

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ
FACULTAD DE CIENCIAS E INGENIERÍA

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

5ta Práctica (tipo b)

(2024-2)

Indicaciones generales:

- La presentación, la ortografía y la gramática de los trabajos influirán en la calificación.
- Cada alumno, deberá realizar un registro escrito de las acciones y resultados obtenidos en cada pregunta.

Puntaje total: 20 puntos

1. Pregunta 1 (3 puntos) Creación de instancias: Windows Server 2025

Crear tres (3) instancias EC2 Windows Server 2025, desde la consola de administración AWS. Considerar las siguientes características y condiciones.

- Considere la VPC que creó en el primer laboratorio. Esta cuenta con 4 subredes: 2 subredes públicas y 2 subredes privadas. Elija un entorno de trabajo con una subred pública y una subred privada, considerando que su infraestructura de Directorio Activo será implementada en una subred privada.
- La primera instancia de nombre GW, debe ser la única creada en una subred pública. Además, tendrá asignado un IP elástico. A través de esta instancia, vía escritorio remoto a IPs privados accederá a su despliegue.
- Una instancia representará a un Controlador de Dominio (DC) y la otra, un servidor miembro del dominio (SERV).
- AMI: Windows Server 2025 Base , para todos los casos.
- Tamaños: t2.medium, para el DC; y, t2.micro para el servidor miembro.
- Red: Parámetros de configuración por defecto y configurar una misma zona de disponibilidad.
- Almacenamiento: Configuración por defecto (30GiB)
- Grupos de Seguridad: Editar uno existente con permisos por defecto para instancias Windows o crear uno (nombre MiDominio), que permita conexión desde Escritorio Remoto (puerto 3389) solo a su red personal (considerada su red de administración). Agregar además una regla que permita todo tráfico de red en la subred privada común a las instancias (10.0.0.0/16 o similar).
- Nombre desde la consola de administración AWS las instancias, según corresponda, como: GW, DC y SERV respectivamente.

Presente evidencia de creación de las tres (3) instancias, según lo solicitado.

Verifique el acceso a cada una de las instancias y renombre cada una de ellas de modo que coincida su nombre de host con el asignado en la consola AWS. Presente evidencia al ejecutar el comando: *hostname*.

2. Pregunta 2 (4 puntos) Directorio Activo: Primer Controlador de Dominio

Configurar el servidor de nombre DC, como PDC (Primary Domain Controller); es decir, el primer controlador de dominio con DNS integrado. Considerando lo siguiente:

- Nombre de dominio: SuApellido.adso
- Anotar el nivel funcional de bosque y de dominio; asegurándose se encuentre en el nivel más alto.
- Anotar nombre NetBIOS del dominio.
- Copie y pegue el script PowerShell equivalente para toda la configuración previa realizada de manera gráfica:
- Ignorar las advertencias por DHCP (asignación automática IP), pues se considera “fijo” para la instancia.
- Ignorar advertencias sobre DNS, considerando no existe delegación para el dominio a crear. Se instala el servicio DNS y configura como servidor primario del nuevo dominio. Al culminar la instalación y luego de reiniciar presente evidencia de la zona y tipo de DNS creado.
- Cambie la contraseña del usuario Administrator de dominio y verifique que puede conectarse, vía escritorio remoto a DC, con esas credenciales.

3. Pregunta 3 (2 puntos) Directorio Activo: Primer servidor miembro

Recuerde que el servicio DNS es necesario para encontrar al controlador de dominio, por lo que se requiere que este parámetro en SERV apunte al IP del servidor DC, antes de proceder a unirlo al dominio.

Proceda con la asignación DNS y luego evidencie existe comunicación a través del comando *ping* desde SERV al controlador de dominio (DC) por su nombre completo de dominio (FQDN, no usar IP privado).

Configurar el servidor SERV, como el primer servidor miembro del dominio y presente evidencia de que fue unido al dominio satisfactoriamente.

Evidencie, que logra acceder al servidor miembro con el usuario Administrator de su dominio (no necesita descifrar la contraseña con su llave privada, solo recordar la contraseña asignada en la pregunta anterior)

4. Pregunta 4 (2 puntos) Directorio Activo: OUs – Equipos y Usuarios

En su dominio, desde Active Directory Users and Computers, proceda a crear las Unidades Organizativas (OUs): Servidores y Usuarios.

Ubique en la OU Servidores el único objetos equipo de su dominio (SERV).

En la OU Usuarios, crear desde el entorno gráfico dos usuarios de dominio: Un usuario con el formato SuNombre.SuApellido y que tenga los mismos privilegios que el usuario administrador de dominio; es decir pertenece a los mismos grupos. Y, User1 con los privilegios por defecto al crear un usuario de dominio. Mencione los grupos a los que pertenece cada usuario creado.

Valide que puede conectarse vía Escritorio Remoto, a SERV y DC, con el primer usuario creado. ¿Porqué cree que esto es posible?

Si intenta, con el usuario User1, conectarse vía Escritorio Remoto a SERV, no le será posible. ¿Qué mensaje le apareció al intentarlo? ¿Miembro de qué grupo local, sin ser Administrador, en SERV, deberá pertenecer User1 para conseguir conectarse vía Escritorio Remoto?

Evidencie, que el usuario User1 fue agregado al grupo necesario y logró establecer sesión remota a SERV. Sugerencia: Usar comando *netstat -ant*

5. **Pregunta 5** (2 puntos) **Directorio Activo: Elevación de privilegios con runas**

Con la sesión iniciada con User1 en SERV, notar que no cuenta con privilegios elevados de administrador local, ni de dominio (User1 es solo miembro del grupo Domain Users).

Entonces para proceder con la creación de usuarios en el dominio, requiere elevar privilegios a nivel del grupo Domain Admins.

Desde una ventana cmd, ejecutada sin privilegios elevados, con el comando *runas* (Ejecutar como) invoque otra ventana cmd como el usuario SuNombre.SuApellido que es administrador de dominio:

runas /user:SuNombre.SuApellido@SuApellido.adso cmd

Desde esta nueva consola, proceder a crear el usuario User2, con privilegios por defecto, a través de línea de comandos y otro usuario User3 que sea miembro del grupo Administradores de Dominio (Domain Admins). Evidencie con el mismo comando que se crearon los usuarios antes mencionados con los atributos y grupos deseados. Puede, además, validarlo desde la consola gráfica en DC.

¿En qué OU fueron creados por defecto?

Asegúrese de ubicar todos los usuarios creados en la OU: Usuarios.

Nota: Revisar para crear usuarios *net user /?* ;y, para añadir a grupos *net group /?*

6. Pregunta 6 (2 puntos) Directorio Activo: PowerShell crear usuarios por lotes

Desde DC, usando PowerShell, cree el usuario User4, con privilegios estándar. Considere que el usuario está definido por un archivo separado por comas (Users.csv), en el que de igual manera podría definir muchos más usuarios por cada línea (notar la primera línea en mayúscula es la cabecera que define los campos):

USERPRINCIPALNAME,SAMACCOUNTNAME,NAME,GIVENNAME,SURNAM
E,EMAILADDRESS,PASSWORD

User4@SuApellido.adso,User4,Usuario4,Usuario,Cuatro,user4@email.adso,Passw0rd

Y usará el siguiente script en PoweShell:

```
Import-Csv .\Users.csv | ForEach-Object {New-ADUser -UserPrincipalName  
$_.userPrincipalName -SamAccountName $_.SamAccountName -Name $_.Name -  
GivenName $_.GivenName -Surname $_.SurName -EmailAddress $_.EmailAddress -  
Path " OU=Usuarios,DC=carpio,DC=adso " -AccountPassword (ConvertTo-  
SecureString $_.Password -AsPlainText -force) -Enabled $True -PassThru}
```

Sugerencias: Use Windows Power Shell ISE y su ejecución en modo script. Ejecute desde la ruta en la que está el archivo Users.csv. Notar que debe cambiar los valores que corresponde a su dominio (su apellido).

Evidencie la creación del usuario desde el servidor miembro, con privilegios de administrado, con el comando *net user*.

7. Pregunta 7 (3 puntos) Directorio Activo: Creación de Políticas de Grupo

En el servidor miembro SERV, habilitar la característica (feature) Group Policy Management, usando Server Manager.

Recuerde que debe ser administrador local del servidor para agregar la característica y debe ser administrador de dominio para gestionar la característica añadida. Ambas condiciones son satisfechas por los usuarios miembros del grupo Domain Admins, entonces se sugiere ejecutar estas tareas con un usuario miembro de este grupo.

Crear las siguientes políticas:

- Una política a los equipos, de nombre WSUSPolicy, desde una plantilla administrativa que permita a los servidores (OU Servidores) se actualicen automáticamente desde un servidor WSUS (no se ha desplegado y se asume existe en su infraestructura con nombre ServerWSUS). Considere configurar al menos:
 - Configure Automatic Updates: Modo 4, cada día y hora 12:00.
 - Specify intranet Microfoft update servide location:
http://ServerWSUS.SuApellido.adso:8530

- Una política a los usuarios, de nombre UserPolicy, desde una plantilla administrativa al Escritorio, que impida a los usuarios ver la papelera de reciclaje en el escritorio. Deberá afectar a todos los usuarios en la OU Usuarios.

8. Pregunta 8 (2 puntos) Directorio Activo: Verificar aplicación y configuración de políticas de grupo a usuarios y equipos.

Aplicadas las GPOs: WSUSPolicy a OU Servidores y UsersPolicy a OU Usuarios.

Reinicie el servidor miembro (SERV), para asegurar que la política al equipo tenga efecto y muestre evidencias de la correcta aplicación de las respectivas GPOs tanto al equipo como al usuario elegido para autenticarse (puede ser cualquiera de los alojados en la OU Usuarios).

Sugerencias:

1. En modo gráfico puede usar la propia consola GPMC, mediante el asistente de resultados de directiva de grupo (Group Policy Results) ubicado en la parte inferior del panel izquierdo de la consola.
2. En modo comando, puede verificar los resultados, elevando privilegios con el comando *gpresult /V*. Sin elevar privilegios, solo se mostrará parcialmente y en función de los privilegios del usuario que ejecuta el comando. Además, puede redirigir el resultado, por ejemplo: *gpresult /V > gpresultGPOLab.txt*.
Para la política a los equipos también puede usar: *gpresult /R /SCOPE computer*
Observar en el resultado :Appliet Group Policy Objects (Computer Settings y User Settings)
3. Por inspección podrá observar que en el escritorio no aparece el ícono de Papelera de Reciclaje.

Elaborado por: Mario Carpio

Profesor del curso: Mario Carpio

Lima, 12 de noviembre del 2024.