Administración de Sistemas Operativos - 1a Evaluación (RA 4 – CE c, i)

Unidad Didáctica 4. Configuración multiusuario centralizada

**Preparar un videotutorial, con una duración máxima de 20 minutos, sobre la**

**administración remota de sistemas Windows. El trabajo abarca la administración**

**remota con las herramientas:**

* **WinRS en Cmd.**
* **Cmdlets de PowerShell.**
* **Herramienta “Windows Admin Center**”.

**De cada una de las herramientas incluimos una introducción donde se explicarán, de forma breve, conceptos teóricos (protocolo, puerto, certificados, etc.), instalación y configuración.**

1. **Qué es la administración remota:**

La administración remota consiste en la capacidad de gestionar, controlar y solucionar problemas de sistemas informáticos ubicados en lugares diferentes al del administrador, utilizando una conexión de red

* **Ventajas principales**
  + Permite a los administradores supervisar y realizar tareas en computadoras o servidores sin estar físicamente presentes. Esto es especialmente útil para trabajar con equipos en diferentes oficinas, ciudades o países.
  + Menos necesidad de personal técnico en cada ubicación física.
  + Ideal para empresas que manejan redes grandes con cientos o miles de dispositivos.
* **Herramientas a usar:**
  + **WinRS en Cmd:** herramienta para ejecutar comandos remotos mediante el protocolo WS-Management**.**
  + **Cmdlets de PowerShell:** comandos específicos para la administración remota utilizando el protocolo WinRM (Windows Remote Management).
  + **Windows Admin Center:** interfaz gráfica basada en web para gestionar de forma remota servidores y estaciones de trabajo Windows

**Conceptos sobre WinRS en Cmd:**

1. **Protocolo: WS-Management**

El protocolo WS-Management (WS-Man), basado en SOAP, permite la comunicación entre dispositivos para realizar tareas administrativas de forma remota. Es una herramienta clave en entornos empresariales para la gestión centralizada de sistemas.

1. **Puertos Utilizados:**

Los puertos son los "canales" por los que se envían y reciben datos entre equipos. WinRM utiliza dos principales:

* **5985**: Para comunicación no cifrada mediante HTTP.
* **5986**: Para comunicación segura mediante HTTPS (recomendado).

Si usas el parámetro /usessl, el sistema emplea automáticamente el puerto 5986 para conexiones cifradas.

1. **Certificados:**

Un certificado es un archivo digital que valida la identidad de un servidor o equipo y permite establecer conexiones seguras mediante HTTPS.

* **Certificado autofirmado**: Útil para pruebas, pero no seguro a largo plazo.
* **Certificado de una CA**: Ideal para entornos empresariales, garantiza seguridad y confianza externa

**Instalación de WinRS**

1. **Abrir el símbolo del sistema como administrador**
2. **Instalar WinRS**

Ejecuta el siguiente comando para instalar el componente WinRM que incluye WinRS:

* winrm quickconfig

1. **Crear un Listener HTTP**

Ejecuta el siguiente comando para habilitar un Listener HTTP en el puerto predeterminado (5985):

* winrm create winrm/config/Listener?Address=\*+Transport=HTTP

Y para crear los permisos de Firewall usamos:

* netsh advfirewall firewall add rule name="WinRM HTTP" protocol=TCP dir=in localport=5985 action=allow

1. **Verificar la instalación y configuración**

* winrm enumerate winrm/config/Listener

**Uso de WinRS**

* **Instalación de algún rol o característica:**winrs -r:Sistemas -u:usuario -p:usuario dism /online /enable-feature /featurename:TelnetClient
* **Configuración del nombre del equipo y la red:**winrs -r:Sistemas -u:usuario -p:usuario netdom renamecomputer %COMPUTERNAME% /newname:ServidorCentral

* **Creación/modificación de variables de entorno:**Comando: winrs -r:NombreDelEquipo setx NUEVA\_VARIABLE valor\_variable

.

* **Creación/modificación de usuarios y grupos:**Comando: winrs -r:NombreDelEquipo net user UsuarioContraseña /add
* **Inicio/parada de servicios:**Comando: winrs -r:NombreDelEquipo net start Servicio
* **Configuración de directivas:**Comando: winrs -r:NombreDelEquipo secedit /configure /db secedit.sdb /cfg Directiva.inf /areas SECURITYPOLICY
* **Comprobación de actualizaciones:**Comando: winrs -r:NombreDelEquipo powershell -command "Install-WindowsUpdate"
* **Apagado/reinicio del servidor:**Comando: winrs -r:NombreDelEquipo shutdown /r /t 0

**Conceptos sobre Cmdlets de PowerShell**

1. **Protocolo: WS-Management**

PowerShell remota utiliza el protocolo WS-Management, basado en SOAP, para permitir la comunicación remota segura entre equipos y realizar tareas administrativas de forma eficiente.

1. **Puertos Utilizados:**
   * **5985 (HTTP)**: Comunicación no cifrada, recomendada solo en redes internas confiables.
   * **5986 (HTTPS)**: Canal seguro y cifrado, requiere un certificado válido para proteger las conexiones remotas
2. **Certificados:**
   * **Certificado autofirmado**: Adecuado para pruebas rápidas, pero no confiable a largo plazo.
   * **Certificado de una CA**: Esencial en entornos empresariales, garantiza validación y seguridad externa..

**Instalación y Configuración de Cmdlets de PowerShell**

1. **Abrir PowerShell como Administrador**
2. **Habilitar la Administración Remota en PowerShell**

Ejecuta el siguiente comando para habilitar la administración remota:

* Enable-PSRemoting -Force

1. **Verificar la Configuración**

Confirma que PowerShell remoto está correctamente habilitado y funcionando:

* Test-WSMan -ComputerName localhost

**Uso de Cmdlets de PowerShell**

* **Instalación de algún rol o característica:**Comando: Install-WindowsFeature -Name Web-Server -ComputerName NombreDelEquipo
* **Configuración del nombre del equipo y la red:**Comando: Rename-Computer -NewName "NuevoNombre" -ComputerName NombreDelEquipo
* **Creación/modificación de variables de entorno:**Comando: [System.Environment]::SetEnvironmentVariable("NuevaVariable", "Valor", "Machine")
* **Creación/modificación de usuarios y grupos:**Comando: New-LocalUser -Name "NuevoUsuario" -Password (ConvertTo-SecureString "Contraseña" -AsPlainText -Force)

* **Inicio/parada de servicios:**Comando: Start-Service -Name "NombreServicio"
* **Configuración de directivas:**Comando: Set-GPRegistryValue -Name "Directiva" -Key "RutaClave" -ValueName "NombreValor" -Type Dword -Value 1
* **Comprobación de actualizaciones:**Comando: Get-WindowsUpdate -ComputerName NombreDelEquipo
* **Apagado/reinicio del servidor:**Comando: Restart-Computer -ComputerName NombreDelEquipo

**Conceptos sobre Windows Admin Center**

1. **Protocolo y Puertos**

**HTTP/HTTPS:** utiliza el protocolo HTTPS para garantizar la seguridad de las comunicaciones. Todas las conexiones son cifradas, lo que protege la información administrativa

**Puerto utilizado**: Por defecto WAC usa el puerto 443 para conexiones seguras a HTTPS.

1. **Certificados de seguridad**

**Certificados SSL/TLS:** Durante la instalación, puedes optar por usar un certificado autofirmado o uno emitido por una autoridad certificadora (CA).

**Instalación de Windows Admin Center**

### **Descargar Windows Admin Center**

1. Accede al sitio oficial de Microsoft para descargar la herramienta:  
   [Descargar Windows Admin Center](https://www.microsoft.com/windows-admin-center).

### **Instalación paso a paso**

1. **Ejecutar el instalador**Una vez descargado, haz doble clic en el archivo ejecutable (WindowsAdminCenter.msi).
2. **Aceptar los términos de la licencia**Marca la casilla para aceptar los términos y condiciones y haz clic en **Siguiente**.
3. **Configurar el puerto**
   * Por defecto, Windows Admin Center utiliza el puerto **443** (HTTPS).
4. **Certificado SSL**
   * Puedes optar por usar un certificado autofirmado o proporcionar uno válido emitido por una autoridad certificadora (opcional para entornos seguros).
5. **Finalizar la instalación**Una vez completada, el instalador iniciará automáticamente Windows Admin Center

**Uso de Windows Admin Center**

**Instalación de algún rol o característica**: Utilizando la interfaz gráfica, accede a "Roles y características" y selecciona el rol deseado para instalarlo**.**

**Configuración del nombre del equipo y la red**: En la sección "Configuración del sistema", cambia el nombre del equipo y configura los ajustes de red.

**Creación/modificación de variables de entorno**: Desde "Configuración avanzada del sistema", edita las variables de entorno**.**

**Creación/modificación de usuarios y grupos**: Usa la sección "Usuarios y grupos locales" para administrar usuarios.

**Inicio/parada de servicios**: En la sección "Servicios", inicia o detén servicios según sea necesario.

**Configuración de directivas**: Usa la sección de "Directivas de grupo" para aplicar nuevas configuraciones.

**Comprobación de actualizaciones**: Accede a "Windows Update" para buscar e instalar actualizaciones.

**Apagado/reinicio del servidor**: Usa la opción de "Apagar o reiniciar" disponible en el menú principal.

**UBUNTU**

**Preparar un videotutorial, con una duración máxima de 20 minutos, sobre la administración remota de sistemas GNU/Linux. El trabajo abarca la administración remota con las herramientas:**

* **Webmin.**
* **Otra herramienta de administración web seleccionada a decisión del alumno. Esta decisión, a partir de un análisis previo, deberá ser justificada durante la introducción de la herramienta.**

**De cada una de las herramientas incluimos una introducción donde se explicarán, de forma breve, conceptos teóricos (protocolo, puerto, certificados, etc.), instalación y configuración.**

**Conceptos sobre Webmin**

Webmin es una herramienta de administración remota basada en web diseñada para gestionar sistemas operativos mediante una interfaz gráfica.

**Protocolo y Puerto**:

* Webmin utiliza los protocolos HTTP y HTTPS para comunicarse con los navegadores web.
* Por defecto, opera en el puerto **10000**, que debe estar habilitado en el firewall para permitir el acceso remoto
  + **sudo ufw allow 10000**

**Certificados**:

* Para garantizar la seguridad de las conexiones, Webmin soporta certificados SSL/TLS. Se puede usar un certificado autofirmado o integrar uno de una autoridad certificadora como Let's Encrypt

**Instalación de Webmin**

1. **Descargar manualmente la clave GPG:**

* wget -q -O jcameron-key.asc http://www.webmin.com/jcameron-key.asc

1. **Importar la clave con el método recomendado**

* sudo cp jcameron-key.asc /etc/apt/trusted.gpg.d/

1. **Verificar la configuración del repositorio**

Edita el siguiente archivo:

* sudo nano /etc/apt/sources.list.d/webmin.list

Agrega la siguiente línea:

* deb http://download.webmin.com/download/repository sarge contrib

Guarda el archivo y actualiza los índices del repositorio:

* sudo apt update

1. **Instalamos Webmin**

* sudo apt install webmin

**Uso de Webmin**

### **1. Configuración del nombre del equipo y la red**

* **Accede a Webmin.**
* En el menú de la izquierda, ve a **System** > **Networking**.
* Allí podrás modificar el **hostname** (nombre del equipo) y la configuración de la red, como la **IP address**, **netmask**, **gateway**, y otros parámetros relacionados con la red.
* Haz clic en **Save** después de realizar los cambios.

### **2. Creación/modificación de variables de entorno**

* Ve a **System** > **Environment Variables**.
* En esta sección, puedes agregar nuevas variables de entorno, modificar las existentes o eliminar aquellas que no sean necesarias.
* Haz clic en **Save** después de realizar cualquier cambio.

### **3. Gestión de paquetería**

* Dirígete a **System** > **Package Management**.
* Desde allí puedes buscar, instalar, eliminar o actualizar paquetes en el sistema.
* También puedes configurar los repositorios desde esta sección si es necesario.
* Selecciona el paquete que desees gestionar y sigue las opciones disponibles.

### **4. Creación/modificación de usuarios y grupos**

* Ve a **System** > **Users and Groups**.
* Para **crear un nuevo usuario**, haz clic en **Create a new user**. Completa los campos requeridos, como nombre de usuario, contraseña y configuración del grupo.
* Para **modificar un usuario existente**, selecciona el usuario y haz clic en **Edit**. Aquí puedes cambiar su contraseña, grupo, permisos, etc.
* Para **crear un nuevo grupo**, selecciona la opción **Create a new group**, define su nombre y asigna los usuarios correspondientes.
* Haz clic en **Save** para aplicar los cambios.

### **5. Inicio/parada de servicios**

* Ve a **System** > **Bootup and Shutdown**.
* Verás una lista de los servicios en ejecución en el sistema.
* Para **iniciar o detener un servicio**, selecciona el servicio y haz clic en el botón correspondiente: **Start** o **Stop**.
* También puedes configurar los servicios para que se inicien automáticamente al arrancar el sistema desde esta sección.

### **6. Comprobación de actualizaciones**

* Ve a **System** > **Software Package Updates**.
* Webmin mostrará una lista de paquetes que tienen actualizaciones disponibles.
* Puedes seleccionar qué actualizaciones instalar o simplemente hacer clic en **Upgrade all** para instalar todas las actualizaciones disponibles.
* Es importante revisar regularmente las actualizaciones de seguridad.

### **7. Apagado/reinicio del servidor**

* Ve a **System** > **Shutdown and Reboot**.
* Desde esta sección, puedes apagar el servidor, reiniciarlo o programar un apagado/reinicio en una hora específica.
* Haz clic en el botón correspondiente para realizar la acción

**Conceptos sobre Cockpit**

#### **1. Protocolo utilizado**

* **HTTP/HTTPS**:  
  Cockpit utiliza conexiones cifradas HTTPS por defecto para garantizar la seguridad en la comunicación entre el cliente (navegador) y el servidor.

#### **2. Puertos necesarios**

Por defecto CockPit usa el puerto 9090 ya que se utiliza para acceder a la interfaz web.

**Instalación de Cockpit**

1. **Instalar Cockpit**

* sudo apt install cockpit -y

1. **Habilitar y arrancar el servicio:**

* sudo systemctl enable --now cockpit.socket

1. **Abrir el puerto 9090 en firewall:**

* sudo ufw allow 9090/tcp

1. **Acceder a la interfaz web:**

En el navegador, abre https://IP\_DEL\_SERVIDOR:9090.

**Verificación de instalación**

Para confirmar que Cockpit está funcionando, ejecuta:

* sudo systemctl status cockpit.socket

**Uso de Cockpit**

**Instalación de algún rol o característica:** sudo apt install paquete

Usa el terminal integrado de Cockpit para instalar paquetes.

**Configuración del nombre del equipo y la red:** Accede a "Red" para configurar adaptadores y DNS.

**Creación/modificación de variables de entorno::** Edita archivos relevantes desde el terminal o el editor de configuración.

**Creación/modificación de usuarios y grupos**:: Usa la sección "Cuentas" para gestionar usuarios.

**Inicio/parada de servicios**:: Desde la sección "Servicios", administra el estado de los mismos.

**Configuración de directivas**:: Configura SELinux o ajustes de seguridad desde la interfaz.

**Comprobación de actualizaciones**:: Usa el módulo "Software Updates" para aplicar actualizaciones.

**Apagado/reinicio del servidor**: Usa el botón "Reiniciar" o "Apagar" en la interfaz principal.