Linux

Guida: Generare e Copiare una Chiave SSH su un Server Remoto

Questa guida illustra la generazione di una chiave pubblica SSH e due metodi per installarla su un server Linux.

Generazione della Chiave SSH

Generare una nuova coppia di chiavi SSH utilizzando l'algoritmo Ed25519:

```
ssh-keygen -t ed25519 -C "tuo_indirizzo_email@example.com"
```

Nota: Premere Invio per accettare il percorso predefinito. È possibile inserire una passphrase per maggiore sicurezza oppure lasciare vuoto e premere Invio per non utilizzarla.

Metodo 1: Utilizzo di ssh-copy-id (Automatico)

Questo metodo richiede che l'autenticazione con password sia abilitata sul server remoto.

Comando standard:

```
ssh-copy-id utente@indirizzo_server
```

Comando con porta SSH personalizzata (es. 2222):

```
ssh-copy-id -p 2222 utente@indirizzo_server
```

Comando con file chiave specifico:

```
ssh-copy-id -i ~/.ssh/id_ed25519.pub utente@indirizzo_server
```

Nota: Alla richiesta, inserire la password dell'utente remoto. I caratteri non verranno visualizzati.

Metodo 2: Inserimento Manuale (Copia e Incolla)

Utilizzare questo metodo se ssh-copy-id fallisce o se l'autenticazione con password è disabilitata.

1. Macchina Locale

Visualizzare il contenuto della chiave pubblica e copiarlo negli appunti:

```
cat ~/.ssh/id_ed25519.pub
```

2. Server Remoto

Accedere al server remoto.

Creare la directory SSH e impostare i permessi:

```
mkdir -p ~/.ssh
chmod 700 ~/.ssh
```

Aprire il file delle chiavi autorizzate:

```
nano ~/.ssh/authorized_keys
```

Incollare il contenuto della chiave copiato in precedenza. Salvare e uscire (In nano: CTRL+O, Invio, CTRL+X).

Impostare i permessi di sicurezza sul file:

```
chmod 600 ~/.ssh/authorized_keys
```

Log

Gestione dei log con systemd-journald

1. Introduzione

`systemd-journald` è il servizio responsabile della raccolta e gestione dei log di sistema nei sistemi Linux basati su `systemd`.

Con il tempo, i log possono occupare molto spazio su disco, specialmente su server o VPS che rimangono attivi a lungo. Questa guida mostra come:

- verificare lo spazio occupato dai log;
- ruotare i log correnti;
- eliminare i log vecchi;
- configurare limiti permanenti.

---

2. Verificare lo spazio occupato dai log

Per vedere quanto spazio stanno occupando i log di `journald`:

```
journalctl --disk-usage
```

Esempio di output

```
Archived and active journals take up 1.8G in the file system.
```

---

3. Ruotare i log

Prima di eliminare i log vecchi è consigliato forzare la rotazione dei file correnti.

```
sudo journalctl --rotate
```

Questo comando crea nuovi file journal e archivia quelli attualmente in uso.

---

4. Pulire i log

4.1 Eliminare i log in base alla dimensione

Mantieni ad esempio solo 200 MB di log:

```
sudo journalctl --vacuum-size=200M
```

Puoi usare anche:

- `50M`
- `1G`
- `2G`

4.2 Eliminare i log più vecchi di un certo periodo

Mantieni solo gli ultimi 7 giorni:

```
sudo journalctl --vacuum-time=7d
```

Altri esempi:

```
sudo journalctl --vacuum-time=12h
sudo journalctl --vacuum-time=30d
sudo journalctl --vacuum-time=1month
```

4.3 Limitare il numero di file journal

Mantieni solo 5 file journal archiviati:

```
sudo journalctl --vacuum-files=5
```

5. Pulizia rapida con un comando

Ruota i log e mantieni solo 100 MB:

```
sudo journalctl --rotate && sudo journalctl --vacuum-size=100M
```

Oppure conserva solo gli ultimi 3 giorni:

```
sudo journalctl --rotate && sudo journalctl --vacuum-time=3d
```

6. Configurazione permanente

Per impostare limiti automatici modifica il file:

```
sudo nano /etc/systemd/journald.conf
```

Esempio di configurazione:

```
[Journal]
SystemMaxUse=500M
SystemKeepFree=100M
SystemMaxFileSize=50M
SystemMaxFiles=10
MaxRetentionSec=2week
```

Significato dei parametri

Parametro	Descrizione
`SystemMaxUse`	Spazio massimo totale usato dai log
`SystemKeepFree`	Spazio libero minimo da lasciare sul disco
`SystemMaxFileSize`	Dimensione massima di ogni file journal
`SystemMaxFiles`	Numero massimo di file journal
`MaxRetentionSec`	Tempo massimo di conservazione

Dopo la modifica riavvia il servizio:

```
sudo systemctl restart systemd-journald
```

---

7. Note importanti

- I comandi di pulizia eliminano definitivamente i log vecchi.
- È consigliato mantenere almeno alcuni giorni di log per troubleshooting e audit.
- La rotazione (`--rotate`) non elimina nulla: prepara solo i file correnti all'archiviazione.
- Alcune distribuzioni usano storage volatile (`/run/log/journal`) invece di storage persistente (`/var/log/journal`).

Per verificare dove vengono salvati i log:

```
ls -ld /var/log/journal
ls -ld /run/log/journal
```

Suggerimento: su server piccoli o VPS con poco spazio disco, una combinazione comune è:

```
SystemMaxUse=200M
MaxRetentionSec=7day
```

Installazione e implementazione sudo

Su un'installazione minimale Debian

Diventa root:

```
su -
```

(metti la password di root impostata in fase di installazione)

> Installa sudo se manca e aggiungi il tuo utente al gruppo:

```
apt update && apt install sudo
usermod -aG sudo iltuoutente
exit
```

> Poi esci e rientra con quell'utente (il gruppo si applica solo a nuovo login), oppure al volo:

```
newgrp sudo
```

Verifica che funzioni:

```
sudo whoami
```

Se ti risponde root, sei a posto.