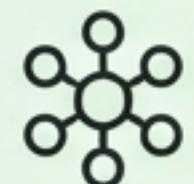




# SSH: La Clave de tu Clúster Hadoop

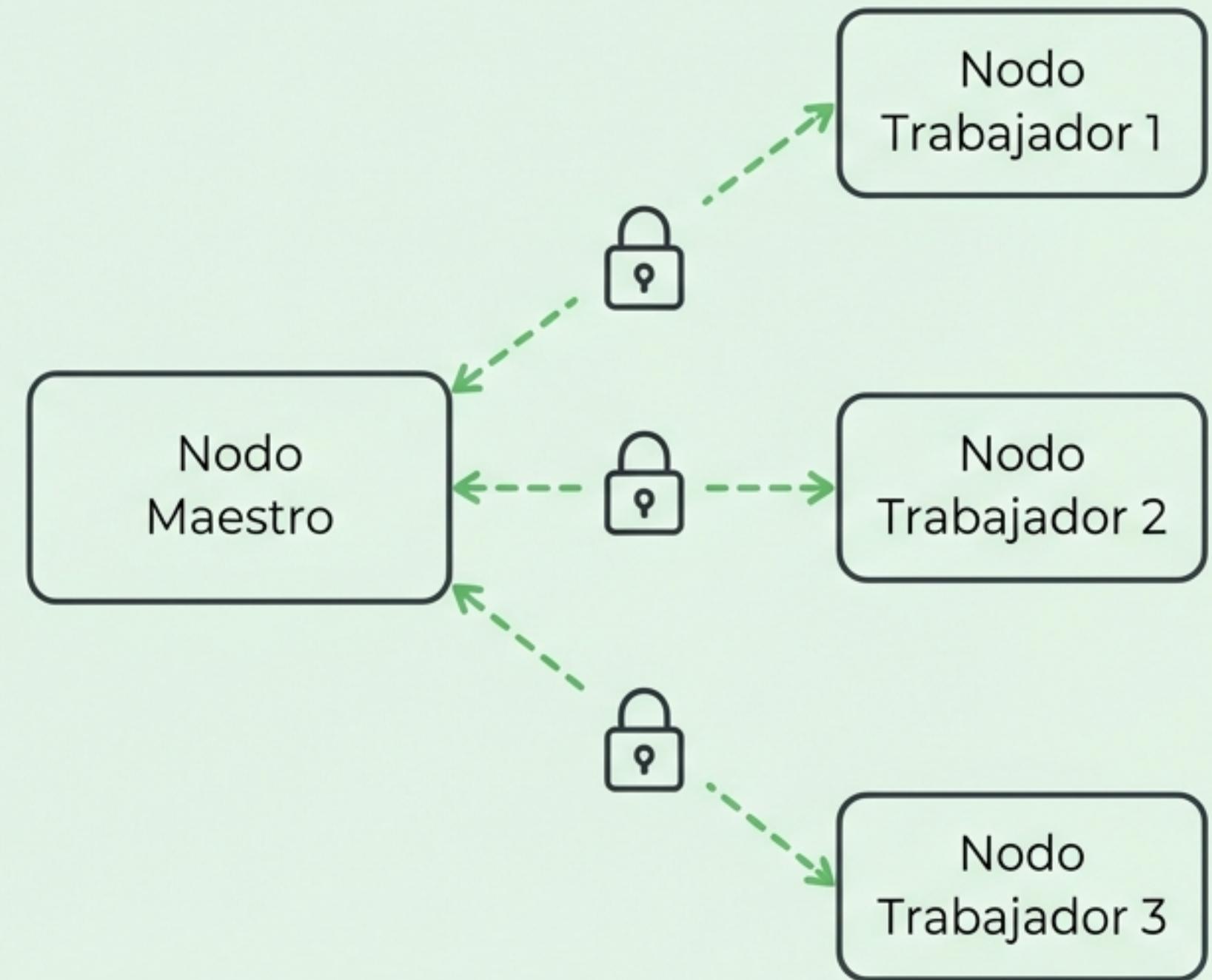


Una guía práctica para configurar el acceso sin contraseña,  
desde el principio teórico hasta el comando final.



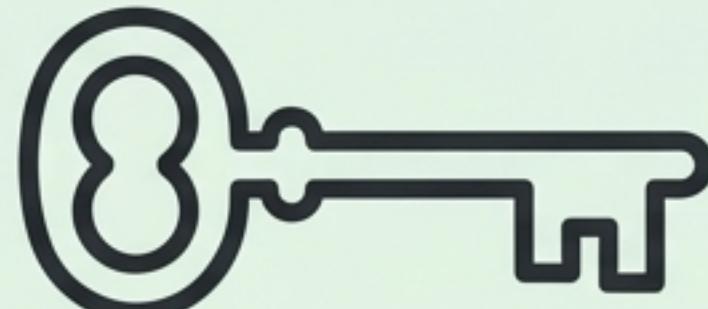
# El Requisito Fundamental: ¿Por Qué Hadoop Necesita SSH?

- Hadoop es un sistema distribuido. Sus componentes, repartidos en diferentes nodos, necesitan comunicarse constantemente para coordinar tareas.
- Esta comunicación debe ser segura y, fundamentalmente, **automatizada**. No puede depender de que un administrador introduzca una contraseña para cada operación.
- La solución estándar es el acceso SSH mediante autenticación por clave, que permite a los nodos del clúster conectarse entre sí de forma segura y sin intervención manual.



# El Principio #1: La Magia de la Criptografía Asimétrica

En el corazón de la autenticación SSH se encuentra un par de claves digitales:



## Clave Privada (`id\_rsa`)

Es tu secreto. Se guarda en el equipo desde el que te conectas y nunca debe compartirse. Es la única “llave” que puede abrir la cerradura.



## Clave Pública (`id\_rsa.pub`)

Es tu identidad compartida. Puedes distribuirla libremente. Actúa como una “cerradura” que instalas en los servidores a los que quieres acceder.

# La Práctica: Generando Tu Identidad con `ssh-keygen`

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/hadoop/.ssh/id_rsa): [ENTER]
Created directory '/home/hadoop/.ssh'.
Enter passphrase (empty for no passphrase): [ENTER]
Enter same passphrase again: [ENTER]

Your identification has been saved in /home/hadoop/.ssh/id_rsa.
Your public key has been saved in /home/hadoop/.ssh/id_rsa.pub.
```

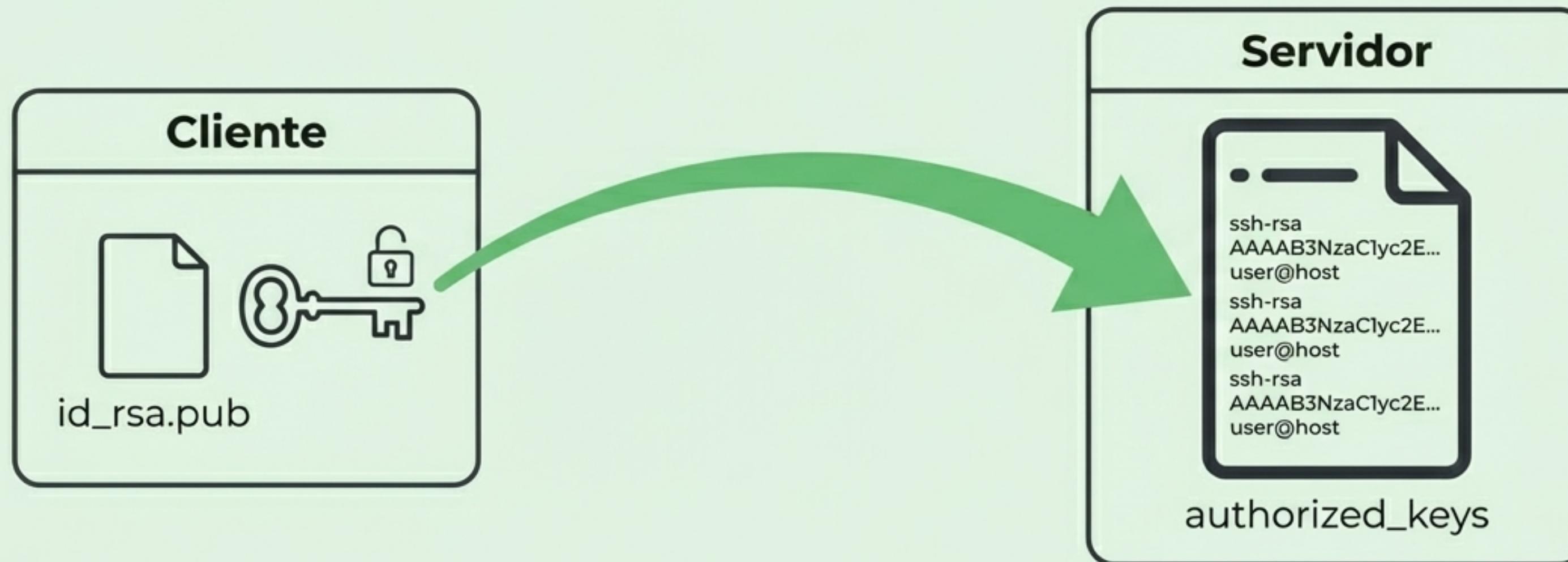


Se crea el directorio .ssh para alojar tus claves.

Se generan los dos ficheros cruciales: la clave privada (id\_rsa) y la pública (id\_rsa.pub).

## El Principio #2: Otorgando Confianza al Servidor

Para que un servidor te permita el acceso sin contraseña, debes informarle de que confíe en tu clave pública. Esto se hace añadiendo el contenido de tu clave pública (``id_rsa.pub``) a un fichero especial en el servidor llamado ``~/.ssh/authorized_keys`` . Cada clave pública en este fichero representa una identidad autorizada para acceder.



# La Práctica: Instalando la Clave en `authorized\_keys`

En una configuración de Hadoop, incluso en un solo nodo, el sistema necesita poder conectarse por SSH a sí mismo ('localhost' o 'nodo1'). Por tanto, nuestro primer paso es autorizar nuestra propia clave pública en nuestro propio sistema.

```
• • •  
# Navegamos al directorio de configuración de SSH  
$ cd .ssh  
  
# Copiamos la clave pública para crear el fichero de autorización  
$ cp id_rsa.pub authorized_keys
```

# El Principio #3: La Seguridad Reside en los Permisos



La seguridad de todo el sistema se anula si tu clave privada (`id\_rsa`) es accesible para otros usuarios en el mismo sistema. El protocolo SSH es estricto: se negará a funcionar si detecta que los permisos de tu clave privada o de tu directorio `ssh` son demasiado abiertos.

La regla de oro es: **solo el propietario debe poder leer la clave privada.**

# La Práctica: Inspeccionando Permisos con `ls -l`

```
...  
$ ls -l .ssh  
total 16  
-rw-----. 1 hadoop hadoop 1675 dic 26 18:45 id_rsa  
-rw-r--r--. 1 hadoop hadoop 394 dic 26 18:45 id_rsa.pub
```

**Correcto.** Solo el propietario (`hadoop`) tiene permisos de lectura (`r`) y escritura (`w`). El acceso para el grupo y otros está denegado (`---`).

**Seguro.** La clave pública está diseñada para ser compartida, por lo que permisos más abiertos son aceptables y normales.

# El Momento de la Verdad: Conexión Exitosa

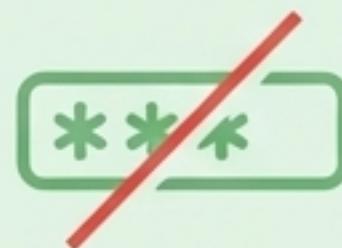
Con las claves generadas, la autorización configurada y los permisos verificados, probamos la conexión. La primera vez, el sistema te pedirá que confirmes la autenticidad del host. Tras aceptarla, el acceso será instantáneo.

```
● ● ●  
$ ssh nodo1  
The authenticity of host 'nodo1(::1)' can't be established.  
ECDSA key fingerprint is 3d:94:76:5e:20:c4:b7:c1:98:91:bb:db:fb:e2:01:ea.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added nodo1 (ECDSA) to the list of known hosts.  
  
Last login: Sun Apr 19 10:33:40 2015  
[hadoop@nodo1 ~]$ █
```



# Próximos Pasos: Fortaleciendo la Seguridad del Servidor

La configuración del cliente es solo la mitad de la historia. Para un entorno de producción, es fundamental 'endurecer' la configuración del servidor SSH (`/etc/ssh/sshd\_config`).



## 1. Deshabilitar Autenticación por Contraseña

Forzar el uso exclusivo de claves editando la línea `PasswordAuthentication no`.



## 2. Cambiar el Puerto por Defecto

Reducir la exposición a bots cambiando `Port 22` a un número de puerto alto y no estándar.



## 3. Limitar el Acceso de Root

Mejorar la seguridad deshabilitando el login directo del superusuario con `PermitRootLogin no`.

# Resumen del Proceso: De la Teoría al Terminal

## Paso 1: GENERAR

Creas tu identidad digital única (clave privada y pública).

```
...  
$ ssh-keygen
```

## Paso 2: AUTORIZAR

Le dices al servidor que confíe en tu identidad copiando tu clave pública.

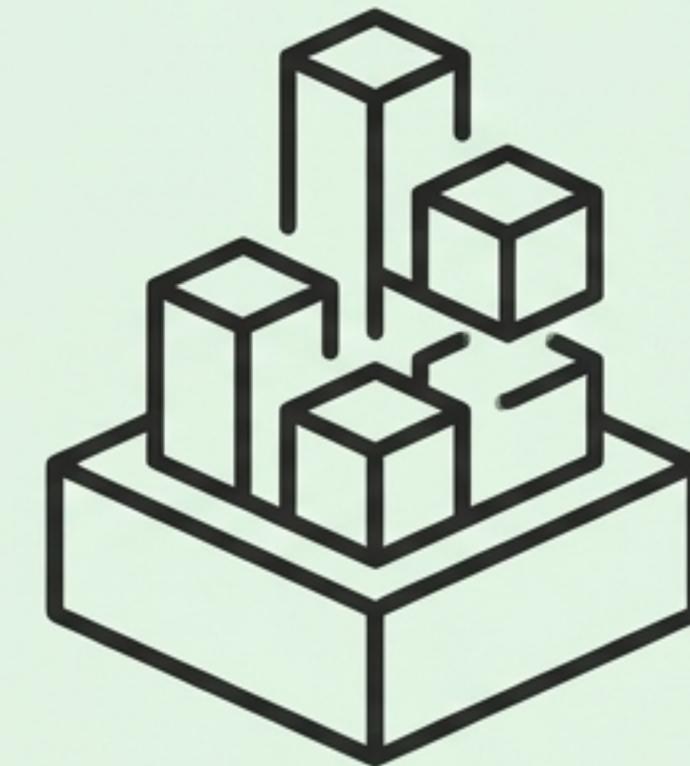
```
...  
$ cp id_rsa.pub authorized_keys
```

## Paso 3: CONECTAR

Accedes al sistema de forma segura, verificando que la configuración funciona.

```
...  
$ ssh nodo1
```

# El Dominio de los Fundamentos



Configurar SSH correctamente no es solo un paso técnico en una larga lista de tareas. Es la base sobre la que se construye la comunicación segura y automatizada de todo tu clúster. Entender el '*'porqué'* detrás de cada comando es lo que distingue a un simple ejecutor de un verdadero arquitecto de sistemas.