
RA4. Administració remota del sistema operatiu en xarxa

Índex

1. Introducció: per què administrar remotament?	1
2. Mètodes d'accés i administració remota	1
2.1 Terminals en mode text	1
2.2 Escriptori remot	2
2.3 Protocols i ports implicats	2
3. Serveis orientats a sessió vs. no orientats a sessió	2
3.1 Serveis orientats a sessió	3
3.2 Serveis no orientats a sessió	3
4. Eines d'administració remota del propi sistema operatiu	3
4.1 Linux/Unix	3
4.2 Windows Server	4
5. Instal·lació de serveis d'accés i administració remota	4
5.1 SSH a Linux (Debian/Ubuntu)	4
5.2 Escriptori remot gràfic a Linux (XRDP)	5
5.3 RDP a Windows Server	5
5.4 WinRM / PowerShell Remoting a Windows Server	5
6. Comandes i eines gràfiques de gestió	6
6.1 Client SSH (Linux, i també Windows 10/11 nadiu)	6
6.2 PowerShell Remoting	6
6.3 Eines gràfiques	7
7. Comptes d'usuari per a l'accés remot	7
7.1 Linux	7
7.2 Windows	8
8. Proves d'accés entre sistemes heterogenis	8
8.1 Des de Windows cap a Linux	8
8.2 Des de Linux cap a Windows	8
8.3 Taula resum de proves recomanades al laboratori	9
9. Xifratge de la informació transferida	9
9.1 SSH	9
9.2 RDP	10
9.3 WinRM sobre HTTPS	10
9.4 VNC	10
10. Documentació dels processos i serveis administrats	11
10.1 Què s'ha de documentar per a cada servei remot	11
10.2 Exemple de fitxa de documentació (plantilla)	11

Cicle formatiu: Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0374. Administració de sistemes operatius

1. Introducció: per què administrar remotament?

En un entorn professional real, un administrador de sistemes gestiona desenes o centenars de servidors i estacions de treball que, majoritàriament, **no té davant seu físicament**. Poden estar en un CPD a un altre edifici, en un datacenter a un altre país o en el núvol.

L'administració remota permet:

- **Eficiència:** gestionar molts equips sense desplaçament físic.
- **Escalabilitat:** aplicar canvis massius (scripts, GPO, Ansible...) a molts sistemes alhora.
- **Disponibilitat 24/7:** resoldre incidències fora de l'horari laboral sense presencialitat.
- **Centralització:** monitoratge i gestió des d'un únic lloc de treball.

Però també introdueix **riscos de seguretat** importants: si algú intercepta o suplanta una connexió d'administració remota, obté el control del sistema. Per això, tota la resta d'aquest document gira al voltant d'un principi central:

AVÍS

L'administració remota mai s'ha de fer amb protocols que transmetin credencials o dades en text pla. La comoditat no pot anar per davant de la seguretat.

2. Mètodes d'accés i administració remota

Hi ha dues grans famílies de mètodes d'accés remot:

2.1 Terminals en mode text

Ofereixen una línia d'ordres remota, sense interfície gràfica. Són lleugers, ràpids i ideals per a servidors sense entorn gràfic (headless).

Protocol	Port	Xifrat?	Ús recomanat
Telnet	TCP/23	No	Obsolet , només per a proves de connectivitat de ports
rlogin / rsh	TCP/513, 514	No	Obsolet, no s'ha d'utilitzar
SSH	TCP/22	Sí	Estàndard actual en Linux/Unix i també disponible a Windows
WinRM (mode text via PowerShell Remoting)	TCP/5985 (HTTP) / 5986 (HTTPS)	(5986)	Estàndard a Windows

2.2 Escriptori remot

Ofereixen una interfície gràfica completa, com si l'usuari estigués assegut físicament davant l'equip.

Protocol	Port	Xifrat?	Plataforma
RDP (Remote Desktop Protocol)	TCP/3389	Sí (TLS/CredSSP)	Windows (nadiu), Linux via xrdp
VNC (Virtual Network Computing)	TCP/5900+	Depèn de la implementació	Multiplataforma
Spice	TCP/5900 (variable)	Depèn	Virtualització (KVM/Proxmox)

2.3 Protocols i ports implicats

És fonamental que un tècnic sàpiga identificar quins ports ha d'obrir al tallafoc per a cada servei:

SSH	TCP/22
Telnet	TCP/23 (a evitar)
RDP	TCP/3389
VNC	TCP/5900 + N (display 0 = 5900, display 1 = 5901...)
WinRM HTTP	TCP/5985
WinRM HTTPS	TCP/5986

NOTA

Recorda que canviar el port per defecte d'un servei (per exemple, SSH al port 2222) **no és una mesura de seguretat real** (és “seguretat per obscuritat”), sinó només una manera de reduir soroll d'escanejos automàtics. La seguretat real ve de l'autenticació forta i el xifratge.

3. Serveis orientats a sessió vs. no orientats a sessió

Aquest és un concepte clau que sovint es confon:

3.1 Serveis orientats a sessió

Mantenen un **estat persistent** de la connexió mentre dura la interacció: l'usuari s'autentica una vegada i, mentre la sessió estigui oberta, el sistema recorda qui és, quin directori de treball té, quines variables d'entorn s'han definit, etc.

Exemples: SSH, RDP, VNC, Telnet, una sessió de PowerShell Remoting interactiva (Enter-PSSession).

Característiques:

- Consumeixen recursos al servidor mentre estan obertes (procés, memòria).
- Si la connexió de xarxa es talla, la sessió es pot perdre (tot i que eines com tmux, screen o RDP amb reconexió ho pal·lien).
- Adequades per a tasques interactives d'administració.

3.2 Serveis no orientats a sessió

Cada petició és **independent** de les anteriors; el servidor no manté un estat de “qui està connectat” entre peticions.

Exemples: Invoke-Command de PowerShell contra un equip remot sense obrir una sessió persistent, crides SNMP, una petició HTTP puntual a una API REST d'administració (com Redfish/iDRAC/iLO), `ssh servidor "ordre"` executant una única ordre i tancant.

Característiques:

- Més eficients per a automatització massiva (llançar la mateixa ordre a 200 servidors).
- No cal mantenir l'estat al servidor, per la qual cosa escalen millor.
- Ideal per a scripts, cron, sistemes d'orquestració (Ansible, que de fet fa servir SSH però de forma no interactiva/orientada a tasca).

4. Eines d'administració remota del propi sistema operatiu

Tant Linux com Windows Server porten “de fàbrica” (o quasi) eines d'administració remota, sense necessitat d'instal·lar programari de tercers.

4.1 Linux/Unix

- **OpenSSH** (sshd): pràcticament l'estàndard universal. Sol venir preinstal·lat o disponible als dipòsits oficials.
- **systemd**: permet gestionar serveis remotament, combinat amb SSH (`systemctl status nginx` executat via SSH).
- **Cockpit**: consola web d'administració (RHEL/Fedora/Debian), pensada per a gestionar el sistema des del navegador sense necessitat d'instal·lar client SSH.

4.2 Windows Server

- **Escriptori remot (RDP)**: activat des de *Configuració de l'equip* → *Sistema* → *Escriptori remot*, o via PowerShell.
- **Windows PowerShell Remoting (WinRM)**: basat en el protocol WS-Management, permet executar ordres i scripts PowerShell en equips remots.
- **Windows Admin Center**: eina web moderna (successora del gestor de servidors clàssic) per administrar Windows Server des del navegador.
- **MMC en mode remot**: moltes consoles de gestió (*Usuaris i equips d'Active Directory*, *Gestor de DNS*, *Gestor de DHCP*) es poden connectar a un servidor remot directament des de la interfície gràfica.

NOTA

En un domini Active Directory com TH0S.LOCAL, les eines RSAT (*Remote Server Administration Tools*) permeten gestionar els controladors de domini (per exemple SRV-D01) des d'una estació de treball client, sense necessitat d'obrir una sessió RDP al servidor.

5. Instal·lació de serveis d'accés i administració remota

5.1 SSH a Linux (Debian/Ubuntu)

```
sudo apt update
sudo apt install openssh-server -y
sudo systemctl enable --now ssh
sudo systemctl status ssh
```

Comprovació que el servei escolta al port corresponent:

```
sudo ss -tln | grep :22
```

Fitxer de configuració principal: `/etc/ssh/sshd_config`. Alguns paràmetres crítics de seguretat:

```
Port 22
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
X11Forwarding no
MaxAuthTries 3
```

Després de qualsevol canvi:

```
sudo sshd -t                # verifica sintaxi abans de reiniciar
sudo systemctl restart ssh
```

5.2 Escriptori remot gràfic a Linux (XRDP)

```
sudo apt install xrdp -y
sudo systemctl enable --now xrdp
sudo adduser xrdp ssl-cert
sudo systemctl restart xrdp
```

Obertura del tallafoc (UFW):

```
sudo ufw allow 3389/tcp
```

5.3 RDP a Windows Server

Per PowerShell (útil quan no tenim accés gràfic previ, per exemple en un Server Core):

```
# Activa l'escriptori remot
Set-ItemProperty -Path
  ↳ 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name
  ↳ "fDenyTSConnections" -Value 0

# Habilita l'autenticació a nivell de xarxa (NLA) - recomanat
Set-ItemProperty -Path
  ↳ 'HKLM:\System\CurrentControlSet\Control\Terminal
  ↳ Server\WinStations\RDP-Tcp' -Name "UserAuthentication" -Value 1

# Obre el tallafoc
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

5.4 WinRM / PowerShell Remoting a Windows Server

```
# Configuració ràpida (entorn de domini/prova)
Enable-PSRemoting -Force

# Comprovar l'estat del servei
Get-Service WinRM

# Llistar els listeners actius
winrm enumerate winrm/config/listener
```

Per a un entorn de producció, cal configurar el listener amb HTTPS i un certificat vàlid en lloc del HTTP per defecte (vegeu apartat 9).

AVÍS

Enable-PSRemoting -Force configura per defecte un *listener* HTTP (port 5985) sense xifratge de transport addicional (encara que l'autenticació Kerberos/NTLM xifra les credencials, el contingut de la sessió no va xifrat amb TLS). En producció, configura

sempre un listener HTTPS.

6. Comandes i eines gràfiques de gestió

6.1 Client SSH (Linux, i també Windows 10/11 nadiu)

```
# Connexió bàsica
ssh usuari@srv-web01.thos.local

# Connexió amb clau privada específica i port no estàndard
ssh -i ~/.ssh/id_ed25519 -p 2222 usuari@10.0.10.15

# Executar una única ordre remota (no orientat a sessió)
ssh usuari@srv-web01 "df -h && uptime"

# Copiar fitxers (SCP)
scp informe.pdf usuari@srv-fs01.thos.local:/home/usuari/

# Transferència interactiva (SFTP)
sftp usuari@srv-fs01.thos.local
```

Generació de claus per a autenticació sense contrasenya:

```
ssh-keygen -t ed25519 -C "ramon@thos.local"
ssh-copy-id usuari@srv-web01.thos.local
```

6.2 PowerShell Remoting

```
# Sessió interactiva (orientat a sessió)
Enter-PSSession -ComputerName SRV-DC01

# Execució d'una ordre puntual en múltiples equips (no orientat a
↪ sessió)
Invoke-Command -ComputerName SRV-DC01, SRV-FS01 -ScriptBlock {
↪ Get-Service | Where-Object Status -eq 'Running' }

# Sessió persistent reutilitzable (millor rendiment en múltiples
↪ ordres)
$session = New-PSSession -ComputerName SRV-DC01
Invoke-Command -Session $session -ScriptBlock { Get-Process }
Remove-PSSession $session
```

6.3 Eines gràfiques

Eina	Plataforma origen	Plataforma destí	Ús
Connexió a Escriptori remot (mstsc)	Windows	Windows	RDP nadiu
Remmina	Linux	Windows/Linux/VNC	Client multiprotocol (RDP, VNC, SSH)
PuTTY	Windows	Linux/Unix	Client SSH clàssic
Windows Admin Center	Navegador	Windows Server	Gestió web centralitzada
Cockpit	Navegador	Linux	Gestió web (serveis, xarxa, logs, actualitzacions)
RSAT	Windows	Active Directory / DNS / DHCP	Consoles MMC remotes

7. Comptes d'usuari per a l'accés remot

Un principi essencial de seguretat: **mai s'ha d'administrar remotament amb el compte root o Administrator directament**. Cal crear comptes nominals amb privilegis elevats controlats.

7.1 Linux

```
# Crear l'usuari
sudo adduser jsanchez

# Afegir-lo al grup amb permisos d'escalada (sudo a Debian/Ubuntu)
sudo usermod -aG sudo jsanchez

# Restringir l'accés SSH només a un grup concret
sudo groupadd sshusers
sudo usermod -aG sshusers jsanchez
```

A /etc/ssh/sshd_config:

```
AllowGroups sshusers
```

7.2 Windows

```
# Crear l'usuari
New-LocalUser -Name "jsanchez" -Description "Tècnic de suport remot"
↪ -NoPassword:$false

# Afegir-lo al grup local d'usuaris d'escriptori remot
Add-LocalGroupMember -Group "Remote Desktop Users" -Member "jsanchez"

# En entorn de domini (THOS.LOCAL), es faria amb els cmdlets d'AD:
New-ADUser -Name "Joan Sanchez" -SamAccountName "jsanchez" -Enabled
↪ $true
Add-ADGroupMember -Identity "Remote Desktop Users" -Members "jsanchez"
```

NOTA

Per a l'accés a **WinRM/PowerShell Remoting**, l'usuari ha de pertànyer al grup local Remote Management Users (o ser administrador), a més de tenir permisos concedits explícitament si es restringeix per Set-PSSessionConfiguration.

8. Proves d'accés entre sistemes heterogenis

Un dels reptes reals en entorns empresarials mixtos és connectar sistemes Windows i Linux entre si.

8.1 Des de Windows cap a Linux

Client SSH nadiu (Windows 10/11 i Windows Server, des de PowerShell):

```
ssh jsanchez@srv-web01.thos.local
scp .\informe.pdf jsanchez@srv-fs01.thos.local:/home/jsanchez/
```

Amb PuTTY (interfície gràfica): cal indicar l'adreça IP/nom, el port 22 i el tipus de connexió SSH.

8.2 Des de Linux cap a Windows

RDP des de Linux amb xfreerdp (línia d'ordres) o Remmina (gràfic):

```
sudo apt install freerdp2-x11 -y
xfreerdp /u:jsanchez /p:'ContrasenyaSegura!' /v:srv-dc01.thos.local
↪ /cert:ignore
```

PowerShell Remoting des de Linux (PowerShell 7 és multiplataforma):

```
sudo apt install -y powershell
pwsh
```

```
# Dins de pwsh, connectant a un Windows amb WinRM configurat sobre
↪ HTTPS
$cred = Get-Credential
New-PSSession -ComputerName srv-dc01.thos.local -UseSSL -Credential
↪ $cred
```

8.3 Taula resum de proves recomanades al laboratori

Origen	Destí	Protocol	Eina
Linux	Linux	SSH	ssh, scp
Windows	Linux	SSH	client SSH nadiu de Windows, PuTTY
Linux	Windows	RDP	xfreerdp, Remmina
Linux	Windows	WinRM	PowerShell 7 (pwsh)
Windows	Windows	RDP	mstsc
Windows	Windows	WinRM	Enter-PSSession, Invoke-Command

9. Xifratge de la informació transferida

Totes les credencials i dades que circulen per la xarxa durant una sessió d'administració remota han d'anar **xifrades**, per evitar atacs de tipus *sniffing* o *man-in-the-middle*.

9.1 SSH

El xifratge és nadiu al protocol. Bones pràctiques:

```
# /etc/ssh/sshd_config
Protocol 2
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com
KexAlgorithms curve25519-sha256
HostKeyAlgorithms ssh-ed25519,rsa-sha2-512
```

9.2 RDP

Cal forçar el nivell de xifratge i exigir NLA (Network Level Authentication), que autentica l'usuari **abans** d'establir la sessió completa d'escriptori, reduint la superfície d'atac:

```
Set-ItemProperty -Path
↳ 'HKLM:\System\CurrentControlSet\Control\Terminal
↳ Server\WinStations\RDP-Tcp' -Name "MinEncryptionLevel" -Value 3
↳ # Alt
```

9.3 WinRM sobre HTTPS

Cal un certificat (idealment emès per la CA interna del domini, com la que es pot desplegar amb AD CS a THOS.LOCAL):

```
# Crear el listener HTTPS amb un certificat ja instal·lat (Thumbprint)
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object
↳ {$_ .Subject -eq "CN=srv-dc01.thos.local"}
New-Item -Path WSMan:\localhost\Listener -Transport HTTPS -Address *
↳ -CertificateThumbPrint $cert.Thumbprint -Force

# Obrir el port corresponent al tallafo
New-NetFirewallRule -DisplayName "WinRM-HTTPS" -Direction Inbound
↳ -Protocol TCP -LocalPort 5986 -Action Allow
```

9.4 VNC

VNC "clàssic" (RFB) **no xifra per defecte**. Cal: - Fer servir una implementació que ho suporti nativament (TigerVNC amb TLS), o - Encapsular la connexió dins d'un túnel SSH:

```
ssh -L 5901:localhost:5901 usuari@servidor-remot
# I després connectar el client VNC a localhost:5901
```

AVÍS

Un error molt habitual és exposar un servidor VNC directament a Internet sense xifratge ni túnel. Aquesta configuració ha causat incidents de seguretat reals en entorns de producció. **Mai** VNC sense xifratge cap a l'exterior.

10. Documentació dels processos i serveis administrats

Documentar no és opcional: en un entorn professional, si el tècnic que ha configurat un servei no hi és disponible, un altre membre de l'equip ha de poder-lo mantenir.

10.1 Què s'ha de documentar per a cada servei remot

- **Nom i propòsit del servei** (què fa i per què existeix).
- **Equip(s) on s'executa** (nom, IP, rol dins la infraestructura).
- **Port(s) i protocol(s) utilitzats**.
- **Mètode d'autenticació** (claus públiques, Kerberos, certificats...).
- **Usuaris/grups amb accés** i el nivell de privilegi de cadascun.
- **Data de la darrera revisió/canvi de configuració**.
- **Procediment de recuperació** en cas de fallada.

10.2 Exemple de fitxa de documentació (plantilla)

```
## Servei: SSH --- SRV-WEB01

- **Equip**: srv-web01.thos.local (10.0.10.15)
- **Protocol/Port**: SSH / TCP 22
- **Autenticació**: clau pública (contrasenya deshabilitada)
- **Usuaris amb accés**: jsanchez (grup sshusers), rlopez (grup
  ↳ sshusers)
- **Root login**: deshabilitat (PermitRootLogin no)
- **Última revisió**: 2026-09-10, per R. López
- **Observacions**: fail2ban actiu amb bloqueig després de 3 intents
  ↳ fallits
```

Versions d'aquest document

- [HTML](#)
- [PDF](#)
- [ODT](#)
- [MD](#)

[Domini Públic \(CC0\)](#)