PHP: connessione SSH con le chiavi RSA

In questo articolo vedremo connettersi con PHP tramite SSH usando le chiavi RSA.

Possiamo implementare la seguente funzione:

```
function connect_to_ssh_with_keys($host, $port,
$username, $private_key, $public_key) {

    $connection = ssh2_connect($host, $port);

    if (!$connection) {
        throw new Exception("Could not connect to
$host on port $port.");
    }

    if(!file_exists($private_key) ||
!is_readable($private_key)) {
        throw new Exception("Private key file
$private_key does not exist.");
    }

    $private_key_file =
file_get_contents($private_key);

    if(!file_exists($public_key) ||
!is_readable($public_key)) {
        throw new Exception("Public key file
$public_key does not exist.");
```

```
    }

    if (!ssh2_auth_pubkey_file($connection,
$username, $public_key, $private_key)) {
        throw new Exception("Could not authenticate
with username $username " .
            "and private key $private_key.");
    }

    return $connection;
}
```

La funzione ha cinque parametri: `$host` (l'indirizzo dell'host SSH), `$port` (la porta SSH), `$username` (il nome utente per l'autenticazione), `$private_key` (il percorso del file della chiave privata) e `$public_key` (il percorso del file della chiave pubblica).

Viene utilizzata la funzione `ssh2_connect()` per stabilire una connessione SSH al server specificato utilizzando l'indirizzo `$host` e la porta `$port`. Se la connessione non riesce ad essere stabilita, viene generata un'eccezione con un messaggio di errore corrispondente.

Viene verificata l'esistenza e la leggibilità del file della chiave privata specificato utilizzando le funzioni `file_exists()` e `is_readable()`. Se il file non esiste o non è leggibile, viene generata un'eccezione con un messaggio di errore appropriato.

Viene letto il contenuto del file della chiave privata utilizzando la funzione `file_get_contents()` e il risultato viene assegnato alla variabile `$private_key_file`.

Viene verificata l'esistenza e la leggibilità del file della chiave pubblica specificato utilizzando le funzioni `file_exists()` e `is_readable()`. Se

il file non esiste o non è leggibile, viene generata un'eccezione con un messaggio di errore appropriato.

Viene utilizzata la funzione `ssh2_auth_pubkey_file()` per autenticarsi con il server SSH utilizzando il nome utente `$username`, il percorso del file della chiave pubblica `$public_key` e il percorso del file della chiave privata `$private_key`. Se l'autenticazione fallisce, viene generata un'eccezione con un messaggio di errore appropriato.

Infine, se tutte le verifiche e l'autenticazione hanno successo, la funzione restituisce l'oggetto di connessione SSH.

Riferimenti

PHP: SSH2