna.	41
Creando Grupos de Seguridad.	43
Agregando usuarios a un grupo de seguridad.	45
Creando unidades organizativas.	47
Mover un Grupo a una Unidad Organizativa.	48
Creando GPO para restringir el uso del panel de control	50
Crear una GPO para restringir el acceso al regedit.	55
Bloquear un programa por medio de una GPO.	60
Ocultar Unidades en Mi Pc.	65
Vincular un GPO existente a una unidad organizativa.	71
Eliminar una GPO.	73
Delegar Control sobre una Unidad organizativa.	75
Revisar los permisos delegados.	78

Revocar los permisos delegados.	81
Delegar control para unir maquinas al dominio.	84
El entorno de red.	
Entorno de red.	85
DNS	
DNS	87
Agregando un registro (A)	91
Eliminar un registro (A)	92
Agregando un registro (MX)	92
DHCP	
Instalacion y configuracion del DHCP	94
Configurar las estaciones de trabajo como clientes DHCP	98
Permisos locales	
Permisos locales	101

En este manual se explica paso a paso con ilustraciones como instalar un controlador de dominio con samba 4.1 en openSUSE 13.1 con BIND como backend para DNS, en este caso se explica una implementación para la empresa SIENIC (Sistemas Informáticos de Entretenimiento) que cuenta con una red de 125 computadoras, a lo largo del manual se explica desde la instalación de samba 4.1 hasta la configuración y creación de políticas de grupo, delegación de privilegios, creación de grupos de seguridad, creación de usuarios, el manejo del DNS y DHCP, tratando de cubrir todos los aspectos básicos que se requieren para empezar a utilizar un controlador de dominio.

Esta guía no pretende ser una Biblia de samba 4.1 ni de Active Directory, pero si una herramienta que ayudara al administrador de red a tener una visión amplia de las cosas que se pueden hacer con Active Directory y tener una idea clara de que dirección tomar una vez terminada la implementación.

Samba es un proyecto que está evolucionando rápida y constantemente por lo que se recomienda estar al pendiente de nuevas versiones en el sitio oficial, para estar al día con estos cambios.



Configuración inicial del SO

Configuración de la red

Lo primero que hay que hacer es configurar una dirección IP estática para ello nos vamos a **Yast/Dispositivos de red/Configuración de red** y realizamos las configuraciones que se muestran a continuación adecuando las opciones a su respectivo caso.

		YaST2		00	×
Configur	ación de	Red			
pciones Globa	ales) <u>V</u> ista resu	ımen No <u>m</u> bre de Host/DNS E <u>r</u>	<u>n</u> caminamiento		
Método de Co	nfiguración de	Red			
O Controla	ada por el <u>U</u> sua <u>T</u> radicional con	rio mediante NetworkManager ifup			
Configuración	del Protocolo I	Pv6			
H <u>a</u> bilita	ar IPv6				
Opciones del	cliente DHCP				
Identificado	or de Cliente DH	ICP			٦
					3
Nombre de	host a enviar				
AUTO					
⊻ Mo <u>d</u> ific	ar el encamina	do Predeterminado Mediante DI	нср		
Ayuda		Cance	elar	Ac <u>e</u> pta	ar.
		YaST2) (
0		Ded			
 Configur	ación de	Red			
Configur pciones Globa	ación de ales Vista resi	umen No <u>m</u> bre de Host/DNS I	E <u>n</u> caminamiento		
Configur pciones Globa Nombre	ación de ales Vista resi	umen No <u>m</u> bre de Host/DNS I v i Dirección IP	E <u>n</u> caminamiento : Dispositivo	Nota	:

Configuración de tarjo General Direcco Tipo de Dispositivo	eta de red
General Direco Tipo de Dispositivo	
Tipo de Dispositivo	ción <u>H</u> ardware
(Nombre de Configuración
Ethernet 🔹	eno16777736
No están Configurados el enlace	y la IP(Esclavos asociados)
Dirección Dinémico	
Direccion Dinamica DHCP	DHCP Versiones 4 y 6(ambas)
 Dirección IP estática asignada 	
Direction IP Mase	cara de Subred Nombre de host
192.108.0.20 /24	smb4server01.sienic.site
Aña <u>d</u> ir <u>E</u> ditar	Eli <u>m</u> inar
Ayuda	<u>Cancelar</u> Siguiente
κ 😡	YaST2 😒 🔊
Configuración de Reg	d
Opciones Globales Vista resumen	Nombre de Host/DNS Encaminamiento
Nombre de Host y Nombre de Domir	nio
Nombre de host	Nombre de Dominio
smb4server01	sienic.site
🖉 Modificar Nombre de Host me	ediante DHCP Ningún interfaz con dhcp
	IR de bucle local
Asignar nombre de host a la	IF de bucie iocal
Asignar nombre de host a la	
Asignar nombre de host a la Modificar la configuración del DNS	Reglas Personalizadas
 ▲signar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados ◄ 	Reglas Personalizadas
△ Asignar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados → Servidores de Nombres y Lista de Bu	Reglas Personalizadas
△ Asignar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados Servidores de Nombres y Lista de Bu Servidor de Nombres <u>1</u>	Reglas Personalizadas úsqueda de Dominios <u>B</u> úsqueda de Dominio
 ▲signar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados → Servidores de Nombres y Lista de Bu Servidor de Nombres <u>1</u> 192.168.0.20 	Reglas Personalizadas úsqueda de Dominios Búsqueda de Dominio sienic.site
▲ signar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados → Servidores de Nombres y Lista de Bu Servidor de Nombres <u>1</u> 192.168.0.20 Servidor de Nombres <u>2</u>	Reglas Personalizadas úsqueda de Dominios Búsqueda de Dominio sienic.site
▲ signar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados ▼ Servidores de Nombres y Lista de Bu Servidor de Nombres <u>1</u> 192.168.0.20 Servidor de Nombres <u>2</u> 8.8.8.8	Reglas Personalizadas úsqueda de Dominios Búsqueda de Dominio sienic.site
▲ signar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados ▼ Servidores de Nombres y Lista de Bu Servidor de Nombres <u>1</u> 192.168.0.20 Servidor de Nombres <u>2</u> 8.8.8.8 Servidor de Nombres <u>3</u>	Reglas Personalizadas úsqueda de Dominios Búsqueda de Dominio sienic.site
 ▲signar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados → Servidores de Nombres y Lista de Bu Servidor de Nombres 1 192.168.0.20 Servidor de Nombres 2 8.8.8 Servidor de Nombres 3 	Reglas Personalizadas úsqueda de Dominios Búsqueda de Dominio sienic. site
▲signar nombre de host a la Modificar la configuración del DNS Usar Valores Predeterminados → Servidores de Nombres y Lista de Bu Servidor de Nombres <u>1</u> 192.168.0.20 Servidor de Nombres <u>2</u> 8.8.8.8 Servidor de Nombres <u>3</u>	Reglas Personalizadas úsqueda de Dominios Búsqueda de Dominio sienic.site

Desinstalar los paquetes samba que vienen con la distribución

zypper rm samba samba-client

eduardo:zypper - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
eduardo@linux-35wc:~> su
Contraseña:
linux-35wc:/home/eduardo # zypper rm samba samba-client
Obteniendo los datos del repositorio...
Leyendo los paquetes instalados...
Resolviendo dependencias...
Los siguientes paquetes van a ser ELIMINADOS:
samba samba-client
2 paquetes a quitar.
Luego de la operación, se liberarán 3,9 MiB.
¿Desea continuar? [s/n/? mostrar todas las opciones] (s):

Instalar los paquetes necesarios.

```
zypper install libacl-devel acl attr autoconf make \
    python-devel python gdb sqlite3-devel libgnutls-devel binutils \
    popt-devel keyutils-devel gcc \
    libidn-devel libxml2-devel \
    libattr-devel zlib-devel cyrus-sasl-devel gcc \
    krb5-client krb5-devel openldap2-devel libopenssl-devel\
    bind-utils bind-libs bind yast2-dns-server
```

<pre>> python-devel python gdb sqlite3-devel libgnutls-devel binutils \ > popt-devel keyutils-devel gcc nano\ > libidn-devel libxml2-devel libsepol-devel \ > libattr-devel zlib-devel cyrus-sasl-devel gcc \ > krb5-client krb5-devel openldap2-devel libopenssl-devel\ > bind-utils bind-libs bind vast2-dns-server</pre>
 python-devel python gdb sqlite3-devel libgnutls-devel binutils \ popt-devel keyutils-devel gcc nano\ libidn-devel libxml2-devel libsepol-devel \ libattr-devel zlib-devel cyrus-sasl-devel gcc \ krb5-client krb5-devel openldap2-devel libopenssl-devel\ bind-utils bind-libs bind vast2-dns-server
> popt-devel keyutils-devel gcc nano\ > libidn-devel libxml2-devel libsepol-devel \ > libattr-devel zlib-devel cyrus-sasl-devel gcc \ > krb5-client krb5-devel openldap2-devel libopenssl-devel\ > bind-utils bind-libs bind vast2-dns-server
Libidn-devel Libxml2-devel Libsepol-devel \ libattr-devel zlib-devel cyrus-sasl-devel gcc \ krb5-client krb5-devel openldap2-devel libopenssl-devel\ bind-utils bind-libs bind vast2-dns-server
> libattr-devel zlid-devel cyrus-sasl-devel gcc \ > krb5-client krb5-devel openldap2-devel libopenssl-devel\ > bind-utils bind-libs bind vast2-dns-server
> krb5-client krb5-devel openidap2-devel libopenssi-devel > bind-utils bind-libs bind vast2-dns-server
>DING-ULIUS DING-ULDS DING VASUZ-GNS-Server
Obteniende les detes del nenesitàrie
oreniendo los datos del repositorio
Leyenno los paquetes instatados
pytnon ya esta instatauo. Na hav actualización para 'python-275-821 y8664'. La última versión dieponi.
We hay actualization para python-2.7.5-6.5.1.800_04 . La uttima version disponi
indh' va está instalado
ya bay actualización para 'gdb-7.6.50.20130731-3.1.2.x86.64' La última versión
disponible va se encuentra instalada.
'acl' va está instalado.
No hay actualización para 'acl-2.2.52-2.1.2.x86 64'. La última versión disponibl
e ya śe encuentra instalada.
'bind-utils' ya está instalado.
No hay actualización para 'bind-utils-9.9.3P2-2.1.2.x86_64'. La última versión d
isponible ya se encuentra instalada.
'attr' ya está instalado.
No hay actualización para 'attr-2.4.47-2.1.2.x86_64'. La última versión disponib
le ya se encuentra instalada.
'bind-libs' ya esta instalado.
No hay actualizacion para 'bind-libs-9.9.3P2-2.1.2.x86_64'. La ultima version di
sponible ya se enduentra instalada.
Resolviendo dependencias,
es siguientes pequetes NUEVOS ven a sen instaladas.
Los siguientes paquetes NOEVOS van a ser instatados:
amodevel kevutils-devel krb5-client krb5-devel liberl-devel liberno
libatomic] libattr-devel libcom err-devel libgmoxx4 libgnutls-devel
libidn-devel libitml libnettle-devel libopenssl-devel libsepol-devel

Instalación de samba 4.x

Descargar samba 4.x

http://www.samba.org/samba/ftp/stable/samba-4.1.3.tar.gz

Instalar samba

tar -xzvf samba-4.1.3.tar.gz

cd samba-4.1.3

./configure && make && make install

Editar los PATH

Editar el archivo ~/.bashrc y agregar lo siguiente al final

export PATH=\$PATH:/usr/local/samba/sbin:/usr/local/samba/bin

Provisionamiento de samba 4.x

Provisionar samba

samba-tool domain provision --interactive

eduardo: bash - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS, CN=System, DC=sienic, DC=site
Creating CN=MicrosoftDNS, CN=System, DC=sienic, DC=site
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
See /usr/local/samba/private/named.conf for an example configuration include file for BIND
and /usr/local/samba/private/named.txt for further documentation required for secure DNS updates
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /usr/local/samba/private/krb5.conf
Once the above files are installed, your Samba4 server will be ready to use
Server Role: active directory domain controller
Hostname: sienic.site
DOMAIN SID: S-1-5-21-378946540-4025370916-4104212663
smb4server01:/home/eduardo #

Iniciar samba

Es necesario iniciar samba manualmente

samba

Reiniciar samba

Estos son los comandos necesarios en caso que necesitemos reiniciar samba

killall samba samba

Volver a leer la configuración de smb.conf

```
smbcontrol all reload-config
```

Probar conectividad

Los siguientes comando nos sirven para probar el servidor, el primero es para verificar la versión de samba, el segundo es para listar los recursos compartidos en el servidor, el ultimo es para probar la autenticación conectándonos a netlogon usando las credenciales de administrator.

```
smbclient --version
smbclient -L localhost -U%
smbclient //localhost/netlogon -UAdministrator -c 'ls'
```

La salida de estos comandos debe ser similar a la mostrada en la siguiente imagen

```
server01:/home/eduardo # smbclient --version
Version 4.1.0-3.5.1-3087-SUSE-oSI3.1-x86 64
smb4server01:/home/eduardo # smbclient -L localhost -U‰
Domain=[SIENIC] OS=[Unix] Server=[Samba 4.1.3]
         Sharename
                           Туре
                                       Comment
                           Disk
         netlogon
         sysvol
                           Disk
                                       IPC Service (Samba 4.1.3)
         IPC$
                           IPC
Domain=[SIENIC] OS=[Unix] Server=[Samba 4.1.3]
         Server
                                 Comment
         Workgroup
                                 Master
 mb4server01:/home/eduardo # smbclient //localhost/netlogon -UAdministrator -c 'ls'
Enter Administrator's password:
Domain=[SIENIC] OS=[Unix] Server=[Samba 4.1.3]
                                                      0 Thu Dec 26 09:48:20 2013
                                                      0 Thu Dec 26 09:48:30 2013
                  40059 blocks of size 524288. 28958 blocks available
  nb4server01:/home/eduardo # 🚪
```

Configuración de DNS

Configurar Bind

Yast/servicios de red/servidor DNS



En **Lista de redireccionadores** poner el ip de este servidor DNS y del servidor DNS del ISP o el que convenga y clic en añadir.

×		YaST2	\odot \odot \otimes
Instalación de Política DNS netconfig	el servidor DNS: Política personalizada	Configuración de	el redireccionado
auto 🔹	auto		
Añadir dirección IP			
Dirección IPv4 o IPv6			Añadir
Lista de redireccionado	pres		
192.168.0.20 8.8.8.8			Eliminar
Ayuda	Atrás	Cancelar	Siguiente

Hacemos clic en **Siguiente** y procedemos a eliminar la zona ipv6 que aparece en la lista de zonas si no hacemos uso de ipv6 y damos clic en **siguiente**.

<u>A</u>trás

Nombre		<u>T</u> ipo	
example.com		Maestro 👻	Aña <u>d</u> ir
onas DNS configurad	as		
ona		✓ Tipo	Eliminar
.0.0.0.0.0.0.0.0.0.0.0.0.0.0		.o.ipo.arpa Maestro	Editar
	<u> </u>		
Ayuda	<u>A</u> trás	Cancelar	Siguient
istalación de	al servidor DNS: Zon	as DNS	
adir nueva zona			
adir nueva zona	YaST2 <2>	2 0 0 0	
adir nueva zona <u>N</u> ombre example.com	YaST2 <2> (2 ⊗ ⊙ ⊗ leccionada? →	Aña <u>d</u> ir
adir nueva zona Vombre example.com	X S YaST2 <2>	2 🛛 🔿 🗶	Aña <u>d</u> ir
iadir nueva zona <u>N</u> ombre example.com	YaST2 <2> (2 ⊗ ⊙ ⊗ leccionada? →	Aña <u>d</u> ir
adir nueva zona <u>N</u> ombre example.com onas DNS configurad:	YaST2 <2> (2 2 2 2 2 2 2 2 2 2 2 2 2	2 S S S	Aña <u>d</u> ir
iadir nueva zona Nombre example.com onas DNS configurada	YaST2 <2> ¿Eliminar la entrada sel <u>Sí</u> <u>N</u> o	2 ∞ ∞ ⊗ leccionada?	Aña <u>d</u> ir Elimina <u>r</u>

En esta pantalla seleccionamos las opciones a como se muetran en la siguiente imagen y damos clic en **terminar**.

<u>C</u>ancelar

Ayuda

Puerto ab	pierto en el cortafuegos	Detalles del cortafuegos	1
El puerto del o	cortafuegos está abiert	o en todas las interfaces	
Soporte <u>L</u> DA	AP activo		
Comportamiento	o durante el inicio		
and the second			
• Act <u>i</u> var: inicia	ar ahora y durante el ar	ranque	
• Act <u>i</u> var: inicia De <u>s</u> activar: s	ar ahora y durante el ar solo iniciar manualmente	ranque e	
• Act <u>i</u> var: inicia De <u>s</u> activar: s	ar ahora y durante el an colo iniciar manualmento	ranque e	
Act <u>i</u> var: inicia De <u>s</u> activar: s Redirecci Dominios	or ahora y durante el ar olo iniciar manualmente onadores: 192.168.0.2 :: ., localhost, 0.0.127.ir	ranque e 0, 8.8.8.8 n-addr.arpa	
 Act<u>i</u>var: inicia De<u>s</u>activar: s Redirecci Dominios 	ar ahora y durante el ar colo iniciar manualmento onadores: 192.168.0.2 :: ., localhost, 0.0.127.ir	ranque e 0, 8.8.8.8 n-addr.arpa	
 Act<u>i</u>var: inicia De<u>s</u>activar: s Redirecci Dominios 	ar ahora y durante el ar colo iniciar manualmento onadores: 192.168.0.2 :: ., localhost, 0.0.127.ir	ranque e 0, 8.8.8.8 n-addr.arpa	
Act <u>i</u> var: inicia De <u>s</u> activar: s Redirecci Dominios	ar ahora y durante el ar colo iniciar manualmento onadores: 192.168.0.2 :: ., localhost, 0.0.127.ir	ranque e 0, 8.8.8.8 n-addr.arpa	
 Act<u>i</u>var: inicia De<u>s</u>activar: s Redirecci Dominios 	ar ahora y durante el an colo iniciar manualmento onadores: 192.168.0.2 :: ., localhost, 0.0.127.ir	ranque e 0, 8.8.8.8 n-addr.arpa	

Ahora nos vamos a Yast/Seguridad y Usuarios/Configuracion Apparmor



Seleccionamos Configuracion y hacemos clic en ejecutar



Quitamos el check a Habilitar AppArmor

🗙 🐷 Config	Yas⊺2 uración de AppArmor	000
g	abilitar AppArmor	
Configu	urar AppArmor	
	Configurar modos de perfiles	
	Definir modos de perfiles Co <u>n</u> figurar	
Ayuda	<u>A</u> trás <u>C</u> ancelar	Terminado

Le damos los permisos adecuados a la carpeta /usr/local/samba/private/dns

chown named:named -R /usr/local/samba/private/dns

Ahora procederemos a editar el archivo /etc/named.conf y agregamos lo siguiente en la sección de opciones:

tkey-gssapi-keytab "/usr/local/samba/private/dns.keytab";

Luego agregamos esto al final del archivo

```
include "/usr/local/samba/private/named.conf";
```

Editamos el archivo /usr/local/samba/private/named.conf y habilitamos la sección

database "dlopen /usr/local/samba/lib/bind9/dlz_bind9_9.so";

Y comentamos la opción que estaba habilitada por defecto que es

database "dlopen /usr/local/samba/lib/bind9/dlz_bind9.so";.

El archivo debe quedar a como se muestra en la siguiente ilustración

```
# This DNS configuration is for BIND 9.8.0 or later with dlz_dlopen support.
#
# This file should be included in your main BIND configuration file
#
# For example with
# include "/usr/local/samba/private/named.conf";
#
# This configures dynamically loadable zones (DLZ) from AD schema
# Uncomment only single database line, depending on your BIND version
#
dlz "AD DNS Zone" {
    # For BIND 9.8.0
    #database "dlopen /usr/local/samba/lib/bind9/dlz_bind9.so";
    # For BIND 9.9.0
    database "dlopen /usr/local/samba/lib/bind9/dlz_bind9_9.so";
};
```

Editamos el archivo /etc/sysconfig/named y modificamos las siguientes opciones para que queden asi:

NAMED_RUN_CHROOTED="no"

Opcionalmente podemos deshabilitar el uso de ipv6 si no lo utilizamos en nuestra red.

NAMED_ARGS="-4"

Probando DNS

```
# host localhost. 127.0.0.1
# host 127.0.0.1 127.0.0.1
# host -t SRV _ldap._tcp.sienic.site.
# host -t SRV _kerberos._udp.sienic.site.
# host -t A smb4server01.sienic.site.
```

```
smb4server01:/home/eduardo # host localhost. 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
localhost has address 127.0.0.1
localhost has IPv6 address ::1
smb4server01:/home/eduardo # host 127.0.0.1 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1
Address: 127.0.0.1#53
Aliases:
1.0.0.127.in-addr.arpa domain name pointer localhost.
smb4server01:/home/eduardo # host -t SRV _ldap._tcp.sienic.site.
ldap._tcp.sienic.site has SRV record 0 100 389 smb4server01.sienic.site.
smb4server01:/home/eduardo # host -t SRV _kerberos._udp.sienic.site.
kerberos._udp.sienic.site has SRV record 0 100 88 smb4server01.sienic.site.
smb4server01:/home/eduardo # host -t A smb4server01.sienic.site.
smb4server01.sienic.site has address 192.168.0.20
smb4server01:/home/eduardo #
```

Configuracion de Kerberos

Configurar Kerberos

Editamos el archivo /etc/krb5.conf y le ponemos el siguiente contenido suponiendo que el nombre del realm es SIENIC.SITE, este tiene que estar escrito en mayúsculas.

[libdefaults]

default_realm = SIENIC.SITE
dns_lookup_realm = false
dns_lookup_kdc = true

Probando kerberos

kinit administrator@SIENIC.SITE

klist

Archivo Editar Ver Marcadores Preferencias Ayuda smb4server01:/home/eduardo # kinit administrator@SIENIC.SITE
Password for administrator@SIENIC.SITE:
Warning: Your password will expire in 41 days on jue 06 feb 2014 09:48:28 CST
smb4server01:/home/eduardo # klist
Ticket cache: DIR::/run/user/0/krb5cc/tkt59RGN5
Default principal: administrator@SIENIC.SITE
Valid starting Expires Service principal
26/12/13 10:23:08 26/12/13 20:23:08 krbtgt/SIENIC.SITE@SIENIC.SITE
renew until 27/12/13 10:23:02

Configuración de ntp

Configurar ntp

Nos vamos a la ruta /usr/local/samba/var/lib/ y cambiar los permisos del directorio ntp_signd

chgrp -R ntp /usr/local/samba/var/lib/ntp_signd

chmod -R 750 /usr/local/samba/var/lib/ntp_signd

Editamos el archivo /etc/ntp.conf y le ponemos el siguiente contenido:

```
server 127.127.1.0
fudge 127.127.1.0 stratum 12
ntpsigndsocket /usr/local/samba/var/lib/ntp_signd/
restrict default mssntp
```

Habilitar y arrancar el servicio ntp

Los comando para habilitar y arrancar el servicio NTP son:

systemctl enable ntp.service

systemctl start ntp.service

Sugerencia: Una excelente herramienta para mantener sincronizados los relojes en las estaciones de trabajo con Windows es <u>http://www.timesynctool.com/</u>

🌙 NetTime Op	otions				
	Hostr	name or IP Address	Protoc	ol	Port Number
Time Servers:	192.	168.0.20	SNTP	-	123
				-	
				÷]
				¥]
				•]
Update Interval:	2	hours 👻			
Retry Interval:	1	minutes 🔻			
Demote Serv	ers af	ter 4 failures.			
Allow other	compu	ters to sync to this co	mputer		
Always (orovide	time (NOT recommen	ded!)		
V Show NetTir	ne icon	in the system tray at	login		
📝 Start NetTim	e servi	ce at bootup			
Max Free Run:	24	hours -			
If Time adjustme	nt grea	ater than 2	minutes 👻	Adjust Sys	tem Time ,
V Automatical	y Chec	k For Updates every	7 day(s)	Check Now	
Logging Level:	Norm	nal 👻 Vie	ew		

Ajustes de seguridad

Cambiar políticas de complejidad de password

samba-tool domain passwordsettings set --complexity=off samba-tool domain passwordsettings set --min-pwd-length=5 samba-tool domain passwordsettings set --history-length=0 samba-tool domain passwordsettings set --min-pwd-age=0 samba-tool domain passwordsettings set --max-pwd-age=0

Para ver las políticas actuales.

samba-tool domain passwordsettings show



Cambiar la clave de Administrator

samba-tool user setpassword administrator

Agregar permisos administrativos varios al grupo Domain Admins

net rpc rights grant 'SIENIC\Domain Admins' SeMachineAccountPrivilege SePrintOperatorPrivilege SeAddUsersPrivilege SeDiskOperatorPrivilege SeRemoteShutdownPrivilege -Uadministrator



Para listar los permisos asignados escribimos

net rpc rights list accounts -Uadministrator

Cuenta administradora de dominio alterna.

Se recomienda crear una cuenta administradora alterna que pertenezca únicamente al grupo Domain Admins y desde esta cuenta administrar los recursos compartidos, políticas de seguridad y unir máquinas, esto se puede hacer desde RSAT en Windows, para más información de RSAT pasar a la sección Herramientas de administración remota del servidor para Windows en la pagina.

Configurando el servicio samba

Configurando el servicio samba

El siguente paso es configurar el servicio samba para que arranque automaticamente con el servidor, asi como poder detenerlo, reiniciarlo y arrancarlo, para esto creamos un archivo de texto con el nombre samba.service en la ruta /usr/lib/systemd/system/ con el siguiente contenido.

```
[Unit]
Description=Samba AD Daemon
After=syslog.target network.target
```

```
[Service]
Type=forking
PIDFile=/usr/local/samba/var/run/samba.pid
LimitNOFILE=16384
EnvironmentFile=-/etc/sysconfig/samba
ExecStart=/usr/local/samba/sbin/samba $SAMBAOPTIONS
ExecReload=/usr/bin/kill -HUP $MAINPID
```

```
[Install]
WantedBy=multi-user.target
```

Luego ejecutamos el siguiente comando

ln -s /usr/lib/systemd/system/samba.service /etc/systemd/system/samba.service

ahora procedemos a habilitar el servicio

systemctl enable samba

Ahora para administrar el servicio usaremos los siguientes comandos:

Detener el servicio.

systemctl stop samba.service

Arrancar el servicio.

systemctl start samba.service

Reiniciar el servicio.

systemctl restart samba.service

Ver estado del servicio.

systemctl status samba.service

Compartiendo Archivos

Compartir archivos

Para compartir una carpeta en red es necesario crear la carpeta y asignarle los siguientes permisos, en este ejemplo el nombre de la carpeta es datos, cabe mencionar que el sistema de archivos que tiene la partición donde vamos a compartir los archivos esta formateada con el sistema de archivos XFS.

chown root:root datos

Si no le ponemos como propietario root:root en las propiedades en lugar de administrator va a salir cuenta desconocida.



Luego le damos los permisos necesarios.

chmod 777 datos

Si no le damos los permisos 777 y en su lugar le damos algo como 775 no nos permitirá hacer modificaciones a los permisos de configuración de seguridad avanzada.



Luego editamos el archivo /usr/local/samba/etc/smb.conf y creamos la sección del recurso compartido, en adelante todos los permisos se van a administrar desde un equipo con Windows con una cuenta administrativa de dominio.

[Datos]

```
path = /home/eduardo/datos/
```

read only = no

Luego ejecutamos el comando.

smbcontrol all reload-config

Este comando hace que se vuelva a leer la configuración del archivo smb.conf para que se hagan efectivos los cambios.

Modificar los permisos del recurso compartido.

En una pc con Windows nos vamos a **Administración de equipos/Acción/Conectar con otro equipo** y en el cuadro de dialogo ponemos el IP del servidor y luego damos clic en **aceptar**.

• 🔿 🔲 🗟 🛛 🖸			
Administración del equ	po (loc Nombre		
Herramientas del sis	ema 🛛 👔 Herramientas de	el sistema	
Programador de Visea de supertos	tareas 🛛 🔠 Almacenamient	o	
b Carnetas compa	tidas 📗 📠 Servicios y Aplic	aciones	
Seleccionar equipo			8
Seleccionar equipo Seleccione el equipo que Este complemento siem C Equipo local: (el eq	desea administrar con este com re administrará: jipo en el que se está ejecutano	plemento. do esta consola)	8
Seleccionar equipo Seleccione el equipo que Este complemento siem C Equipo local: (el eq C Otro equipo:	desea administrar con este com re administrará: iipo en el que se está ejecutano 192:168.0.20	plemento. do esta consola)	Examinar

Luego nos vamos a Herramientas del sistemas/Carpetas compartidas/Recursos compartidos y seleccionamos la carpeta que configuramos en el servidor le damos con el boton secundario del mouse y seleccionamos propiedades, una vez en propiedades podemos configurar los permisos en las solapas "Permisos de los recursos compartidos" y "Seguridad".

Administración de equipos Archivo Acción Ver Ayuda Archivo Acción Ver Ayuda Administración de equipos (19. Administración de equipos (19. Administración de equipos (19. Administración de equipos (19. Programador de tareas Visor de eventos Carpetas compartidas Recursos compartid Sesiones	Nombre del r Datos Datos IPCS R netlogon Sysvol	Propiedades: Datos General Publicar Permisos de los re- Nombres de grupos o usuarios: Domain Admins (SIENIC\Domain Domain Users (SIENIC\Domain N	Cursos compartidos Seguridad Admins) Users)
 Sesiones Archivos abiertos Rendimiento Administrador de dispo Almacenamiento Servicios y Aplicaciones 		Permisos de Domain Admins Control total Cambiar Leer <u>Obtener más información acerca de co</u> Acep	Agregar Quitar Pemitir Denegar V V V Ontrol y pemisos de acceso tar Cancelar Aplicar

Nota: Para realizar estos cambios la maquina debe estar unida al dominio y la sesion debe ser con una cuenta administrativa.

Configurando el Firewall

Abrir los puertos correspondientes en el firewall

Yast/Seguridad y usuarios/Cortafuegos.



Servicios autorizados y de la lista desplegable seleccionamos Servidor de Netbios y hacemos clic en Añadir

Inicio Interfaces Servicios autorizados Enmascaramiento	Configuración del cortafue Servicios aut <u>o</u> rizados para la zona selecciona	egos: Servicios
Difusión Nivel de registro Reglas personalizadas	Zona externa <u>S</u> ervicio que se va a autorizar	•
	Cliente NFS	• Añadir
	DNS de Multidifusiónst) Zeroconf/Bonjour dnsmasq dnsmasq (dnsmasq-dns) MySQL server PulseAudio server (TCP)	Elimina <u>r</u>
	Servidor de Netbios Servidor DHCP Servidor mini-HTTP de VNC Servidor Rsync Servidor Samba	•

Despues hacemos clic en **opciones avanzadas**.

 Inicio Interfaces Servicios autorizados Enmascaramiento 	Configuración del cortafuegos: Servicio Servicios aut <u>o</u> rizados para la zona seleccionada	s autc
- Difusión - Nivel de registro - Reglas personalizadas	Zona externa 🔹	
	Servicio que se va a autorizar	
	Cliente NFS Añac	lir
	Servicio autorizado i descripción bind DNS server Open ports for the bind DNS	ia <u>r</u>
	Servidor de Netbios Opens ports for Samba Netbi	
	•	
	Proteger cortafuegos de la zona interna Opciones ava	anza <u>d</u> as

Y procedemos a abrir los siguientes puertos

Puertos TCP

1024:5000 135 139 389 445 464 5353 636 88

Puertos UDP

123 389 464 5353 88

Introduzca aquí los puertos o	Puertos autorizados adicionales
protocolos adicionales que desee habilitar en la zona de cortafuegos.	Configuración para la zona: Zona externa
Los Puertos TCP y los Puertos	1024:5000 135 139 389 445 464 5353 636 88
una lista de números de	Puertos UDP
rangos de puertos separados	389 464 5353 88
por espacios, como 22, http o 137:139.	Puertos <u>R</u> PC
Puertos RPC es una lista de los servicios RPC, como nlockmgr, ypbind o portmap, separados por espacios.	Protocolos <u>I</u> P
Protocolos IP es una lista de protocolos, como esp, smp o chaos, separados por espacios.	<u>A</u> ceptar <u>C</u> ancelar

Hacemos clic en Aceptar/Siguiente/terminar.

 No hay interf 	faces asignadas a esta zona.	
Zona extern	าล	
Interfaces	0	
∘82545	EM Gigabit Ethernet Controller (Copper) / en	016777736
Servicios,	puertos y protocolos abiertos	
∘ Servid ∘ bind D ∘ Puerto 88 ∘ Puerto	or de Netbios NS server os TCP: 1024:5000, 135, 139, 389, 445, 464, os UDP: 123, 389, 464, 5353, 88	5353, 636,

Uniendo estaciones de trabajo al dominio

Unir las estaciones de trabajo al nuevo dominio.

Para unir una maquina al dominio lo primero que hay que hacer es configurar una ip que este dentro de la red en la estacion de trabajo, para ello damos clic derecho sobre el icono de la red y seleccionamos **Abrir el centro de redes y recursos compartidos**.



Luego damos clic en Cambiar configuracion del adaptador.



Seleccionamos el adaptador que vamos a usar y le damos clic con el boton secundario del mouse y seleccionamos **Propiedades**



En este cuadro seleccionamos Protocolo de internet version 4 y le damos clic en propiedades.



Luego llenamos los datos con los numero ip que correspondan a la red, en Direccion IP ponemos una direccion IP que este libre en la red, en mascara de subred ponemos la que corresponda a la red, en puerta de enlace ponemos la direccion del router y en DNS nos aseguramos de poner la direccion IP del servidor samba y le damos **aceptar**.

eneral	
Puede hacer que la configuración IP se red es compatible con esta funcionalidar consultar con el administrador de red cu apropiada.	asigne automáticamente si la J. De lo contrario, deberá ál es la configuración IP
🔘 Obtener una dirección IP automáti	camente
Osar la siguiente dirección IP:	
Dirección IP:	192 . 168 . 0 . 35
Máscara de subred:	255.255.255.0
Puerta de enlace predeterminada:	192.168.0.1
Obtener la dirección del servidor D	NS automáticamente
-) Usar las siguientes direcciones de s	servidor DNS:
Servidor DNS preferido:	192 . 168 . 0 . 20
Servidor DNS alternativo:	· · ·

El siguiente paso es unir la maquina al dominio para esto no vamos a **Inicio** y le damos clic con el boton secundario del mouse a **Equipo** y luego seleccionamos **propiedades**.



En la siguiente pantalla damos clic en **Cambiar configuracion**, despues en el siguiente cuadro de dialogo seleccionamos **Cambiar**... y en el siguiente cuadro en el campo **Dominio** ponemos el nombre del dominio y damos clic en **aceptar**, nos va a pedir las credenciales de una cuenta administrativa con permisos para agregar maquinas al domino, introducimos los datos y damos clic en **aceptar**

V Cambios en el don Puede cambiar el n	Seguridad de Windows Cambios en el dominio o el nombre Escriba el nombre y la contraseña de una cuen al dominio.	e del equipo ta con permiso para unirse	emoto
Cambios podrian ar Cambios podrian ar información Nombre de equipo: EASGS-PC05 Nombre completo d SI EASGS-PC05	Supervisor 	Aceptar Cancelar	2.99 GHz
Miembro del Dominio: sienic Grupo de tra WORKGRO	Aceptar Cancelar	a or commo o Id. de red de red. quipo o cambiar el Cambiar	Cambiar configuración
Centro de actividades Windows Update		Aceptar Cancelar /	Aplicar

Nos mostrara un cuadro informativo que la maquina se a unido al dominio exitosamente

Nombre de equipo:			
EASGS-PC05		"Equipo de María".	
Nombre completo de equipo:		EASGS-PC05	2.99 GHz
EASGS-PC05	Cambios en el dom	inio o el nombre del equipo 🛛 💽	
Miembro del	Se unió	correctamente al dominio sienic.	para esta pantalla
sienic		ar	
Crupo de trabajo: WORKGROUP		Aceptar	Cambiar configuración
	ceptar Cancelar		
tro de actividades	A L		
dows Update		Aceptar Cancelar Aplicar	ida software

El siguiente cuadro nos dice que tenemos que reiniciar la maquina para que los cambios surtan efecto.

Nombre de equipo: EASGS-PC05	Cambios en el dominio o el nombre del equipo o	
Nombre completo de equipo: EASGS-PC05	Debe reiniciar el equipo para aplicar los cambios.	2.99 GHz
Miembro del	cierre todos los programas.	para esta pantalla
Ominio:	(Accessed)	
sienic	Aceptar ar	(Compliant)
🔘 Grupo de trabajo:		configuració
WORKGROUP		conniganacio

Cuando reinicie la maquina le damos clic en cambiar de usuario



Damos clic en otro usuario.



Introduciomos los datos del usuario de dominio y damos enter.

superv	isor
•••••	••••
ómo pi	Iniciar sesión en: SIENIC uedo iniciar sesión en otro dominio?

Con esto ya hemos iniciado sesion dentro del dominio



Usando las RSAT (Remote Server Administration Tools)

Herramientas de administración remota del servidor para Windows

La administracion de Usuarios y Grupos, Unidades organizativas, Directivas de grupo, DNS y recursos compartidos entre otros pueden hacerse desde una estacion de trabajo con Windows XP/Vista/7/8/8.1 instalado, para esto se deben descargar e instalar las Herramientas de administración remota del servidor para Windows, estas se pueden descargar de los siguientes enlaces:

- <u>http://www.microsoft.com/downloads/details.aspx?FamilyId=9FF6E897-23CE-4A36-B7FC-D52065DE9960&displaylang=en</u> (Vista)
- <u>http://www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en</u> (Windows 7)
- <u>http://www.microsoft.com/download/details.aspx?id=28972</u> (Windows 8)
- <u>http://www.microsoft.com/en-us/download/details.aspx?id=39296</u> (Windows 8.1)

La instalacion es como cualquier otro paquete de windows, una vez instaladas las herramientas hay que habilitarlas, para eso nos vamos **a panel de control/Programas/Activar o desactivar las características de Windows** y seleccionamos las opciones a como se muestra en las siguientes imágenes.



tivar o desactivar las caracter	rísticas de Windows	1
ra activar una característica, active la ca silla. Una casilla rellena indica que sólo	asilla correspondiente. Para desactivarla, desactive está activada una parte de la característica.	la
🗾 🔒 Herramientas de admin	istración de directivas de grupo	
📃 📗 Herramientas de almac	enamiento del Explorador	
🗐 📗 Herramientas de clúster	r de conmutación por error	
🔲 🔒 Herramientas de equilib	orio de carga de red	
🔲 🔒 Herramientas del admir	nistrador de recursos del sistema de Windows	
🗐 📗 Herramientas del servid	lor SMTP	
🔲 🔒 Visor de contraseñas de	e recuperación de BitLocker	
🖃 🔲 📗 Herramientas de administra	ación de funciones	
🖃 🔳 🔒 Herramientas de AD DS	y AD LDS	
🖃 🔲 📗 Herramientas de AD	DS	
🔽 🍌 Centro de admir	nistración de Active Directory	
🔽 🌡 Herramientas de	e línea de comandos y complementos de AD DS	
📰 🎳 Herramientas de	el Servidor para NIS	
🔳 Herramientas de lín	ea de comandos y complementos de AD LDS	
🔽 🍌 Módulo de Active D	Directory para Windows PowerShell	
🔲 🔒 Herramientas de Hyper	-V	
🕀 🔲 📔 Herramientas de Servici	ios de archivo	
🕀 🔲 📙 Herramientas de Servici	ios de certificados de Active Directory	
🔲 📗 Herramientas de Servici	ios de Escritorio remoto	
🔲 🔒 Herramientas del servid	lor DHCP	
🛛 🎉 Herramientas del servid	lor DNS	
Internet Explorer 8		

Una vez habilitadas las funciones presionamos la tecla Windows + R y escribimos mmc

	recurso de Inte	ibre del prog ernet que de	jrama, carpet sea abrir con	a, document Windows.	00
brir:	mmc				•

En el siguiente cuadro de dialogo le damos clic en "Si"


En la Raiz de consola damos clic en Archivo/agregar o quitar complemento.

Ar	chivo Acción Ver Favoritos	Ventana	Ayuda
4	Nuevo	Ctrl	+N
1	Abrir	Ctrl	+0
	Guardar	Ctrl	+ S
	Guardar como		
	Agregar o quitar complemento Opciones	Ctrl+	M
	1 C:\Users\\servermanagement		
	2 dsa		
	3 C:\Users\\servermanagement		
	4 compmgmt		
	Salir		

Seleccionar Administracion de directivas de grupo, DNS y Usuarios y equipos de Active Directory y le damos clic en aceptar.

omplemento Firewall de Windows con segurid	Prove	*		Raíz	de cons Idministr	ola ación de dire	ctivas de gruț	Editar extensiones
Monitor de rendimiento Monitor de seguridad IP	Micro				ISUARIOS	y equipos de	Active Direct	Quitar
Plantillas de seguridad Programador de tareas	Micro Micro							Subir
Servicios Servicios de componentes	Micro Micro	4	Agregar >					Bajar
Sitios y servicios de Active Direct Usuarios y equipos de Active Dir	Micro Micro							
Usuarios y grupos locales Vincular a dirección web	Micro Micro	н						
Visor de eventos	Micro	-						<u></u>
III	•							Opciones avanzadas.



Desde esta consola podremos administrar todas las funciones mencionadas anteriormente.



Para administrar el DNS del servidor damos clic derecho sobre la opcion **DNS** y seleccionamos **Conectar con el servidor DNS**.

	Conectar con el servidor DNS	
	Todas las tareas	×
4 3	Ver	÷
E.	Nueva ventana desde aquí	
	Nueva vista del cuadro de tareas	
9	Actualizar	
•	Avuda	

En el siguiente cuadro de dialogo seleccionamos la opcion "**El Siguiente equipo**" y escribimos la direccion IP del servidor samba y damos clic en **aceptar**.

escritorio	Conectar a servidor DNS	
 Contabilidad Domain Contro Objetos de dires Filtros WMI GPO de inicio Sitios 	El servidor DNS de Windows se está ejecutando en: O Este equipo El siguiente equipo: 192, 168.0.20	
 Modelado de directivas Resultados de directiva DNS Usuarios y equipos de Active [Conectarse a este equipo ahora	Cancelar

Una vez realizada la conexión podremos administrar el servidor DNS desde la RSAT



Cuando cerremos la consola no preguntara si deseamos guardar, le damos clic en si.



Le ponemos un nombre descriptivo y la guardamos en el escritorio.

	ᡖ Guardar como					.
	Guardar en:	Escrito	rio		G 🕸 📂 🖽 -	
⊳ 📫 ⊳ 🙀 Sitios № Mode 🧖 Result	Sitios recientes		Bibliotecas Carpeta de sistema	13	Supervisor Carpeta de sisten	na
 ▲ BNS ▲ 192.168.0. ▶ 192.168.1 	Escritorio		Equipo Carpeta de sistema		Red Carpeta de sisten	na
⊿ 🧰 Zonas ⊳ 😭 sie ⊳ 😭 _m	Bibliotecas					
▷ 2 Zonas □ Zon	Equipo					
⊿ 🚑 sienic.site 🚆 Users ⊳ 🛄 Comp	Red					
⊳ 🦳 Builtir ⊳ 💼 Doma ⊳ 🦳 Foreig		Nombre: Tipo:	serveradmin Archivos de Microsoft I	Management Consc	▼ ble (*.msc) ▼	Guardar Cancelar

Ahora con solo dar clic en el icono podremos acceder a las opciones de administracion del servidor previamente configuradas.



Creando cuenta administradora de dominio alterna.

Para crear un usuario administrador alterno nos vamos a **Usuarios y equipos de Active Directory/sienic.site** damos clic derecho en **Users** seleccionamos **Nuevo/Usuario**.



Llenamos los datos Nombre de pila, Nombre completo y nombre de inicio de sesion de usuario y clic en **siguiente**.

Image: Second state Image: Secon	Nuevo objeto: Usuario	sienic.site/U	sers		
ForeignSecurityPrincipal	Nombre de pila:	Supervisor	In	niciales:	
	Nombre completo:	Supervisor			
	Supervisor	sesion de usuan	e. @sienic.site	•	
	Nombre de inicio de	sesión de usuari	o (anterior a Windo	ows 2000):	
	SIENIC		Supervisor		
			< Atrás	iguiente > Cancel	lar

Ponemos la clave y dejamos las demas opciones a como se muestra en la siguiente imagen y clic en **siguiente**.

Contraseña:	•••••
Confirmar contraseña:	•••••
🗌 El usuario debe cambi	iar la contraseña en el siguiente inicio de sesión
📄 El usuario no puede c	ambiar la contraseña
📄 La contraseña nunca	expira
La contraseña nunca La cuenta está desha	expira bilitada
La contraseña nunca	expira

Una vez creado el usuario lo seleccionamos y le damos clic con el boton secundario del mouse y seleccionamos **Propiedades**



Seleccionamos la solapa **Miembro de** y lo hacemos miembro del grupo "Domain Admins" unicamente y le damos clic en **aceptar**.

General	Dirección	Cuenta	Perfil	Teléfonos
Organiz	ación	Miembro de		COM+
Miembro de:				
Nombre	Carpeta de	e los Servicios de d	ominio de <mark>Ac</mark> tive	e Dir
Domain Adm	ins sienic.site/	/Users		
Aaregar	Quitar	6		
Agregar	Quitar	Î		
Agregar	Quitar	ns		
Agregar	Quitar	ns No es necesario ca	ambiar Grupo prir	ncipal
Agregar Grupo principa Establecer	Quitar	ns No es necesario ca sí no tiene clientes aolicaciones como	ambiar Grupo prir de Macintosh o tribles con POS	ncipal

El proceso es similar para cualquier tipo de usuario excepto la parte donde lo hacemos miembro de un grupo ya que los grupos deben corresponder a los privilegios de cada usuario.

Creando Grupos de Seguridad.

Para crear un grupo nos vamos a **Usuarios y equipos de Active directory/Users** damos clic con el boton secundario seleccionamos **Nuevo/Grupo**.



Ponemos nombre al grupo y en ambito seleccionamos **Global** en tipo de grupo seleccionamos **Seguridad**.

Paíz de con	Nuevo objeto: Grupo		
Admini Admini DNS	🥵 Crear en: sienie	.site/Users	
D 📔 Con	Nombre de grupo:		
⊿ 📰 sien	Logistica		
Þ 🛄	Nombre de grupo (anterior a	Windows 2000):	
	Logistica		
	Ámbito de grupo	Tipo de grupo	
	🔘 Dominio local	Seguridad	
	Global	🔘 Distribución	
	🔘 Universal		

Damos clic en **aceptar** y con esto ya tenemos creado el grupo de seguridad.



Agregando usuarios a un grupo de seguridad.

Para agregar usuarios a un grupo de seguridad damos clic con el boton secundario del mouse sobre el grupo de seguridad y damos clic en **propiedades**, en el cuadro de propiedades seleccionamos la solapa **Miembros** y damos clic en **agregar**.

opieuau	ies. Logisti	.0		
General	Miembros	Miembro de	Administrado por	
Miembro	DS:			
Nomb	re	Carpeta de	los Servicios de dominio de J	Active Dir
Agre	gar)	Quitar		
			Aceptar Cancel	lar Aplicar

En el siguiente cuadro vamos escribiendo los nombre de usuarios que van a pertenecer al grupo y vamos dando clic en **comprobar nombre.**

Usuarios, Cuentas de <mark>s</mark> ervicio, Grupos, o Otros objetos	Tipos de objeto
Desde esta ubicación:	
sienic.site	Ubicaciones
<u>E</u> scriba los nombres de objeto que desea seleccionar (<u>ejemplos</u>):	
easgs03 (easgs03@sienic.site); easgs04 (easgs04@sienic.site); easgs05 (easgs05@sienic.site) easgs06	Comprobar nombre
easdson (easdson)@sieriic.siteT easgson	

Cuando ya tengamos a todos los usuarios requeridos damos clic en aceptar.

Usuarios, Cuentas de servicio, Grupos, o Otros objetos	Tipos de objeto
Desde esta ubicación:	
sienic.site	Ubicaciones
Escriba los nombres de objeto que desea seleccionar (<u>ejemplos</u>):	
easgs03 (easgs03@sienic.site); easgs04 (easgs04@sienic.site); easgs05 (easgs05@sienic.site); easgs06 (easgs06@sienic.site)	Comprobar nombres
easqsub (easqsub@sienic.site); easqsub (easqsub(@sienic.site))	

En el siguiente cuadro damos clic en aceptar.

General Miembros	Miembro de Administrado por	
Miembros:		
Nombre	Carpeta de los Servicios de dominio de Active Dir	
<pre>& easgs03 & easgs04 & easgs05 & easgs06</pre>	sienic.site/Users sienic.site/Users sienic.site/Users sienic.site/Users	
	Quitar	
Agregar		

Creando unidades organizativas.

Para crear una unidad organizativa, nos vamos a **Usuarios y equipos de Active Directory** y damos clic con el boton secundario del mouse sobre el dominio, seleccionamos **Nuevo/Unidad Organizativa.**



Ponemos un nombre descriptivo a la Unidad organizativa y damos clic en aceptar.

Nuevo o	bjeto: Unidad organizativa
2	Crear en: sienic.site/
Nom	re:
Logi	tica
Pi	oteger contenedor contra eliminación accidental

Ahora la nueva unidad organizativa se mostrara dentro del dominio.



Mover un Grupo a una Unidad Organizativa.

Damos clic con el boton secundario del mouse sobre el grupo que queremos agregar a la unidad organizativa y seleccionamos **Mover**.



En el siguiente cuadro seleccionamos la Unidad Organizativa a la que queremos mover el grupo y clic en **aceptar**.



Con esto el grupo aparecera en el active directory dentro de la unidad organizativa seleccionada



El procedimiento es el mismo para un usuario tambien podemos arrastar los objetos.

Creando GPO para restringir el uso del panel de control

Para crear una GPO nos vamos a Administracion de directivas de grupo, nos vamos al dominio y hacemos clic con el boton secundario del mouse sobre la unidad organizativa a la que vamos a aplicar la politica de seguridad, en el menu seleccionamos **Crear un GPO en este dominio y vincularlo aquí.**



Ponemos un nombre descriptivo a la nueva politica de grupo y damos clic en aceptar.

and server adminit " [Raiz de consola Adminit" [Raiz de consola Adminit" [Raiz de consola Adminit	os Ventana	Ayuda
📔 Raíz de consola		Logistica
Administración de directivas de A Posque sienis site	e grupo	Objetos de directiva de grupo vinculados Herencia de directivas
Dosque: sienic.site Dominios Pi sienic.site Default Domain Default Domain Doctabilidad	Policy	Orden de vínculos GPO E
 Domain Contro Logistica Obietee de dies 	Nombre:	
Distribution of the second	Bloquear Par	nel
GPO de inicio	GPO de inicio	de origen:
Sitios	(ninguno)	▼
Resultados de directiva		Aceptar Cancelar

En el panel derecho damos doble clic sobre la nueva politica.



Nos va a aparecer un aviso como el de la siguiente imagen damos clic en aceptar.



Aquí podemos ver que en **filtrado de seguridad** por default nos aparece el grupo Authenticated Users, pero digamos que queremos que esta GPO se aplique a otro grupo, entonces seleccionamos el grupo y damos clic en **quitar**.

📷 serveradmin - [Kaiz de Consola/Administración	ae airectivas ae grupo\Bosque: sienic.site\Dominios\sienic.site\Logistica\Blo. Ayuda	
🏅 🔿 🖄 📰 🙆 🛛		
Raíz de consola	Bloquear Panel Ambito Detalles Configuración Delegación	Acciones Bloquear P
 A Bosque: sienic.site B Dominios Sienic.site Default Domain Policy 	Vínculos Mostrar vínculos en esta ubicación:	Accio
😰 Contabilidad ⊳ 😰 Domain Controllers ⊿ 😰 Logistica	Ubicación Exigido Vínculo habili Logistica No Sí	
😹 Bloquear Panel Þ 🎯 Objetos de directiva de gru Þ 👺 Filtros WMI	× •	
▷ i GPO de inicio	Filtrado de seguridad La configuración en este GPO sólo se puede aplicar a los grupos, usuarios y equip Nombre	
Resultados de directivas de grupo B DNS Usuarios y equipos de Active Directory [sr	& Authenticated Users	
 Consultas guardadas isienic.site Users 	Agregar Quitar Propiedades	
▷ Computers ▷ Computers ▷ Computers ▷ Computer Controllers	Filtrado WMI Este GPO está vinculado al siguiente filtro WMI:	
EnreignSecurityDringinals	Abrir	_

En el cuadro de dialogo de confirmacion damos clic en aceptar.

 serveradmin - [Raíz de consola\Administración d Archivo Acción Ver Favoritos Ventana Archivo I (2) 	de directivas de grupo\Bosque: sienic.site\Dominios\sienic.site \Logistica\Blo Ayuda	- 6 X
Raíz de consola	Bloquear Panel	Acciones
Administración de directivas de grupo A Bosquer sienic site	Ambito Detalles Configuración Delegación	Bloquear P 🔺
 ▲ Bosque stencsite ▲ Dominios ▲ ¥ sienic.site 	Vínculos Mostrar vínculos en esta ubicación: sienic.site	Accio 🕨
Default Domain Poli Adminis	stración de directivas de grupo	
 Contabilidad Domain Controllers Cogistica Bloquear Panel Objetos de directiva 	¿Desea quitar este privilegio de delegación?	
 Filtros WMI GPO de inicio Gitos 	Aceptar Cancelar grupos, usuarios y equir	
Modelado de directivas de grupo	Nombre Read Authenticated Users	
Ostarios y equipos de Active Directory [si Consultas guardadas	4	
⊿ ﷺ sienic.site ☐ Users	Agregar Quitar Propiedades	
Computers Computers	Filtrado WMI Este GPO está vinculado al siguiente filtro WMI: <ninguno> Abrir </ninguno>	

Ahora que hemos removido el grupo por default debemos agregar el grupo al que queremos aplicar la politica, damos clic en **agregar** y escribimos el nombre del grupo deseado luego damos clic en **comprobar nombre** y finalmente clic en **aceptar**.

Archivo Acción Ver	Favoritos Ventana Ayuda		
Þ 🔿 🔁 🖬 🙆			
🗎 Raíz de consola	A Bloquear Panel		
Administración de A Bosque: sienic.s	Seleccionar Usuario, Equipo o Grupo		? <mark>- × -</mark>
a 😭 Dominios	Seleccionar este tipo de objeto:		
a 🚔 sienic.sit	Usuario, Grupo, o Entidad de seguridad integrada	Tipos de	e objeto
Defa	Desde esta ubicación:		
⊳ 🛱 Dom	sienic.site	Ubicad	ciones
a 📴 Logi:	Escriba el nombre de obieto para seleccionar (ejemi	plos):	
B	Logistica	Comprobr	ar nombres
⊳ iltra		<u></u>	
D 🛅 GPO	1		
Sitios	Opciones avanzadas	Aceptar	Cancelar
🙀 Modelado d			al
Resultados de	directivas de grupo		
DNS DNS	e Active Directory for		
a suanos y equipos o b Consultas guarda	das	m	
⊿ 🚔 sienic.site			Propiodados
📑 Users	Agregar		riopieuades

Ahora ya nos aparece reflejado el grupo deseado.

serveradmin - [Raíz de consola\Administración	de directivas de grupo\Bosque: sienic.site\Dominios\sienic.site \Logistica\Blo	
	Аубиа	×
Raíz de consola	Bloquear Panel	Acciones
Administración de directivas de grupo	Ambito Detalles Configuración Delegación	Bloquear P 🔺
Bosque: sienic.site	Vinculos	Accio 🕨
A 🛱 sienic.site	Mostrar v ínculos en esta ubicación: sienic site	100 March 100 March 100
Default Domain Policy Contabilidad	Los siguientes sitios, dominios y unidades organizativas están vinculados a este G	
Domain Controllers	Ubicación Exigido Vínculo habili	
⊿ 📴 Logistica 🛒 Bloquear Panel	Logistica No Sí	
 Objetos de directiva de gru Filtros WMI Go de directiva 	Image: State of the second dial	
GPU de micio	Hitrado de segundad	
Modelado de directivas de grupo	Nombre	
A Structure de ancernos de grupo A DNS Usuarios y equipos de Active Directory (sr	Logistica (SIENIC\Logistica)	
Consultas guardadas	K	
⊿ 🚔 sienic.site ── Users	Agregar Quitar Propiedades	
▷ Computers ▷ Builtin	Filtrado WMI Este GPO está vinculado al siguiente filtro WMI:	
Domain Controllers Consign Security Principals	Abrir	

Ahora para configurar la nueva politica le damos clic con el boton secundario del mouse y seleccionamos **editar**.

serveradmin - [Raíz de consola\Administración	de directivas de grupo\Bosque: sienic.site\Dor	ninios\sienic.sit	e \Logistica\Blo	
🖀 Archivo Acción Ver Favoritos Ventana 🧇 🔿 🖄 📰 💥 💁 🔝	Ayuda			_ 8 ×
 Raíz de consola Administración de directivas de grupo 	Bloquear Panel Ambito Detalles Configuración Delegación	1		Acciones Bloquear P 🔺
 Administración de directivas de grupo A Bosque: sienic.site Bominios Sienic.site Default Domain Policy Contabilidad Demain Controllers 	Vínculos Mostrar vínculos en esta ubicación: sienic.s Los siguientes sitios, dominios y unidades organ	ite nizativas están vin Evinido	▼ Iculados a este G Vínculo babili	Accio 🕨
Domain Controllers Dogistica	Logistica	No	Sí	
S Dict Editar Dict Editar Dict Editar Filtros V Exigido Dict Editar Dict Editar Dict Editar Dict Editar Vinculo habilities	ado		•	

En el editor de administracion de directivas de grupo nos vamos a **Configuracion de usuario/Directivas/Plantillas administrativas/Panel de control** y en el panel derecho le damos doble clic a la opcion **Prohibir el acceso al panel de control**.



En la siguiente ventana seleccionamos Habilitada y damos clic en aceptar.

🍨 Prohibir el acceso al P	anel de control		3
Prohibir el acceso al	^p anel de control	Valor anterior Valor siguiente	
 No configurada Habilitada 	omentario:		
Deshabilitada			
- 0	ompatible con:	Al menos Windows 2000	њ. т
Opciones:		Ayuda:	
		Deshabilita todos los programas del Panel de control. Esta opción impide que Control.exe, el archivo de programa del Panel de control, se inicie. En consecuencia, los usuarios no pueden iniciar el Panel de control ni ejecutar los elementos de éste. Además, esta opción quita el Panel de control del menú Inicio. Esta opción también quita la carpeta Panel de control del Explorador de Windows. Si los usuarios intentan seleccionar un elemento del Panel de control desde la opción Propiedades de un menú contextual, aparece un mensaje que explica que una opción de configuración impide dicha acción.	*
		Aceptar Cancelar Aplicar	

Crear una GPO para restringir el acceso al regedit.

Para crear una GPO para restringir el acceso al registro de Windows seleccionamos la OU a la que deseamos aplicar la politica y le damos clic con el boton secundario del mouse, luego seleccionamos **Crear un GPO en este dominio y vincularlo aquí.**



En el siguiente cuadro le ponemos un nombre descriptivo para tener una referencia clara de lo que hace la politica y damos clic en **aceptar**.

serveradmin - [Raíz de consola\Adm	ninistración d	e directiva	s de grupo\Bosque: sienic.site	Dominios\sienic.site	\Logisti	ca] 🕞 🗗	23
Archivo Acción Ver Favorito	s Ventana	Ayuda				- 6	5 ×
🗢 🔿 🖄 🖬 📋 🗙 🗟 🧔	? 🗊						
📔 Raíz de consola	*	Logisti	ca			Acciones	
Administración de directivas de	grupo	Objetos	de directiva de grupo vinculados	Herencia de directivas	s 4 >	Logistica	
 Dosque: sienc.sice Social de la contractiona de la contractione 			Orden de vínculos	GPO	E	Acciones adici	. •
⊿ 🚔 sienic.site 📓 Default Domain P	olicy	8	1 2	🚮 bloqueo de red 🚮 Bloquear panel	N N		
▷ in Contabilidad ▷ in Control ▷ in Control	Nuevo GPO			×			
 Dijetos de dire Citara MAN 	Nombre: bloqueo regis	tro					
Filtros WMI GPO de inicio	GPO de inicio	de origen:					
Modelado de directiva	(ninguno)						
Resultados de directiva			Aceptar	Cancelar			

En la lista de GPO asignados a esta OU hacemos doble clic sobre la GPO recien creada.



En esta pantalla nos aseguramos que en **filtrado de seguridad** este el grupo al que deseamos aplicar la politica.

🚡 Archivo Acción Ver Favoritos Ventana	Ayuda		
🖮 🐟 📶 💽 💽 🛸			
 Raíz de consola Administración de directivas de grupo 	bloqueo registro		
 Bosque: sienic.site Bosque: sienic.site 	Ambito Detalles Configuración Delegación Vínculos		
 sienic.site Default Domain Policy 	Mostrar v ínculos en esta ubicación: sienic.site Los siguientes sitios, dominios y unidades organiza	tivas están vin	▼ culados a
Contabilidad Domain Controllers	Ubicación	Exigido	Vincul
⊿ 📴 Logistica 🛒 Bloquear panel	Dogistica	No	Sí
🗟 bloqueo de red			F
 Image: Objetos de directiva de gru Image: Filtros WMI Image: Objetos de directiva de gru 	La configuración en este GPO sólo se puede aplic	ar a los <mark>g</mark> rupos	, usuarios
 Image: Second elinicity Image: Sitios Image: Modelado de directivas de grupo 	Nombre & Logistica (SIENIC\Logistica)		
Resultados de directivas de grupo	۰. m		Þ
Usuarios y equipos de Active Directory [sr b Consultas quardadas	Agregar Quitar	Propiedad	es

Ahora seleccionamos la GPO y le damos clic con el boton secundario del mouse y seleccionamos **editar.**

 serveradmin - [Raíz (co Archivo Acción Ver Archivo Acción Ver Archivo Acción Ver Archivo Acción Ver Raíz de consola Administración de dir A Bosque: sienic.site Boninios M sienic.site 	Editar Exigido Vínculo habilitado Guardar informe Ver Nueva ventana desde aquí	a
 ☑ Default ☑ Contab ☑ Domain ☑ Logistic ☑ Bloc ☑ bloc ☑ bloc 	Nueva vista del cuadro de tareas Eliminar Cambiar nombre Actualizar Ayuda	05

En el editor de politicas de grupo nos vamos a **configuracion de usuario/Preferencias/Configuracion de Windows/Registro**, hacemos clic con el boton derecho sobre este ultimo y seleccionamos **Nuevo/elemento del registro**.



En la siguiente ventana en subarbol seleccionamos HKEY_CURRENT_USER y en ruta de la clave nos vamos a Software\Microsoft\Windows\CurrentVersion\Policies y al final agregamos System

Editor de administración de direc	ctivas de grupo			
Archivo Acción Ver Ayuda				
🧢 🔿 🖄 🖬 🗶	Propiedades: DisableRe	gistryTools 🧮	<u></u>	
 Directiva bloqueo registro (sm Configuración del equipo Directivas Preferencias Configuración de usuario 	General Comunes	Actualizar 🔻	Acción	Subárbol
 Directivas Preferencias Configuración de V Anlicaciones 	Subárbol: Ruta de la clave:	HKEY_CURRENT_USER	Actuali	HKEY_CURRENT_USI

	Group Policy Group Policy Group MomeGroup Group Internet Set Group McT	Objects
	RanDaR Greensave	's
Nombre	Tipo	Datos

En nombre del valor ponemos **DisableRegistryTools** en tipo de valor seleccionamos **REG_DWORD** y en informacion del valor ponemos **1**, en base debe estar **Decimal**, al final se debe mostrar como la siguiente imagen, al final damos clic en **aceptar**.

 Image: Second sec	General Comunes	Actualizar 💌		
 ▶ Preferencias ♥ Configuración de usuario ▶ Directivas ▲ Preferencias ▲ Configuración de Wind 	Subárbol: Ruta de la clave: - Nombre de valor	HKEY_CURRENT_USER	Acción Actuali	Subárbol HKEY_CURRENT_USI
 Splicaciones Splicaciones de un Entorno Archivos 	Predeterminado	DisableRegistryTools REG_DWORD		
Carpetas Archivos .ini Registro Accesos directos Configuración del Pane	Información del valor:	1 Base Hexadecimal Occimal		
Configuración del Pane	Aceptar	Cancelar Aplicar Ayuda		

Bloquear un programa por medio de una GPO.

En ocaciones es necesario bloquear un programa ya sea poque se trata de un juego o un programa que genera algun tipo de trafico en la red y los usuarios estan abusando del uso de este, para esto nos vamos a la OU a la que le vamos a aplicar la politica le damos clic con el boton secundario del mouse y seleccionamos **Crear un GPO en este dominio y vincularlo aquí**.

🛅 Raíz de consola	-	Logistic	a		
Administración de directivas de grupo A A Bosquer cienic site		Objetos d	e directiva de grupo vinculados	Herencia de directivas	de 🚺
 A Bosque stemetste A A Dominios 			Orden de vínculos	GPO	Exigi
⊿ 🚔 sienic.site हि Default Domain Policy		会	1	Bloqueo de red	No
Contabilidad			3	bloqueo registro	No
 ▷ I Domini Contoines ▷ I Dogistica ○ Objetos ○ Filtros W ▷ I GPO de i Bloquez ▷ Sitios 	n GPO e un GP r heren	en este dom O existente, ocia	inio y vincularlo aquí 		

En el siguiente cuadro poner un nombre descriptivo para llevar un control de lo que hacen las GPO que tenemos en el servidor y clic en **aceptar**.

and the second se	
Nombre:	
bloqueo solitario	
GPO de inicio de origen:	
(ninguno)	

En la lista de GPO damos doble clic sobre la que acabamos de crear.



Nos aseguramos que en **filtrado de seguridad** este el grupo o los grupos correspondientes. <u>http://easgs.wordpress.com</u>

🖀 serveradmin - ᠺíz de consola\Administración c	le directivas de grupo\Bosque: sienic.site\Domini	os\sienic.sit	e \Logistica\	.blo 🗖 🗗 🔀
Archivo Acción Ver Favoritos Ventana	Ayuda			- 8 ×
				92
📔 Raíz de consola 📃 🔺	bloqueo solitario			Acciones
Administración de directivas de grupo	Ambito Detalles Configuración Delegación			bloqueo solitario 🔺
 Bosque: stenic.site Bominios Bienic.site Cefault Domain Policy 	Vínculos Mostrar vínculos en esta ubicación: sienic.site	vas están vin	▼	Acciones ad 🕨
 ▷ □ Contabilidad ▷ □ Domain Controllers □ Logistics 	Ubicación	Exigido	Víncuk	
Bioquear panel			•	
 Bioqueo registro bloqueo solitario Objetos de directiva de gru Filtros WMI GPO de inicio 	Filtrado de seguridad La configuración en este GPO sólo se puede aplica Nombre Logistica (SIENIC\Logistica)	ir a los grupos	s, usuarios	
Modelado de directivas de grupo Resultados de directivas de grupo B DNS Usuarios y equipos de Active Directory [si	Agregar Quitar	Propiedad	les j	

Hacemos clic con el boton secundario del mouse sobre la GPO y seleccionamos Editar.

🚡 serveradmin - [Raíz de consola\Administ	ración de diिctivas de grupo\Bosque: sienic.s	ite\Dominios\sienic.site \Logistica	(blo 👝 🗗 🎫
Archivo Acción Ver Favoritos	Editar Exigido Vínculo habilitado		_ & ×
Administración de directivas de gru	Guardar informe	ación	bloqueo solitario 🔺
Dosque, sienciste A Dominios A A A A	Ver Nueva ventana desde aquí	nic.site 🔻	Acciones ad 🕨
📓 Default Domain Poli > 😭 Contabilidad	Nueva vista del cuadro de tareas	organizativas están vinculados a	
Domain Controllers	Eliminar	Exigido Vínculo	
🔺 📴 Logistica	Cambiar nombre	No Sí	
Bloquear panel	Actualizar	Þ	
bloqueo registro	Ayuda		

Luego nos vamos a Configuracion de usuario/Configuracion de Windows/Directivas de restriccion de software damos clic con el boton secundario del mouse y seleccionamos Nuevas directivas de restriccion de software.



Hacemos clic con el boton secundario sobre **Reglas adicionales** y seleccionamos **Regla de nuevo** hash.

Directiva bloqueo solitario [smb4server ⁰¹	<u>iania de 1</u>			Tipo	Nive
	Regla de nuevo certificado Regla de nuevo hash Nueva regla de zona de red Regla de nueva ruta de acceso		_LOCAL_MACHINE\SOFTWARE\ _LOCAL_MACHINE\SOFTWARE\	Ruta de a Ruta de a	Ilim Ilim
Configuración de software	Todas las tareas	•			
Configuración de Windows	Ver	•			
 Lonfiguración de segurio Configuración de segurio Directivas de clave pu Configuración de restricci 	Actualizar Exportar lista				
Niveles de segurio Reglas adicionales	Ayuda				
N 🦳 Redirección de carnetas					

En el siguiente cuadro hacemos clic en examinar.

Archivo Acción ver Ayuo				
♦ ♦ 2 11 1 0 1	Regla de nuevo hash			A.P.
 Directiva bicqueb solitano (s Configuración del equipo Directivas Preferencias Configuración de usuario Directivas Configuración de Configuración de Scripts (inicio Configuración Configuración Directivas (inicio) 	Use reglas para invalidar el nivel de seguridad predeterminado. Haga clic en Examinar para seleccionar el archivo sobre el que desea aplicar un algoitmo hash. Los atributos del archivo, como el tamaño y la fecha y hora de creación, se completarán automáticamente. Información del archivo:	DFTWARE\ DFTWARE\	Tipo Ruta de a Ruta de a	Nive Ilim Ilim
 Directivas i Niveles Reglas Redirección de QOS basada er Impresoras im Mantenimient Plantillas administ Preferencias 	Nivel de seguridad: No permitido Descripción: Obtener más información acerca de las directivas de restricción de software			
	Aceptar Cancelar Aplicar			

Buscamos la ruta del ejecutable del programa que deseamos bloquear lo seleccionamos y damos clic en **aceptar**.

i 🔁 👘 🗘	J Abrir					×
Directiva bloqueo s	Micr	osoft G	ames 🕨 Solitaire 🕨 👻	↓ Busco	ar Solitaire	٩
Configuración e Directivas	Organizar 👻 Nue	va carp	eta		III • [1 0
 Preferencias ^A ^(A) Configuración d 	Favoritos		Nombre	F	Fecha de modifica	Tipo
a 🔛 Directivas	🙏 Descargas		🎍 es-ES	1	14/07/2009 2:48	Carpeta d
Configure	Escritorio		Solitaire	1	13/07/2009 19:14	Aplicació
A Configui	🔛 Sitios recientes		SolitaireMCE	1	10/06/2009 15:34	Imagen P
≥ Scrip → Conf → □ D → □ D → □ C → □ D → □ D	 Bibliotecas Documentos Imágenes Música Vídeos 	III	🔊 Solitario de Media Center	1	13/07/2009 22:42	Acceso di
⊳ C Plantillas	C Red		m			,
	N	lombre	Solitaire	Todos Ab	los archivos (*.*) rir 🔽 Can	• celar

En el siguiente cuadro se muestra toda la informacion del ejecutable, damos clic en **aceptar**.

Arcnivo Accion ver Ayur	Regla de nuevo hash	<u>]</u>		
Arcnivo Accion ver Ayue Arcnivo Accion ver Ayue Directiva bloqueo solitario [s Directiva bloqueo solitario [s Directivas Directivas Configuración de usuaric Directivas Directivas Configuración de Configuración de Scripts (inicio	Regla de nuevo hash General Use reglas para invalidar el nivel de seguridad predeterminado. Haga clic en Examinar para seleccionar el archivo sobre el que desea aplicar un algoritmo hash. Los atributos del archivo, como el tamaño y la fecha y hora de creación, se completarán automáticamente. Información del archivo:) DFTWARE\ DFTWARE\	Tipo Ruta de a Ruta de a	Nive Ilim Ilim
 ▲ Configuración ▶ ■ Directivas ▲ ■ Directivas ▲ ■ Directivas ■ Niveles ■ Reglas ▶ ■ Redirección de ▶ ■ QoS basada er ▶ ■ Impresoras im 	solitaire.exe (6.1.7600.16385) solitaire.exe Executable for Solitaire Game Microsoft® Windows® Operating System Nivel de seguridad: No permitido			
 ▶ ∰ Mantenimient ▶ ☐ Plantillas administ ▶ ☐ Preferencias 	Obtener más información acerca de las <u>directivas de restricción de software</u> Aceptar Cancelar Aplicar			

Ahora se nos muestra el ejecutable en el panel derecho.



Ahora cuando el usuario trate de ejecutar el programa le aparecera este cuadro de dialogo.



Ocultar Unidades en Mi Pc.

En este ejercicio vamos a ocultar las unidades A, B, C Y D para que el usuario no pueda verlar cuando haga doble clic sobre el icono Mi PC, para esto nos vamos a la OU a la que vamos a aplicar la politica hacemos clic con el boton derecho del raton y seleccionamos **Crear un GPO en este dominio y vincularlo aquí.**



En el siguiente cuadro le ponemos un nombre descriptivo a la GPO y clic en aceptar.

Nombre:	
Ocultar iconos de unidades	
GPO de inicio de origen:	
(ningung)	

Hacemos doble clic sobre la GPO



En la siguiente ventana nos aseguramos que en **filtrado de seguridad** esten los grupos a los que deseemos aplicar la politica de seguridad.

Raíz de consola	Ocultar iconos de unidades			Acciones
Administración de directivas de grupo	Ámbito Detalles Configuración Delegación			Ocultar iconos de u 🔺
 Bosque: stenic.site Bominios Bisenic.site Default Domain Policy Contabilidad 	Vínculos Mostrar vínculos en esta ubicación: sienic.site Los siguientes sitios, dominios y unidades organiza	tivas están vin	▼	Acciones adici 🕨
Domain Controllers	Ubicación	Exigido	Vin	
a 💼 Logistica 😹 Bloquear panel	📓 Logistica	No	Sí	
 bloqueo de red bloqueo registro bloqueo solitario Ocultar iconos de unidade Objetos de directiva de grupo Filtros WMI GPO de inicio Sitios Modelado de directivas de grupo 		ar a los grupos	s, usuari	
Les nesultados de directivas de grupo	Agregar Quitar	Propiedad	des	

El siguiente paso es hacer clic con el boton secundario del mouse sobre la GPO y seleccionamos **Editar**.

🚡 serveradmin - [Raí 🕽 e consola\Ac	lministración de	directivas de grupo\Bosqu	e: sienic.site\Dom	inios\sienic.site	e \Logis
Archivo Acción Ver Favorit Archivo Acción Ver Favorit Acción Ver Favorit Acción Ver Favorit Acción de directi Acción de di	os Ventana Editar Exigido Vínculo habilit Guardar inforr Ver	Avuda tado ne	ades n Delegación]	-
	Nueva ventan Nueva vista de	a desde aquí el cuadro de tareas	unidades organi	zativas están vin Exigido	culados Vín
	Eliminar Cambiar noml Actualizar	bre		No	Si •
	Ayuda os de unidadem	La configuracion en este GP	U sólo se puede ap	licar a los grupos	. usuari
▷ i Objetos de direc ▷ i Filtros WMI ▷ i OPO de inicio	tiva de grupo	Nombre & Logistica (SIENIC\Logis	stica)		

Luego nos vamos a Configuracion de usuario/Plantillas administrativas/Componentes de Windows/Explorador de Windows y hacemos doble clic sobre la opcion Ocultar estas unidades especificadas en Mi PC.



En este cuadro seleccionamos la opcion Habilitada y en Elegir una de las siguientes combinaciones seleccionamos Restringir solo las unidades A, B, C y D.

🌺 Ocultar estas unidades especificadas e	n Mi PC		x
Ocultar estas unidades especificadas	en Mi PC	Valor anterior Valor siguiente	
 No configurada Habilitada Deshabilitada Compatible con: 	Al menos Windows 200	0	* *
Opciones:		Ayuda:	
Elegir una de las siguientes combinacione Restringir todas las unidades Restringir solo las unidades A y B Restringir solo la unidad C Restringir solo las unidades A, B y C Restringir solo las unidades A, B y C Restringir todas las unidades No restringir unidades	25	Quita los iconos que representan los discos duros seleccionados de Mi PC y Explorador de Windows. Además, las letras de unidad que representan las unidades seleccionadas no aparecerán en el cuadro de diálogo Abrir estándar. Para usar esta opción, seleccione una unidad o una combinación de unidades de la lista desplegable. Para mostrar todas las unidades, deshabilite esta opción o seleccione la opción "No restringir unidades" de la lista desplegable. Nota: esta opción quita los iconos de las unidades. Los usuarios seguirán teniendo acceso al contenido de las unidades a través de otros métodos, como puede ser escribir la ruta de acceso a un directorio de la unidad en el cuadro de diálogo Conectar a unidad de red, en el cuadro de diálogo Ejecutar o en una ventana de comandos.	

Damos clic en **aceptar**, con esto ya tenemos configurada la GPO.

📑 Directiva Ocultar iconos de unidades [smb4serve	Configuración	Estado	•
 Configuración del equipo Directivas Preferencias Configuración de usuario Directivas Configuración de software Configuración de Windows Plantillas administrativas: definiciones Carpetas compartidas Componentes de Windows Administrador de datos adjunt Administrador de ventanas del Almacén digital 	 Desactivar todas las características de bibliotecas de Windo Deshabilitar carpetas conocidas Deshabilitar carpetas conocidas Desactivar que se muestren las entradas de búsqueda recien Permitir solo extensiones de shell aprobadas o por usuario Desactivar que se muestren fragmentos en el modo de vista No hacer un seguimiento de accesos directos al Shell durant Número máximo de documentos recientes Quitar las características de grabación de CD Desactivar el almacenamiento en caché de imágenes en mi Quitar UI para cambiar la configuración de la animación de Quitar UI para cambiar la opción de subrayado de teclas de Ouitar la ficha DFS 	No configurada No configurada No configurada No configurada No configurada No configurada No configurada No configurada No configurada No configurada	E
 Buscar Búsqueda instantánea Calendario de Windows Centro de movilidad de Windo Compatibilidad de aplicacione Configuración de presentaciór Copia de seguridad Directivas de Reproducción au 	Ocultar estas unidades especificadas en Mi PC Sin red completa en Ubicaciones de red Quitar el menú Archivo del Explorador de Windows Quita el menú Opciones de carpeta del menú Herramientas Ocultar la ficha Hardware Oculta el elemento Administrar del menú contextual del Exp Quitar Documentos compartidos de Mi PC	Habilitada No configurada No configurada No configurada No configurada No configurada	
Explorador de Windows	Concerns annous de red y Desconectar de dindadam	No comiguiada	P.

A como podemos ver en la siguiente imagen no se muestra nada cuando hacemos doble clic sobre el icono Mi PC.



Esta ultima configuracion solo oculta las unidades pero el usuario podra entrar a la unidad de red si escribe la ruta en el cuadro de dialogo ejecutar o si escribe la ruta en la barra de direcciones del explorador de Windows, para impedir que el usuario tenga acceso a las unidades espeficicadas hay que usar la opcion **Impedir acceso a las unidades desde mi PC**.



Habilitamos la opcion y seleccionamos las unidades que queremos bloquear, luego le damos clic en **aceptar**.

🐉 Impedir acceso a las unidades desde N	ti PC 🗖 🗗
Impedir acceso a las unidades desde l	Valor anterior Valor siguiente
 No configurada Habilitada Deshabilitada Compatible con: 	Al menos Windows 2000
Opciones:	Ayuda:
Elegir una de las siguientes combinacione Restringir solo las unidades A, B, C y D Restringir solo las unidades A y B Restringir solo la unidad C Restringir solo las unidades A, B y C Restringir solo las unidades A, B, C y D Restringir todas las unidades No restringir unidades	Impide que los usuarios usen Mi PC para tener acceso al contenido de las unidades seleccionadas. Si habilita esta opción, los usuarios podrán explorar la estructura de directorios de las unidades seleccionadas en Mi PC o el Explorador de Windows, pero no podrán abrir las carpetas y tener acceso a su contenido. Tampoco podrán usar el cuadro de diálogo Ejecutar o el cuadro de diálogo Conectar a unidad de red para ver los directorios de estas unidades. Para usar esta opción, seleccione una unidad o una combinación de unidades de la lista desplegable. Para permitir el acceso a todos los directorios de las unidades" de la lista desplegable. Nota: los iconos que representan las unidades especificadas seguirán apareciendo en Mi PC, pero si los usuarios hacen doble clic en los iconos,

Con eso ya tenemos habilitada la opcion para que los usuarios no puedan entrar a las Unidades que hemos bloqueado.

Configuración de presentació	 Quitar el boton busqueua del Explorador de Windows Desactivar la ordenación numérica en el Explorador de Wind Quitar el menú contextual predeterminado del Explorador d 	No configurada No configurada No configurada	
a 🧰 Explorador de Windows	Impedir acceso a las unidades desde Mi PC	Habilitada	
 Diálogo común para abrir Panel de marcos del Explo Versiones anteriores 	 Desactivar las teclas de acceso rápido Windows+X Sin "Equipos próximos" en Ubicaciones de red Solicitar credenciales para instalaciones en red 	No configurada No configurada No configurada	

Si el usuario escribe la ruta ya sea en Ejecutar o en la barra de direcciones de Windows explorer recibira un error.

	recurso de Internet que	desea abrir con Win	dows.
brir:	C:\		2



Vincular un GPO existente a una unidad organizativa.

En ocaciones es necesario aplicar un GPO existente a otra unidad organizativa, esto nos permite aplicar politicas de seguridad a otros usuarios de otros departamentos sin necesidad de volver a crear otra politica con los mismos parametros evitando asi redundancia, para llevar a cabo esta tarea, nos vamos a la OU a la que deseemos aplicar la directiva ya existente y le damos clic con el boton derecho del mouse, luego seleccionamos **Vincular un GPO existente**.



En la siguiente ventana seleccionamos la GPO que deseamos aplicar y damos clic en aceptar.

Raíz de consola	Seleccionar GPO
 Administración de direc A Bosque: sienic.site 	Buscar en este dominio:
Dominios	sienic,site
Default D	Objetos de directiva de grupo:
⊳ 🖬 Contabili ⊳ 🖬 Domain (Nombre
⊿ 🔂 Logistica	Bloquear Panel
Bloqu Dipetos d	Default Domain Controllers Policy Default Domain Policy
⊳ 🕞 Filtros WI	
Sitios	
Modelado de dir 院 Resultados de dir	
Usuarios y equipos de A Services puerdada	
▲ jii sienic.site	
Users	Aceptar Cancelar

Ahora podemos ver que la GPO aparece en la lista de objetos vinculados a esta OU a como se muestra a continuacion, es importante saber que esto es solo un vinculo a un objeto GPO, por lo que si la borramos lo que estamos borrando es un acceso directo no la GPO en si.

 Serveradmin - [Raíz de consola\Administració Archivo Acción Ver Favoritos Ventar Archivo Image: Archivo Acción Ver Favoritos Ventar 	n de d na A	lirectiva kyuda	s de grupo\Bosque: sienic.site	\Dominios\sienic.site \C	ontab	ilidad] 👝 🗗 📑	×
 Raíz de consola Administración de directivas de grupo A Rosque: cienic site 		ontab	ilidad	-	_	Acciones	
		Objetos (de directiva de grupo vinculados	Herencia de directivas	•	Contabilidad	•
▲ 🙀 Dominios			Orden de vínculos	GPO	E	Acciones adici	۲
a 🚔 sienic.site		2	1	🗐 Bloquear Panel	N		
📓 Default Domain Policy > 🖬 Contabilidad							
Domain Controllers		\bigtriangledown					

Hacemos doble clic sobre la GPO y agregamos los grupos de usuarios correspondientes en este caso el grupo contabilidad.
a 🚊 Contabilidad	Los siguientes sitios, dominios y unidad	es organizativas están vinculado
Bloquear panel	Ubicación	Exigido Vin
Domain Controllers	Contabilidad	No Si
D 🔂 Logistica	🔲 Logistica	No Sí
Objetos de directiva de gru	۲ III ا	•
Filtros WMI		
> 📷 GPO de inicio	Filtrado de seguridad	
 GPO de inicio Image: Sitios 	Filtrado de seguridad La configuración en este GPO sólo se p	puede aplicar a los grupos, usua
 ▷ math GPO de inicio ▷ math Sitios ֎ Modelado de directivas de grupo Besultados de directivas de grupo 	Filtrado de seguridad La configuración en este GPO sólo se p Nombre	ouede aplicar a los grupos, usua
 ▷ mathing GPO de inicio ▷ mathing Sitios ₩ Modelado de directivas de grupo ➡ Resultados de directivas de grupo 	Filtrado de seguridad La configuración en este GPO sólo se p Nombre	ouede aplicar a los grupos, usua
 GPO de inicio GPO de inicio Sitios Modelado de directivas de grupo Resultados de directivas de grupo BDNS Usuarios y equipos de Active Directory [sr 	Filtrado de seguridad La configuración en este GPO sólo se p Nombre & Contabilidad (SIENIC\Contabilidad & Logistica (SIENIC\Logistica)	puede aplicar a los grupos, usua

Aunque en el filtrado de seguridad este agregado el grupo, si no se vincula la GPO a la OU los parametros no se van a aplicar, la GPO tiene que estar vinculada a la OU y el grupo agregado para que esto funcione.

Eliminar una GPO.

Para eliminar una GPO nos vamos a **Administracion de directivas de grupo**, seleccionamos el dominio y luego **Objetos de directiva de grupo**, en el panel derecho se mostraran todas las GPO creadas.

🔊 serveradmin - [Raíz de consola\Administración d a Archivo Acción Ver Favoritos Ventana ← → 2000 [10] [10] [20] [10]	le directivas de grupo\Bosque: Ayuda	sienic.site\Dominios	:\sienic.site \Objet	os de dir 👝 🖨 💌
Raíz de consola	Objetos de directiva d	le grupo en sie	nic.site	Acciones
A Bosque: sienic site	Contenido Delegación			Objetos de directiv 🔺
 Bosque senieste Bosque senieste Bosque senieste 	Nombre	Estado de GPO	Filtro WMI	Acciones adici 🕨
 sienic.site Default Domain Policy Contabilidad Domain Controllers Logistica Objetos de directiva de grupo Filtros WMI GPO de inicio Sitios Modelado de directivas de grupo Resultados de directivas de grupo 	Bloquear panel bloqueo de red bloqueo de solitario bloqueo registro bloqueo solitario Default Domain Contro Default Domain Policy Coultar iconos de unid	Habilitado Habilitado Habilitado Habilitado Habilitado Habilitado Habilitado	Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno	

Seleccionamos la GPO que deseamos eliminar y hacemos clic con el boton secundario del mouse luego seleccionamos **Eliminar**.



Nos va a a aparecer una cuadro de confirmacion donde se nos indica que si borramos la GPO tambien se eliminaran todos los vinculos a OU que hayamos creado.

 Raíz de consola Administración de directivas de grupo A Borques cienic site 		Objetos de directiva de grupo en sienic.site			
		Contenido Delegación			
83	 A Bosque siencisite A Bosque siencisite 		Nombre	Estado de GPO	Filtro WMI
2	a 🛱 sienic.site		Bloquear panel	Habilitado	Ninguno
Image: Second secon		Administi	ración de directivas de grup ¿Desea eliminar este GPO y en este dominio? No se elir dominios.	oo todos los vínculos hacia él ninarán vínculos en otros	Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno Ninguno
	 Sitios Modelado de directivas Resultados de directivas de 	grupo		Sí No	

Damos clic en si y se nos mostrara esta pantalla al terminar damos clic en aceptar.

Raíz de consola	Eliminar	
🔣 Administración	Progreso de eliminación:	
A Bosque: sien		
	Second Se	
	Estado:	
	GPO: bloqueo registroCorrecto],
a 📑 D		
🔺 🛅 Lo		
75		
> 🛅 G		
Sitios		
👸 Modelad		
🧱 Resultadi		
L DNS	1	
Usuarios y equip		Acentar Cancelar

En la siguiente imagen se muestra un vinculo a la GPO que estamos borrando que es bloqueo de registro y que esta vinculado a la OU Logistica.



Aquí se muestra que despues de borrar el objeto GPO tambien se elimina automaticamente el vinculo de las OU.



Delegar Control sobre una Unidad organizativa.

Para hacer efectiva una delegacion de control, los objetos a administrar deben estar dentro de la unidad organizativa, esto es que si existe un usuario que pertenece a un grupo que esta dentro de

la unidad organizativa, pero el usuario en si no esta dentro de la OU, no se podra administrar este usuario a menos que se incluya explicitamente dentro de la OU.

Lo primero que debemos hacer para poder delegar control sobre una OU es modificar el archivo /usr/local/samba/etc/smb.conf y agregar la opcion

acl:search=false

Luego ejecutamos el comando

smbcontrol all reload-config

Para revisar que la configuración del archivo smb.conf este bien ejecutamos el comando.

samba-tool testparm -v

Luego en **Usuarios y equipos de active directory** damos clic derecho sobre la OU en la que deseamos delegar control y en el menu desplegable seleccionamos **Delegar Control**, en el siguiente cuadro damos clic en **siguiente**.



En la siguiente ventana damos clic en **Agregar** y en el cuadro introducimos el usuario al que deseemos delegar control en esta OU, damos clic en **Comprobar nombre** y luego en **aceptar**.

seleccionar osuanos, equipos o orupos	- V -
Seleccionar este tipo de objeto:	
Usuarios, Grupos, o Entidades de seguridad integradas	Tipos de objeto
Desde esta ubicación:	
sienic.site	Ubicaciones
Escriba los nombres de objeto que desea seleccionar (ejemplos):	
easgs05 (easgs05@sienic.site)	Comprobar nombre
Opciones avanzadas	ceptar Cancelar
Agregar Quitar	
< Atrás Siguiente > Cancelar Ayuda	
lers	
rincipals	
	Seleccionar este tipo de objeto: Usuarios, Grupos, o Entidades de seguridad integradas Desde esta ubicación: sienic.site Escriba los nombres de objeto que desea seleccionar (ejemplos): easqs05 (easqs05@sienic.site) Opciones avanzadas Agregar Quitar Agregar Quitar Iers Principals

Damos clic en siguiente.

Seleccione uno o más	usuarios o grupos en los qu	e desea delegar el control.	(
Usuarios y grupos sele	ccionados:		
asgs05 (easgs05	@sienic.site)		
		Agregar Qu	iitar

En este cuadro seleccionamos las tareas que vamos a delegarle al usuario, damos check a las que deseemos.

O Dele	egar las siguientes ta	ireas comunes:		
	Crear, eliminar y ad	lministrar cuentas de l	usuario	^
	Restablecer contra 	aseñas de usuario y fo	rzar el <mark>c</mark> ambio de contraser	ia =
	Crear climicary ad	acion del usuano		
	Modificar la perten	encia de un grupos		
	Administrar v inculo	os de directiva de oru:	0	
17	Generar conjunto r	resultante de directiva	s (planeamiento)	-
		III		•
Crea	ar una tarea personal	lizada para delegar		

Al terminar el asistente le damos clic en finalizar.

Finalización del Asistente para delegación de control Ha finalizado correctamente el Asistente para delegación de control.
Los grupos, usuarios o equipos a los que ha conþedido control son: easgs05 (easgs05@sienic.site) Seleccionó delegar las siguientes tareas: Crear, eliminar y administrar cuentas de usuario Restablecer contraseñas de usuario y forzar el cambio Crear, eliminar y administrar grupos
Para cenar el asistente, haga clic en Finalizar.

Con esto el usuario podra hacer las todas tareas especificadas dentro de esta OU.

Revisar los permisos delegados.

Para revisar los permisos que hemos delegado en una unidad organizativa nos vamos a Usuarios y equipos de Active Directory/Ver/Caracteristicas avanzadas.



Seleccionamos la OU y le damos clic con el boton secundario del mouse y damos clic en **propiedades**.



En el cuadro de propiedades seleccionamos la solapa Seguridad y damos clic en opciones avanzadas.

Contabilid	Propiedades: Logistica
Domain Contaction	General Administrado por Objeto Seguridad COM+ Editor de atributos
E Logistica	Nombres de grupos o usuarios:
> 📑 Objetos de	A Todos
Filtros WM	SELF
D GPO de ini	& Usuarios autentificados
📑 Sitios	& SYSTEM
👸 Modelado de dire	asgs05
📑 🔀 Resultados de dire	& Domain Admins (SIENIC\Domain Admins)
DNS	Agregar Quitar
Usuarios y equipos de Ac	
🗧 📋 Consultas guardadas	Permisos de Todos Permitir Denegar
🛚 🏥 sienic.site	
Users	Control total
Computers	Leer
👂 🧮 Builtin	Escribir
👂 🗾 Domain Controlle	Crear todos los objetos secundarios
ForeignSecurityPr	Eliminar todos los objetos secundarios
LostAndFound	Para especificar permisos especiales o Opciones avanzadas
👂 🚞 Program Data	avanzadas, haga clic en Opciones
System	Obtener más información acerca de control y permisos de acceso
Contabilidad	
📑 Logistica	Aceptar Cancelar Aplicar Avuda
NTDS Quotas	

En este cuadro se muestran los permisos asignados al usuario en esta OU.



Revocar los permisos delegados.

Para revocar una delegacion basta con eliminar el usuario de la solapa **seguridad** de las **propiedades** de la unidad organizativa.



Delegar control para unir maquinas al dominio.

Esta delegacion solo se puede asignar sobre el contenedor Computers y se puede aplicar ya sea a un grupo o a un usuario.

Para llevar a cabo esto nos vamos a **Usuarios y equipos de Active Directory** y damos clic con el boton secundario del mouse sobre el contenedor **Computers**, luego seleccionamos **Delegar control** y damos clic en **siguiente** en el primer cuadro de asistente.



En la siguiente pantalla damos clic en **agregar**, escribimos el nombre del usuario o grupo y damos clic en **comprobar nombre** y clic en **aceptar** y despues en **siguiente**, en la siguiente pantalla seleccionamos la opcion **Crear una tarea personalizada para delegar** y clic en **siguiente**.

🍃 🔿 🖄 🗊 🔏 🖬	Asistente para delegación de control	x
■ Raíz de consola ▶ ▲ Administración de o ▶ ▲ DNS	Tareas que se delegarán Puede seleccionar tareas comunes o personalizar sus propias tareas.	R
 Usuarios y equipos Consultas guard sienic.site Users Computers Builtin Domain Con ForeignSecu LostAndFour System System Contabilidac Logistica 	 Delegar las siguientes tareas comunes: Crear, eliminar y administrar cuentas de usuario Restablecer contraseñas de usuario y forzar el cambio de contraseña Leer toda la información del usuario Crear, eliminar y administrar grupos Modificar la pertenencia de un grupo Crear, eliminar y administrar cuentas inetOrgPerson Restablecer las contraseñas de inetOrgPerson y forzar el cambio de co Trear una tarea personalizada para delegar 	
⊳ 🚞 NTDS Quota	< Atrás Siguiente > Cancelar A	yuda

En la siguiente pantalla seleccionamos la opcion Solo los siguientes objetos en la carpeta, y checamos Objetos Equipo, tambien checamos las otras dos opciones, Crear los objetos

seleccionados en esta carpeta y Eliminar los objetos seleccionados en esta carpeta y luego damos clic en siguiente.

	Asistente para delegación de control	×
 ☐ Raíz de consola ▶ 🛃 Administración de c ▶ 🚊 DNS 	Tipo de objeto de Active Directory Indique el ámbito de la tarea que desea delegar.	R
 ▲ Usuarios y equipos a ▶ ○○ Consultas guard ▲ ○○ sienic.site ▶ ○○ Users 	Delegar el control de: Esta carpeta, los objetos contenidos en la misma y la creación de nuevos objetos e esta carpeta Sólo los siguientes objetos en la carpeta:	'n
Computers Computers Suiltin Signature ForeignSecu CostAndFour Signature Program Dat	 Objetos domainRelatedObject Objetos Dominio de confianza Objetos dynamicObject Objetos Equipo Objetos friendlyCountry Objetos groupOfUniqueNames 	
▷ Contabilidac ▷ Contabilidac ▷ Logistica ▷ NTDS Quota	 ✓ Crear los objetos seleccionados en esta carpeta ✓ Eliminar los objetos seleccionados en esta carpeta 	_
	< Atrás Siguiente > Cancelar Ayı	uda

En la siguiente pantalla checamos las opciones **General** y **Especifico de la propiedad** y de la lista de opciones seleccionamos las siguientes opciones.

Lista en español:

Restablecer contraseña Leer y escribir restricciones de cuenta Leer y escribir atributos de nombre de host de DNS Escritura validada en el nombre de host DNS Escritura validada en el nombre principal de servicio Escribir servicePrincipalName

Lista en Ingles:

Reset password Read and write account restrictions Read and write DNS host name attributes Validated write to DNS host name Validated write to service principal name Write servicePrincipalName

	Asistente para delegación de control	×
Raíz de consola	Permisos Seleccione los permisos que desea delegar.	R
 ✓ Usuarios y equipos a ✓ Consultas guard ✓ Consultas guard ✓ Sienic.site ✓ Users ✓ Computers ✓ Builtin ✓ Domain Con ✓ ForeignSecu ✓ LostAndFour ✓ Program Dat ✓ System ✓ Contabilidac ✓ Logistica ✓ NTDS Quota 	Mostrar estos permisos: General Específico de la propiedad Creación o eliminación de objetos secundarios específicos Permisos: Leer y escribir Información pública Escritura validada en el nombre principal de servicio Recibir como Enviar como Leer Administrado por Escribir Administrado por	•
	< Atrás Siguiente > Cancelar	Ayuda

Damos clic en **siguiente** y se nos mostrara una pantalla con un resumen de lo que hemos configurado y damos clic en **finalizar**.

🗢 🔿 🖄 🗊 🔏 🖬	Asistente para delegación de c	ontrol	X
 Raíz de consola Administración de c DNS Usuarios y equipos Consultas guard Sienic.site Users Computers Builtin Domain Con ForeignSecu LostAndFour Program Dat System Contabilidad 	Asistente para delegación de c	Finalización del Asistente para delegación de control Ha finalizado correctamente el Asistente para delegación control. Con los siguientes permisos: Restablecer contraseña Leer y escribir Restricciones de cuenta Leer y escribir Atributos de nombre de host de DNS Escritura validada en el nombre de host DNS Escritura validada en el nombre principal de servicio Escribir servicePrincipalName Para los siguientes tipos de objeto: Equipo	de
 Contabilidad Logistica MTDS Quota 		Para cerrar el asistente, haga clic en Finalizar.	
		< Atrás Finalizar Cancelar A	yuda

Entorno de red.

En cuanto al entorno de red, por el momento esperemos ver todos los equipos menos el servidor samba en el entorno de red, a como se muestra a continuacion el nombre del servidor de dominio samba es smb4server01



Pero en la siguiente imagen del entorno de red en una estacion con Windows 7 pro, podemos ver que todos los demas equipos se muestran menos el servidor de dominio samba.



Esto significa que para acceder a un recurso compartido en el servidor deberemos introducir la direccion ip del servidor ya sea usando windows+R o en la barra de ubicación.

. Gecu	Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.)
<u>A</u> brir:	\\192.168.0.20	Ŧ
	Acostar Cancelar Evamin	24

Si queremos que el recurso este disponible cada vez que arranque el equipo le damos clic con el boton secundario del mouse y seleccionamos **conectar a unidad de red.**



En la siguiente pantalla seleccionamos la letra de unidad que le queremos asignar y checamos Conectar de nuevo al iniciar sesion.

specifique	la letra de unidad para la conexión y la carpe	ta a la qu <mark>e</mark> dese	ea conectarse:	
nidad:	Z: •			
arpeta:	\\192.168.0.20\Datos	*	Examinar	
	Ejemplo: \\servidor\recurso_compartido			
	🔽 Conectar de nuevo al iniciar sesión			
	Conectar con otras credenciales			
	Conectarse a un sitio web para usarlo com	o almacén de c	locumentos e imágenes	<u>s</u> .

Ahora cada vez que queramos acceder a este recurso no vamos a equipo y damos doble clic sobre la letra de unidad que le asignamos al recurso compartido.



DNS

DNS

El servicio DNS es vital para el funcionamiento de Active Directory, por eso es importante conocer los tipos de registros que debemos manejar para su buen funcionamiento, bajo condiciones normales no deberiamos tener la necesidad de hacer algun tipo de tarea en el DNS ya que las actualizaciones las hace el servidor automaticamente cuando agregamos un equipo a la red, pero en el caso por ejemplo que tuvieramos que formatear una maquina o cambiarle el nombre deberemos borrar el registro en el DNS para mantener nuestro servidor lo mas ordenado posible, para entrar al DNS nos vamos a DNS/IP_DEL_SERVIDOR/Zonas de busqueda directa/sienic.site.

Archivo Acción Ver Favoritos Ven	tana Ayuda				- 8
🕨 🔿 🔀 📰 🖾 🙆 👘					
Raíz de consola	Nombre	Тіро	Datos	Marca de tiempo	Acciones
Administración de directivas de grupo	Sites				sienic.site 🔺
 IDPLES.0.20 IDPLES.0	Ltcp 	Inicio de autoridad (SOA) Servidor de nombres (NS) Hust (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A)	[34], sri b4server01 sienic.s smb4server01.sienic.site. 192.168.0.20 192.168.0.30 192.168.0.30 192.168.0.30 192.168.0.35 192.168.0.50 192.168.0.36 192.168.0.20	11/01/2014 17:00:00 static static 30/12/2013 8:00:00 26/12/2013 11:00:00 26/12/2013 15:00:00 23/01/2014 16:00:00 11/01/2014 18:00:00 11/01/2014 18:00:00 static	Λςείο 🕨

En esta ventana se nos muestran los diferente tipos de registros que tenemos en nuestro servidor DNS, un registro (A) para cada computadora de la red, estos registros estan asociados a la direccion IP de cada maquina, en este ejemplo podemos ver que hay varios registros (A) para una misma direccion IP, esto es debido a que se le a cambiado el nombre a la PC en varias ocaciones, este tipo de registros son los que debemos ir eliminando para que no causen confusion en el DNS, no es mandatorio y de hecho todo va a funcionar debidamente si no se hace, pero conforme pasa el tiempo la lista se puede ir haciendo mas grande de manera innecesaria, otro tipo de registro que tenemos es el servidor de nombre NS y la Inicio de Autoridad (SOA).

📗 🗐 (igual que la carpeta principal)	Inicio de autoridad (SOA)	[34], smb4server01.sienic.s	11/01/2014 17:00:00
📗 🗐 (igual que la carpeta principal)	Servidor de nombres (NS)	smb4server01.sienic.site.	static
📗 🗐 (igual que la carpeta principal)	Host (A)	192.168.0.20	static
blue01	Host (A)	192.168.0.40	30/12/2013 8:00:00
EASGS-PC	Host (A)	192.168.0.30	26/12/2013 11:00:00
EASGS-PC01	Host (A)	192.168.0.30	26/12/2013 15:00:00
easgs-PC03	Host (A)	192.168.0.30	26/12/2013 15:00:00
EASGS-PC07	Host (A)	192.168.0.35	23/01/2014 16:00:00
easgs10	Host (A)	192.168.0.50	11/01/2014 18:00:00
easgs11	Host (A)	192.168.0.36	11/01/2014 18:00:00
smb4server01	Host (A)	192.168.0.20	static

En la siguiente imagen podemos ver un registro (A) en detalle, esta informacion se obtiene al dar clic con el boton secundario del mouse sobre el registro y seleccionando **propiedades**, este registro es de una computadora con el hosname EASGS-PC01, generalmente este registro se crea automaticamente al unir la maquina al dominio.

ost (A) Seguridad	
Host (si se deja en blanco, se us	sa el nombre del dominio primario):
EASGS-PC01	
Nombre de dominio completo (F	QDN):
Nombre de dominio completo (Fi EASGS-PC01.sienic.site	QDN):
Nombre de dominio completo (Fi EASGS-PC01.sienic.site Dirección IP:	QDN):

En la siguiente imagen vemos con detalle el registro (SOA) que contiene informacion acerca de la zona DNS, esta informacion se obtiene al dar clic con el boton secundario del mouse sobre el registro y seleccionando propiedades.

Servidores de nombres	VINS	Transferencias	de zona	Seguridad
General		Inicio de aut	oridad (SC	A)
Número de serie:				
34			In	icremento
Servidor principal:				
smb4server01.sienic.site.			E	xaminar
Persona responsable:				
hostmaster.sienic.site.			E	xaminar
Intervalo de actualización:	15	Minutos	•	
Intervalo de reintento:	10	Minutos	•	
Expira después de:	1	Días	•	
TTL mínimo (predeterminado):	0	Días	•]	
TTL para este registro: 0		1 :0 :0	(DDDDD:I	HH.MM.SS)

En la siguiente imagen se muestra informacion detallada del registro NS, esta informacion se obtiene al dar clic con el boton secundario del mouse sobre el registro y seleccionando propiedades.

General	-	Inicio de a	utoridad (SC	DA)
Servidores de nombres	WINS	Transferencia	is de zona	Seguridad
Fara agregar servidores Servidores de nombres:	de nombres	s a la lista, haga	ciic en Agre	gar.
Nombre de dominio co	mpleto (FQI	DN) del servi	Dirección	IP
smb4server01.sienic.sit	te.		[192.168.0	0.20]
Agregar Modi	ficar)	Quitar		

Al hacer clic con el boton secundario del mouse sobre la zona se mostrara un meno desplegable que nos da la opcion de agregar Registro A, CNAME y MX, los registro MX son para los servidores de correo electronico.

 serveradmin - [Raíz de consola\DNS\192.168.0 Archivo Acción Ver Favoritos Ventana Archivo Ección De Savoritos Ventana 	20\Zonas de 🕁squeda dir a Ayuda	ecta\sienic.site]
 Raíz de consola Administración de directivas de grupo DNS 192.168.0.20 Registros globales Zonas de búsqueda directa sienic.site msdcs.sienic.site Zonas de búsqueda inversa 	Nombre sites tcp udp DomainDnsZon EASGS-PC01 ForestDnsZones (igual que la car	Actualizar archivo de datos del servidor Volver a cargar Host nuevo (A o AAAA) Alias nuevo (CNAME) Nuevo intercambio de correo (MX) Dominio nuevo Delegación nueva Registrar puesos

Agregando un registro (A)

Para agregar un nuevo registro (A) damos clic con el boton secundario del mouse sobre la zona seleccionamos la opcion **Host nuevo (A o AAA)**.

📔 Raíz de consola	Nombre	Volver a carear
 Administración de directivas de grupo DNS 192.168.0.20 Registros globales Conas de búsqueda directa sienic.site 	 _sites _tcp _udp DomainDnsZones EASGS-PC01 ForestDnsZones 	Voiver a cargar Host nuevo (A o AAAA) Alias nuevo (CNAME) Nuevo intercambio de correo (MX) Dominio nuevo Delegación nueva

En la siguiente ventana ponemos el nombre de la PC en el campo **Nombre**, en **Direccion IP** ponemos la direccion IP que tiene la maquina y damos clic en **Agregar Host**

lost nuevo	
No <mark>m</mark> bre (si se deja en blan primario):	co, se usa el nombre del dominio
EASGS-PC15	
Nombre de dominio comple	to (FQDN):
EASGS-PC15.sienic.site.	
Dirección IP:	
192.168.0.65	
Crear registro del punt	ero (PTR) asociado
Permitir a cualquier usu DNS con el mismo nomb	ario autenticado actualizar registros re de propietario
	Agregar host Cancelar

Nos aparecera un cuadro de dialogo como el siguiente, damos clic en aceptar.



Nota: Los registros A se crean automaticamente cuando se une un PC al dominio.

Eliminar un registro (A)

Para eliminar un registro (A) seleccionamos el registro y le damos clic con el boton secundario del mouse, luego seleccionamos **Eliminar**

FASGS-PCL5	Hart /A)	192 168.0.65
	Eliminar	
	Propiedades	
	Ayuda	

En el siguiente cuadro de dialogo damos clic en Si



Agregando un registro (MX)

Para agregar un registro MX primero debemos crear el registro (A) luego seleccionamos **Nuevo intercambio de correo (MX)** del menu desplegable, se mostrara un cuadro de dialogo como el que se muestra a continuacion, en este cuadro damos clic en **examinar** y buscamos el registro (A) del servidor que sera el encargado de manejar el correo.

Agente de intercambio de correo (MX)	
Host o dominio secundario:	
De forma predeterminada, DNS usa el non crea un registro de correo Exchange. Pue secundario, pero en la mayoría de las impl se deja en blanco.	nbre de dominio primario cuando de especificar un host o nombre ementaciones, el campo anterio
Nombre de dominio completo (FQDN):	
sienic.site.	
Nombre de dominio completo (FQDN) del s	ervidor de correo electrónico:
	Examinar
Prioridad del servidor de correo:	

Una vez encontrado el registro (A) damos clic en aceptar

Nombre	Tipo	Datos	Marca de t	
EASGS-PC	Host (A)	192, 168.0.30	26/12/201	
EASGS-PC01	Host (A)	192.168.0.30	26/12/201	
easgs-PC03	Host (A)	192.168.0.30	26/12/201	
EASGS-PC07	Host (A)	192.168.0.35	23/01/201	
easgs 10	Host (A)	192.168.0.50	11/01/201	Ε
easgs 11	Host (A)	192.168.0.36	11/01/201	- 54
smb4serve	Host (A)	192.168.0.20	static	-
elección:	EASGS-PC07	sienic.site		
pos de registro:	Hosts (regist	ros A)		+

Luego ponemos la **prioridad** que tendra el servidor de correo y damos clic en **aceptar**, con eso ya tenemos nuestro registro (MX)

Agente de intercambio de correo (MX)	
Host o dominio secundario:	
De forma predeterminada, DNS usa el nom crea un registro de correo Exchange. Puec secundario, pero en la mayoría de las imple se deja en blanco.	bre de dominio primario cuando de especificar un host o nombre ementaciones, el campo anterio
Nombre de dominio completo (FQDN):	
sienic.site.	
sienic.site. Nombre de dominio completo (FQDN) del se	ervidor de correo electrónico:
sienic.site. Nombre de dominio completo (FQDN) del se EASGS-PC07.sienic.site	ervidor de correo electrónico: Examinar
sienic.site. Nombre de dominio completo (FQDN) del se EASGS-PC07.sienic.site Prioridad del servidor de correo:	ervidor de correo electrónico: Examinar

En la siguiente pantalla utilizamos nslookup para verificar que el registro MX este correcto.

```
C:\Windows\system32\CMD.exe - nslookup
Microsoft Windows [Uersión 6.1.7600]
Copyright (c> 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\supervisor>nslookup
Servidor predeterminado: UnKnown
Address: 192.168.0.20
> server 192.168.0.20
Servidor `redeterminado: [192.168.0.20]
Address: 192.168.0.20
> set g=MX
> sienic.site
Servidor: [192.168.0.20]
Address: 192.168.0.20
sienic.site MX preference = 10, mail exchanger = EASGS-PC07.sienic.site
sienic.site nameserver = smb4server01.sienic.site
EASGS-PC07.sienic.site internet address = 192.168.0.35
smb4server01.sienic.site internet address = 192.168.0.20
> _
```

DHCP

Instalacion y configuracion del DHCP

El servicio DHCP nos permite brindar direcciones IP de manera automatica asi como tambien otros parametros a las estaciones de trabajo ahorrandonos asi la tarea de estar configurando cada PC de la red de manera manual, para configurar el servicio DHCP nos vamos a **Yast/Software/Instalar / desinstalar software**.



× 🎯		YaST2		\odot
Arc <u>h</u> ivo <u>P</u> aquete Configura Ver <u>Buscar</u> Grupos <u>R</u>	ción <u>D</u> ependencia PM Resumen de la <u>i</u>	s <u>O</u> pciones E <u>x</u> tr nstalación Patro <u>n</u> e	ras Ayuda s	(A
Patro <u>n</u> es <u>G</u> rupos de paquetes	▼ <u>B</u> uscar	▼ Paquete	Resumen	Instalado (Dispor Tamaño
Grupos <u>R</u> PM Idiomas				
<u>R</u> epositorios B <u>u</u> scar				
Resumen de la <u>i</u> nstalación				

Damos clic en Ver y seleccionamos la opcion Patrones

En patrones seleccionamos **Servidor DHCP y DNS** y en el panel derecho seleccionamos los paquetes **dhcp-server** y **yast2-dhcp-server**.



Se mostrara una ventana msotrando el progreso de la instalacion.

	YdST2	8 6 8
Ejecutar la	a instalación	
Acci <u>o</u> nes ejecut	adas:	
nstalando yast	2-dhco-server-3.0.0-2.1.4.noarch.rom (tam	año instalado 2,82
nstalando dhci MB)	p-server-4 2 5 P1-0.5.2.1.x86_64.rpm (tama	año instalado 1.99
Instalando dhep	o-server-4,2,5,P1-0.6,2,1,x86_64,rpm (tama	ño instalaco 1,99 MB)
Instalando dhep	o-server-4.2.5.P1-0.6.2.1.x86_64.rpm (tama 0%	ño instalaco 1,99 MB)
Instalando dhop	o-server-4.2.5.P1-0.6.2.1.x86_64.rpm (tama 0%	ño instalaco 1,99 MB)
Instalando dhop	c-server-4.2.5.P1-0.6.2.1.x86_64.rpm (tama 0% uetes(Restante: 1.99 MB 1 paquetes)	ño instalaco 1,99 MB)
Instalando dhop Instalando paqu	o-server-4.2.5.P1-0.6.2.1.x86_64.rpm (tama 0% uetes(Restante: 1.99 MB 1 paquetes) 58%	ño instalaco 1,99 MB)

Una vez instalados los paquetes nos vamos a Yast/Servicios de red/Servidor DHCP



En la siguiente ventana seleccionamos la interface por medio de la cual vamos a asignar las direcciones IP y damos clic en **Seleccionar** y checamos la opcion **Abrir cortafuegos para las interfaces seleccionadas.**

Seleccionada	∨ Nombre de la interfaz	Nombre de dispositivo	I IP I
	eno16777736	82545EM Gigabit Ethernet Con	troller (192.168.0.20

Damos clic en siguiente.

Asistente del servidor DHCP (1 de 4): Selección de tarjetas Tarjetas de red para el servidor DHCP Seleccionada VINombre de la interfaz INombre de dispositivo IP INT ENDI 6777736 82545EM Gigabit Ethernet Controller (192.168.0.20 Seleccionar Seleccionar Deseleccionar	K 💿		YaST2		\odot \odot \otimes
Tarjetas de red para el servidor DHCP Seleccionada Nombre de la interfaz Nombre de dispositivo IP eno16777736 82545EM Gigabit Ethernet Controller (192.168.0.20) Seleccionar Deseleccionar	Asistente	e del servidor DHC	P (1 de 4): Selección	de tarjet	as
Seleccionada V : Nombre de la interfaz : Nombre de dispositivo : IP : x eno16777736 82545EM Gigabit Ethernet Controller (192.168.0.20) Seleccionar Deseleccionar Seleccionar Deseleccionar Abrir cortafuegos para las interfaces seleccionadas Siguiente	Tarjetas de red	para el servidor DHCP			
x eno16777736 82545EM Gigabit Ethernet Controller (192.168.0.20 Seleccionar Deseleccionar ✓ Abrir cortafuegos para las interfaces seleccionadas Avuda Atrás Cancelar Siguiente	Seleccionada	∨ i Nombre de la interfaz	Nombre de dispositivo	: IP	ł
Seleccionar Deseleccionar ✓ Abrir cortafuegos para las interfaces seleccionadas Avuda Atrás Cancelar Siguiente	x	eno16777736	82545EM Gigabit Ethernet Cont	troller (192.16	68.0.20
Seleccionar Deseleccionar					
Abrir cortafuegos para las interfaces seleccionadas Avuda Atrás Cancelar Siguiente		Selec	cionar Deseleccionar		
Abrir cortafuegos para las interfaces seleccionadas Avuda Atrás Cancelar Siguiente					
Abrir cortafuegos para las interfaces seleccionadas Avuda Atrás Cancelar Siguiente					
Avuda Atrás Cancelar Siquiente	Abrir cortaf	uegos para las interfaces sele	ccionadas		
Avuda Atrás Cancelar Siquiente	0				
Avuda Atrás Cancelar Siguiente					
Avuda Atrás Cancelar Siquiente					
	Ayuda	Atrás	Cancelar		Siguiente

En la siguiente ventana ponemos las opciones tal a como se muestran en la siguiente figura y damos clic en **siguiente**, adaptando las opciones a sus necesidades.

Asistente del servidor DH	CP (2 de 4): Configuración glo	bal
Compatibilidad para LDAP		
Nombre de <u>d</u> ominio	Servidor horario N <u>T</u> P	
sienic.site		
IP del se <u>r</u> vidor de nombres primario	Servidor de im <u>p</u> resión	
192.168.0.20		
IP del servidor de nombres <u>s</u> ecundario	Servidor <u>W</u> INS	
Pasarela predeter <u>m</u> inada (Router)	Ti <u>e</u> mpo de asignación predeterminado <u>U</u> nidade	s
192.168.0.1	4 Horas	•
AyudaAtrás	<u>C</u> ancelar	S <u>i</u> guiente

En esta ventana se configura el ambito de direcciones IP que asignara este servidor, ponemos la **Primera direccion IP** y la **Ultima direccion IP** del rango que deseamos configurar y damos clic en siguente.

Red actual		ara de red actual	Bi <u>t</u> s de máscara de rec
192.168.0.0	255	.255.255.0	24
Dirección IP mínima		ción IP má <u>x</u> ima	
192.168.0.1		.168.0.254	
ngo de direcciones IP			
Primera dirección IP	Ú <u>l</u> tim	a dirección IP	
192.168.0.100		.168.0.254	
Permitir <u>B</u> OOTP dinám	ico		
mpo de asignación			
Pr <u>e</u> determinado	<u>U</u> nidades	<u>M</u> áximo	U <u>n</u> idades
4	Horas	• 2	Días 🔹

En la siguiente ventana configuramos el servicio para que arranque junto con el sistema operativo y damos clic en **terminar**.

× 😡	YaST2	\odot \odot \otimes
Asistent	te del servidor DHCP (4 de 4):	Inicio
Inicio del servi	icio	
<u>D</u> urante <u>M</u> anualn	el arranque nente	
	Configuración <u>e</u> xperta del servidor DHCP]
Ayuda	<u>A</u> trás <u>C</u> ancelar	Ţerminar

Se mostrara una ventana con el progreso de las configuraciones.

×		Ya	IST2		\odot \odot \otimes
Gu	ardando I	a configurad	ión del se	ervidor D	НСР
	Escribir la confi	guración del servido	r DHCP		
→	Escribir la confi	guración del cortafu	egos		
-	Reiniciar el sen	idor DHCP			
-	Escribir la confi	guración del servido	r DNS		
Escri	ibiendo la config	uración del cortafue	gos		
		2	:5%		
Ay	uda	<u>A</u> trás	<u>C</u> ancela		Terminar

Configurar las estaciones de trabajo como clientes DHCP.

El siguiente paso es configurar las estaciones de trabajo para que hagan uso del servidor DHCP, para esto damos clic con el boton secundario del mouse sobre el icono de red y seleccionamos **Abrir el Centro de redes y recursos compartidos**.



En la siguiente ventana hacemos clic en la opcion **Cambiar configuracion del adaptador**.



Seleccionamos la conexión que deseamos configurar y le damos clic con el boton secundario del mouse y seleccionamos **Propiedades** del menu desplegable.



Luego seleccionamos Protocolo de Internet version 4 (TCP/IPv4) y damos clic en propiedades.

inciones de red		
Cone <mark>c</mark> tar usando	2	
Conexión c	de red Intel(R) PRO/1	000 MT
		Configurar
Esta conexión us	a los <mark>sig</mark> uientes eleme	entos:
🗹 📑 Cliente p	ara redes Microsoft	
Program	ador de paquetes Qo	S
Compart	ir impr <mark>esoras y archivo</mark>	os para redes Microsoft
Protocol	o de Internet versión	6 (TCP/IPv6)
Protocol	o de Internet versión	4 (TCP/IPv4)
🗹 🔺 Controla	dor de E/S <mark>del</mark> asigna	ador de detección de topol
🗹 🔺 Respon	dedor de detección d	e topologías de nivel de v

El la siguiente ventana seleccionamos las opciones **Obtener una direccion IP automaticamente** y **Obtener la direccion del servidor DNS automaticamente.**

seneral	Configuración alternativa			
Puede red es consult apropia	hacer que la configuración IP se a: compatible con esta funcionalidad. ar con el administrador de red cuá ada.	signe autor De lo contr I es la confi	iátican ario, c guraci	nente si la leberá ón IP
0	btener una dirección IP automática	amente		
_© U:	sar la siguiente dirección IP:			
Dire	cción IP:		- 6	- 8 - Î
Mási	cara de subred:			- 0
Puer	ta de enlace predeterminada:			
0	btener la dirección del servidor DN	S automátic	amen	te
- © U:	sar las siguientes direcciones de se	rvidor DNS	:	
Serv	idor DNS preferido:	4	- 12	141
Serv	idor DNS alternativo:	,		
V	'alidar configuración al salir	Opc	iones	avanzadas

Permisos locales

Permisos locales

En algunas ocaciones necesitamos que un usuario tenga permisos locales administrativos en la estacion de trabajo, esto debido a alguna aplicación que asi lo requiera o por cualquier otro motivo, el problema es que si el usuario no pertenece al grupo Domain Admins su sesion se iniciara con permisos limitados, el problema es que no podemos andar agregando usuarios al grupo de Domain Admins, para resolver este problema vamos a configurar permisos locales con la cuenta de dominio del usuario.

Para configurar los permisos locales con la cuenta de dominio nos vamos a **Panel de** control/Cuentas de usuario/Cuentas de usuario/Administrar cuentas de usuario y damos clic en agregar.

Use la siguiente l equipo, así como	ista para conceder o de para cambiar contrase	enegar acceso de usuario a su eñas y otras configuraciones.
Nombre de usuario	Dominio	Grupo
Na easgs	EASGS-PC07	Administradores
🕵 Supervisor	SIENIC	Administradores

En la siguiente ventana damos clic en el icono Examinar.



Escribimos el nombre de la cuenta de usuario de dominio y damos clic en **Comprobar nombres**.

eleccionar Usuario	- ?
Seleccionar este tipo de objeto:	
Usuario	Tipos de objeto
Desde esta ubicación:	
Todo el directorio	Ubicaciones
Escriba el nombre de objeto para seleccionar (<u>ejemplos</u>):	
easgs03	Comprobar nombre

Una vez comprobado el nombre damos clic en Aceptar.

Comprobar nom	(easgs03@sienic.site)	easgs03 (eas
		~
ptar C	nes avanzadas	Opciones a

En la siguiente ventana nos mostrara el nombre de usuario y automaticamente el dominio, damos clic en **Siguiente.**

Agregar nuevo usuario		
	Escriba el nom permisos de u Nombre de usuario: Dominio: Haga clic en S	nbre y dominio de un usuario para concederle iso en este equipo. easgs03 SIENIC Examinar Siguiente para continuar.
		< Atrás Siguiente > Cancelar

En esta ventana vamos a seleccionar el nivel de permisos locales que va a tener el usuario, seleccionamos **Administrador** si damos clic en **Otro** y abrimos la lista deplegable se nos mostraran mas opciones, una vez hecha nuestra selección damos clic en finalizar.

(X)	© Usuario e Los usua del softw que no a	est que se concede rios con cuentas es vare y pueden camb fecte a los demás u	(Grupo de usuarios) (ándar pueden usar la mayoría iar cualquier configuración suarios.
	Administ Los adm pueden l configur a los adr una confi afectar a	rador inistradores tienen hacer los cambios q ación de las notifica ninistradores que p firmación antes de r otros usuarios.	(Grupo de administradores, acceso completo al equipo y ue deseen. Según la ciones, es posible que se pida oporcionen su contraseña o ealizar cambios que puedan
	🔿 Otro:	Duplicadores	

En la siguiente ventana se muestra el usuario ya agregado a la lista de usuarios, podemos ver que este es miembro del grupo local de la estacion de trabajo Administradores, damos clic en **Aceptar**.

opciones avanzado	IS	
Use la siguiente l equipo, así como Usuarios de este equipo:	ista para conceder o de o para cambiar contrase	enegar acceso de usuario a s eñas y otras configuracione:
Nombre de usuario	Dominio	Grupo
Neasgs	EASGS-PC07	Administradores
🔍 easgs03	SIENIC	Administradores
Supervisor	SIENIC	Administradores
	Agregar	Quitar Propiedade
⊂Contraseña para easgs03	Agregar	Quitar Propiedade
- Contraseña para easgs03 No se puede c	Agregar } ambiar la contraseña d	Quitar Propiedade e easgs03.
- Contraseña para easgs03 No se puede c	Agregar ambiar la contraseña d	Quitar Propiedade e easgs03. Restablecer contraseña

Ahora este usuario tendra permisos de administrador local en esta estacion de trabajo, por lo que si una aplicación tiene este requierimiento funcionara sin problema, sera responsabilidad del administrador del dominio implementar las politicas de seguridad o GPO necesarias para limitar el acceso de este usuario a las unidades del sistema, panel de control, conexiones de red etc.

Creditos

Este manual no hubiera sido posible sin la información contenida en los siguientes sitios, ni la ayuda brindada por los autores y participantes:

https://lists.samba.org/

http://wiki.samba.org/index.php/Samba

http://easgs.wordpress.com/2009/11/23/opensuse-11-2-con-samba-guia-ilustrada/

http://conradjonesit.wordpress.com

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection

http://forums.opensuse.org

La portada gracias a: Daniel Salazar ADNX

Para comentarios y preguntas contactar al autor: Eduardo Adolfo Sotomayor G. adolfo2007@starlinux.net http://easgs.wordpress.com

