

LPIC2 2021 Sesión 14 (2021-03-18)

Documentación relacionada:

- Manual Certificacion LPIC-2.pdf, pag XX
- Material Practicas LPIC-2/LPIC-202/
- Presentaciones/2020/202/
- gdrive://

Clase

E-Mail Services

- DOC: pag 383
- smart host relay: delegar a otro SMTP el envío real

sendmail

- DOC: Material Practicas LPIC-2/LPIC-202/4-E-Mail Services/Laboratorio Servidor de correo-Centos7.pdf
- yum install -y sendmail sendmail-cf
- **/etc/mail**
 - sendmail.mc: fichero de macros
 - **dnl**: comentarios
 - descomentando **define(`SMART_HOST', `smtp.your.provider')** definimos a quien vamos a delegar el envío real del mensaje. Sin autenticación (no apto para Gmails y similares)
 - sendmail.cf: fichero compilado del .mc
 - make -C /etc/mail
- **/etc/aliases**
 - listas de correo «locales»
 - informatica: <user-local>, <user@dominio>
 - newaliases para aplicar los cambios
- netstat -putan | grep -i listen
- relay a través de GMAIL: <https://www.lotor.altervista.org/wiki/en/how-to/sendmail-and-gmail-relay>
 - activar aplicaciones poco seguras en gmail para poder enviar
- **/var/log/maillog**
- mailq: mensajes encolados
 - **/var/spool/mqueue**
- **~/.forward**: dirección de reenvío de los mensajes
- mail
- TIPs: mailman para gestión de listas de correo
- rspamd: aka spam assassin

Laboratorio

- sendmail
 - </etc/mail/sendmail.mc>

- make -C /etc/mail
- systemctl restart sendmail
- dovecot
 - yum install -y dovecot
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - yum install -y mailx: cliente mail
- mkdir /etc/skel/Maildir: estructura que se crea al crear un nuevo usuario
- **/etc/rsyslog.conf**
 - el guión delante de la sección **mail.*** hace que la escritura a disco sea asíncrona (memoria→disco)

TIP: logs remotos

- Provider(s). descomentar **UDP**
- systemctl restart rsyslog
- en la máquina que ha de enviar los logs:
 - @**192.168.2.5** en las rules que queramos. Arroba por ser UDP. Si es TCP son 2 arrobas
- logger
- herramientas:
 - grafana, elastic
 - <https://www.overops.com/blog/las-7-herramientas-para-el-manejo-de-logs-registros-que-todo-desarrollador-java-debe-conocer/> → graylog
 - logAnalyzer (php) → <https://loganalyzer.adiscon.com/>
- para recursos:
 - <https://checkmk.com/>
- zabbix
 - <https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-zabbix-to-securely-monitor-remote-servers-on-ubuntu-20-04-es>
 - <https://techexpert.tips/es/zabbix-es/zabbix-monitor-windows-utilizando-agent/>
- DOC: Laboratorio configuración del sistema de registros de Red Hat 7.pdf

SSH

- DOC: Material Practicas LPIC-2/LPIC-202/5-Configuracion de OpenSSH/
 - Configurar SSHd.txt
 - Configuración de OpenSSH.pdf
 - **/etc/ssh/sshd_config**
 - **Port**
 - **ListenAddress**
 - **PermitRootLogin = no**
 - **X11Forwarding**: reenvio X-Windows
 - **AllowUsers, AllowGroups, DenyUsers, DenyGroups**: al final del fichero
 - filtrado usuario o usuario@ip
 - **UseDNS = no**: no resolver la IP
 - clientes
 - ssh user@direccion
 - ssh -p <puerto> user@direccion
 - sftp -o Port=xxxx user@direccion

- `scp -P xxxxx user@direccion...`
- DOC: Túneles SSH.pdf
- DOC: Presentacion SSH.pdf, pag. 10-15 (opciones del fichero sshd_config)
- opciones generales:

| Opción | Descripción | Valor por defecto |
|------------------------|--|-------------------------------|
| AcceptEnv* | Indica las variables de ambiente enviadas por el cliente que serán aceptadas por el servidor. | Ninguna variable es aceptada. |
| AddressFamily | Especifica la familia de direcciones IP aceptadas por el servidor, los valores pueden ser <i>any</i> , <i>inet</i> ó <i>inet6</i> . | <i>any</i> |
| AllowTcpForwarding | Autoriza el reenvío de puertos. | Yes |
| GatewayPorts | Especifica si ordenadores remotos están autorizados a utilizar puertos reenviados a otros clientes. Los valores posibles son <i>no</i> , <i>yes</i> y <i>clientspecified</i> . | No |
| ListenAddress | Dirección IP local que escucha las conexiones entrantes. Pueden especificarse varias entradas para indicar varias direcciones de red. | Todas las direcciones. |
| Port | Puerto en que permanece a la escucha el servidor en espera de conexiones. Pueden especificarse varias entradas para especificar varios puertos distintos. | 22 TCP. |
| Protocol | Versión de los protocolos SSH soportados por el servidor y orden de preferencia. | Versión 2. |
| TCPKeepAlive | Indica si deben enviarse paquetes para comprobar si la conexión con el cliente se encuentra activa. | Yes |
| UseDNS | Indica si se debe realizar una comprobación inversa de la identidad del cliente. | Yes |
| UsePrivilegeSeparation | Indica si SSH creará un proceso hijo sin privilegios una vez el usuario ha accedido al sistema. | Yes |

- opciones de configuración de acceso:

| Opción | Descripción | Valor por defecto |
|---------------------------------|---|---------------------------------------|
| AuthorizedKeysFile | Fichero con las claves públicas usadas para autenticación. | <code>~/.ssh/authorized_keys</code> . |
| ChallengeResponseAuthentication | Indica si el intercambio de respuestas de autenticación es permitido. | Yes |
| Ciphers* | Indica los cifrados permitidos por el protocolo. | Todos. |
| GSSAPIAuthentication* | Especifica si la autenticación basada en GSSAPI es permitida. | No |
| GSSAPICleanupCredentials* | Especifica si las credenciales son automáticamente destruidas cuando termina la sesión. | Yes |
| HostbasedAuthentication* | Autoriza el acceso mediante clave pública de usuarios de los ordenadores indicados en <i>rhosts</i> o en <i>/etc/hosts.equiv</i> . | No |
| HostKey | Especifica el fichero que contiene la clave privada del servidor. Sus valores por defecto son <i>/etc/ssh/ssh_host_key</i> para la versión 1 y <i>/etc/ssh/ssh_host_rsa_key</i> y <i>/etc/ssh/ssh_host_dsa_key</i> para la versión 2. | Ver descripción. |
| IgnoreRhosts | Deniega el uso de los ficheros <i>.rhosts</i> y <i>.shosts</i> en el acceso remoto. | Yes |
| IgnoreUserKnownHosts | Deniega el uso del fichero <i>~/.ssh/known_hosts</i> para encontrar los ordenadores conocidos. | No |
| LoginGraceTime | Tiempo, en segundos, antes de que se cierre la sesión de autenticación. | 120 segundos. |
| LogLevel | Información que se escribirá en los accesos. Sus valores posibles son, de menor a mayor información QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2 y DEBUG3. | INFO |

| Opción | Descripción | Valor por defecto |
|-------------------------|--|-------------------|
| MaxAuthTries | Número máximo de intentos de autenticación por conexión. | 6 |
| MaxStartups | Número máximo de conexiones simultáneas en estado de autenticación. | 10 |
| PasswordAuthentication | Permite la autenticación mediante contraseña. | Yes |
| PermitEmptyPasswords | Permite el acceso a usuarios sin contraseña. | No |
| PermitRootLogin | Permite el acceso de root mediante SSH. | Yes |
| PermitUserEnvironment | Especifica si las variables de ambiente del usuario serán procesadas por SSH. | No |
| PubkeyAuthentication* | Permite la autenticación mediante clave pública. | Yes |
| RhostsRSAAuthentication | Indica si se permite el uso de <i>rhost</i> o <i>/etc/hosts.equiv</i> en la autenticación mediante RSA. Solo aplicable a la versión 1 del protocolo. | No |
| RSAAuthentication | Permite la autenticación mediante RSA. Solo aplicable a la versión 1 del protocolo. | Yes |
| UseLogin | Indica si se utiliza login para comprobar el acceso de los usuarios. | No |
| UsePAM | Indica si se utiliza PAM para comprobar el acceso de los usuarios. | No |

- opciones de usuarios y grupos:

| Opción | Descripción | Valor por defecto |
|-------------|---|---------------------|
| AllowGroups | Lista de nombres de grupos, separados por espacios, cuyos miembros, sea como grupo primario o grupo suplementario, tienen permitido el acceso al sistema mediante SSH. Pueden utilizarse los caracteres comodín * e ?. | Todos los grupos. |
| AllowUsers | Lista de nombres de usuarios, separados por espacios, cuyo acceso al sistema esta permitido por SSH. Puede tomar la forma usuario@ordenador, comprobando entonces tanto el nombre del usuario como el nombre del ordenador desde el que intenta el acceso. Pueden utilizarse los caracteres comodín * e ?. | Todos los usuarios. |
| DenyGroups | Lista de nombres de grupos, separados por espacios, cuyos miembros, sea como grupo primario o grupo suplementario, no tienen permitido el acceso al sistema mediante SSH. Pueden utilizarse los caracteres comodín * e ?. | Ningún grupo. |
| DenyUsers | Lista de nombres de usuarios, separados por espacios, cuyo acceso al sistema no esta permitido por SSH. Puede tomar la forma usuario@ordenador, comprobando entonces tanto el nombre del usuario como el nombre del ordenador desde el que intenta el acceso. Pueden utilizarse los caracteres comodín * e ?. | Ningún usuario. |

- opciones de reenvío de conexiones X11:

| Opción | Descripción | Valor por defecto |
|------------------|--|-------------------|
| X11DisplayOffset | Indica el primer identificador de pantalla que utilizará SSH en sus conexiones X11 para no interferir con los identificadores locales X11. | 10 |
| X11Forwarding | Permite el reenvío de conexiones X11. | No |
| X11UseLocalhost | Indica si SSH escucha las conexiones X11 en el interfaz de loopback o en los otros interfaz de red existentes. | Yes |
| XAuthLocation | Indica la localización del programa de autorización de acceso mediante X11. | /usr/bin/xauth |

- otras opciones:

| Opción | Descripción | Valor por defecto |
|----------------------|---|------------------------|
| Banner* | Muestra un mensaje antes de acceder al servidor de SSH. | Sin ningún mensaje. |
| ClientAliveCountMax* | Número de paquetes de comprobación sin responder que se espera antes de cerrar la conexión por no obtener respuesta del cliente. | 3 |
| ClientAliveInterval* | Intervalo de inactividad, en segundos, que el servidor espera antes de enviar un mensaje al cliente solicitando una respuesta. | No activado (valor 0). |
| Compression | Especifica si la compresión es permitida o retrasada hasta que el usuario se ha autenticado correctamente. Sus valores son yes, no o delayed. | Delayed. |
| ForceCommand | Fuerza la ejecución del comando especificado. | Ninguno. |
| PrintLastLog | Especifica si al acceder mediante SSH se mostrará la información del último acceso sucedido. | Yes |
| PrintMotd | Especifica si SSH mostrará el mensaje del día indicado en <i>/etc/motd</i> . | Yes |
| StrictModes | Especifica si SSH debe chequear el modo y propietario de los ficheros en el directorio raíz del usuario antes de permitir su acceso. | Yes |
| Subsystem* | Configura un subsistema externo, por ejemplo el <i>sftp-server</i> . | Ninguno. |

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea



Permanent link:

<https://miguelangel.torresegea.es/wiki/info:cursos:pue:lpic2-2021:s14>

Last update: **23/03/2021 10:30**