

Abrufen von Click-User-Schlüsseln für den Zugriff auf die bereitgestellte VM

Inhalt

[Einführung](#)

[Abrufen von Click-User-Schlüsseln für den Zugriff auf die bereitgestellte VM](#)

Einführung

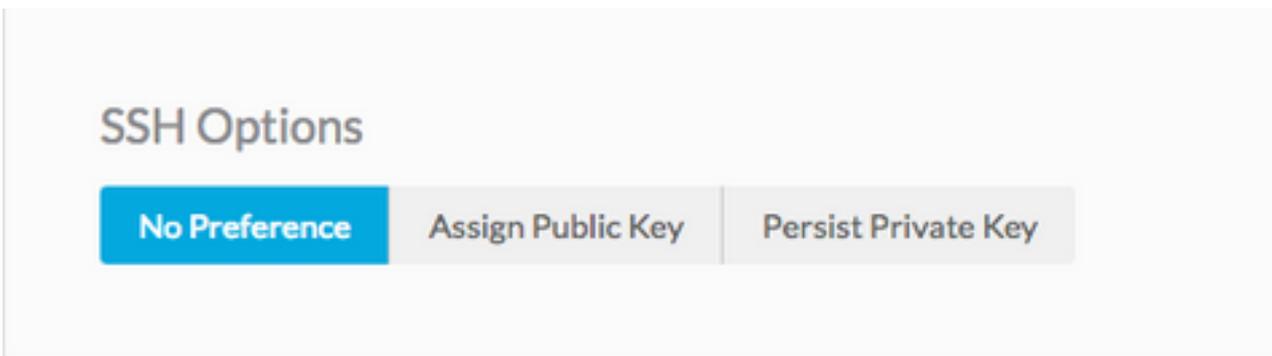
In diesem Dokument wird beschrieben, wie Sie die Datei `cliqr-user-keys.pem` abrufen und verwenden, um auf das bereitgestellte virtuelle System (VM) zuzugreifen, wenn zum Zeitpunkt der Bereitstellung keine benutzerdefinierten Schlüssel bereitgestellt wurden.

Abrufen von Click-User-Schlüsseln für den Zugriff auf die bereitgestellte VM

Wenn ein Benutzer die Anwendung bereitstellt, ohne die benutzerdefinierten Schlüssel bereitzustellen, verwendet er standardmäßig die Schlüssel seines Besitzers, um die Instanz bereitzustellen.

Um die Benutzerschlüssel für den Client abzurufen, gehen Sie wie folgt vor:

1. Melden Sie sich bei der **CCM-GUI** an, und stellen Sie die Anwendung ohne Voreinstellungen wie im Bild gezeigt bereit.



2. Die Schlüssel können mithilfe eines API-Schlüssels abgerufen werden. In diesem Fall wird der Befehl `curl` verwendet, um den Benutzerschlüssel abzurufen, von dem Cliqr die Instanz bereitstellt.

```
curl -k -X GET -H "Accept: application/json" -u cliqradmin:395C1C3A7ACF10D7 "https://<CCM IP>/v1/users/2/keys"
```

Ausgabe:

```
{ "apiKey": { "key": "395C1C3A7ACF10D7" }, "sshKeys": [ { "key": "-----BEGIN RSA PRIVATE KEY-----\nIv5rX89S7a14MzD3LEAKVWYWmRUxHdMT\n0NjAV6zDCztBgclCM+fYzP89rTTIBN29Rzb9c9H9ZtOWOP1\n/f4y+mF0dzqJgHkGT\nnAQKlQ6tX8Ygwu/corazC3gvBozl32RvFR/6hreFpKUDsoqsuo6hXJTua/xyaotmq\nnvPJoqpXwGZK"
```

```
sSMVYHFN2USo2gG21fR7bwhChA6DJY5LsmUKngQoTmWdU7x/F2AMl\n9xSudL0vNVZ+fMuB4k3
rIAupH6LFARot+tpl+QIDAQABAoIBAHLRIri6foJERj8e\nB1ljNrPgPwBKcnJ2Cwwf498ivp0dz561FRT3uYdaVqUJWf5X2
51BslXo02FBpZO\ndG2XedaYRx9tBHAPvfm1D742tyxe+gWv19KpOYaApE7CciVdRyG3OrDbM
diH9cJz\n1s45GQPOs+oXcNGqCofHhsD8frqXt/qTPOKP78hgX3bomk7N4v/2kRW0v6JfB4/W\ntS8D1B9Ngtq+==\n-----
END RSA PRIVATE KEY-----
\n", "cloudAccountId": "1", "cloudAccountName": "12345678908", "cloudRegionId": "1", "cloud": "Vihar_AWS
_HA-us-east-2"}],
```

3. Kopieren Sie den privaten Schlüssel in eine Datei, sobald Sie die Ausgabe erhalten haben.

```
echo -e "insert keys here" > key.pem && chmod 0400 key.pem
```

Hinweis: Sie müssen den Schlüssel kopieren, der von **- BEGINNT RSA to —END RSA Keys—** beginnt. Dies ist die SSH-Option (Secure Shell). Wenn für die Bereitstellung ein benutzerdefiniertes Betriebssystem bereitgestellt wird, kann der Benutzer entsprechend der Cloud-Init Änderungen vornehmen.

4. SSH an die Instanz an, die die **key.pem**-Datei verwendet.

```
ssh -i user2.pem cliqruser@IP ADDR
```