

## Configure SSH without using a password or passphrase between primary and standby server.

### For Linux or Unix. Document version 1.1

To configure SSH without using a password or passphrase the utility ssh-keygen is run. You have to create a RSA authentication key to be able to log into a remote site from your account. This should be done as the Dbvisit software owner, never as root!

#### Important:

Ensure the home directories (cd \$HOME) of the accounts on the primary and standby servers have the following permissions:

```
[oracle@avisit01]$ ls -al .  
drwxr-xr-x 40 oracle dba 4096 Sep 17 02:46 .
```

If the permissions are 775 or 777 then ssh may keep asking for a password. Change permission with: `chmod 755 .`

1. On the primary server as Dbvisit Standby software owner (do not enter passphrase!):

```
[oracle@avisit01]$ ssh-keygen  
Generating public/private dsa key pair.  
Enter file in which to save the key (/oracle/orabase/.ssh/id_dsa):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /oracle/orabase/.ssh/id_dsa.  
Your public key has been saved in /oracle/orabase/.ssh/id_dsa.pub.  
The key fingerprint is:  
73:c7:f5:7c:ee:bd:62:7f:0d:51:ed:8a:c7:45:f7:d9 oracle@avisit01
```

In this example avisit01 is the primary server and avisit03 is the standby server

The public/private key pair may either be dsa or rsa.

On some implementations of ssh, you have to specify: `ssh-keygen -t dsa`

#### On Linux the output may be different:

```
[oracle@avisit01]$ ssh-keygen  
Generating public/private rsa key pair.  
Enter file in which to save the key (/oracle/orabase/.ssh/identity):  
Enter passphrase (empty for no passphrase):  
Enter same passphrase again:  
Your identification has been saved in /oracle/orabase/.ssh/identity.  
Your public key has been saved in /oracle/orabase/.ssh/identity.pub.  
The key fingerprint is:  
a2:88:ad:53:e8:5b:37:a1:82:6d:03:ec:96:c4:6b:df oracle@avisit01
```

In this example avisit01 is the primary server and avisit03 is the standby server

This will generate 2 files under your home directory:

```
.ssh/id_dsa  
.ssh/id_dsa.pub
```

Or generate the following files under your home directory:

```
.ssh/id_rsa  
.ssh/id_rsa.pub
```

On Linux the files may be called different.

```
.ssh/identity  
.ssh/identity.pub
```

2. On the standby server as Dbvisit Standby software owner (do not enter passphrase!):

```
[oracle@avisit03]$ ssh-keygen  
Generating public/private dsa key pair.  
Enter file in which to save the key (/oracle/orabase/.ssh/id_dsa):
```

```

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /oracle/orabase/.ssh/id_dsa.
Your public key has been saved in /oracle/orabase/.ssh/id_dsa.pub.
The key fingerprint is:
73:c7:f5:7c:ee:bd:62:7f:0d:51:ed:8a:c7:45:f7:d9 oracle@avisit03

```

In this example avisit01 is the primary server and avisit03 is the standby server

The public/private key pair may either be dsa or rsa

**On Linux the output may be different:**

```

[oracle@avisit03]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/oracle/orabase/.ssh/identity):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /oracle/orabase/.ssh/identity.
Your public key has been saved in /oracle/orabase/.ssh/identity.pub.
The key fingerprint is:
a2:88:ad:53:e8:5b:37:a1:82:6d:03:ec:96:c4:6b:df oracle@avisit03

```

In this example avisit01 is the primary server and avisit03 is the standby server

This will generate 2 files under your home directory:

```

.ssh/id_dsa
.ssh/id_dsa.pub

```

Or generate the following files under your home directory:

```

.ssh/id_rsa
.ssh/id_rsa.pub

```

**On Linux the files may be called different**

```

.ssh/identity
.ssh/identity.pub

```

3. On the standby server create a new empty file called `.ssh/authorized_keys`

```

[oracle@avisit03]$ cd .ssh
[oracle@avisit03]$ vi authorized_keys

```

In this example avisit01 is the primary server and avisit03 is the standby server

4. Copy the contents of file `.ssh/id_dsa.pub` from the primary server to the new file `.ssh/authorized_keys` on the standby server. The file may be called `identity.pub` or `id_rsa.pub` instead of `id_dsa.pub`.

```

[oracle@avisit01]$ cat id_dsa.pub
ssh-dss AAAAB3NzaC1kc3MAAACBALj5RhJzSDOvRnTID/P2kblmE9qM2zCrzUa0gDL/fbngdcB8EELeJJi
LuhR9uM/XyQr+UySGVeMS1jM0uBfQcs/7p3WAEkxncXzGduxlsyO8iyYfr8Kf7ufGPdJq7n15v0hjUMWSa
w6YcA== oracle@avisit01

```

5. Ensure the new file `.ssh/authorized_keys` has the correct permission:

```

[oracle@avisit01]$ chmod 600 authorized_keys

```

6. On the primary server create a new empty file called `.ssh/authorized_keys`

```

[oracle@avisit01]$ cd .ssh
[oracle@avisit01]$ vi authorized_keys

```

In this example avisit01 is the primary server and avisit03 is the standby server

7. Copy the contents of file `.ssh/id_dsa.pub` from the standby server to the new file `.ssh/authorized_keys` on the primary server. The file may be called `identity.pub` or `id_rsa.pub` instead of `id_dsa.pub`.

```

[oracle@avisit03]$ cat id_dsa.pub
ssh-dss AAAAB3NzaC1kc3MAAACBALj5RhJzSDOvRnTID/P2kblmE9qM2zCrzUa0gDL/fbngdcB8EELeJJi
LuhR9uM/XyQr+UySGVeMS1jM0uBfQcs/7p3WAEkxncXzGduxlsyO8iyYfr8Kf7ufGPdJq7n15v0hjUMWSa
w6YcA== oracle@avisit03

```

8. Ensure the new file `.ssh/authorized_keys` has the correct permission:

```
[oracle@avisit01]$ chmod 600 authorized_keys
```

SSH is now setup and configured. To test:

On the primary server:

```
[oracle@avisit01]$ ssh avisit03 ls -al
The authenticity of host 'avisit03 (10.1.1.82)' can't be established.
RSA key fingerprint is 40:bb:ea:96:48:7d:22:fa:36:a6:8e:e7:37:7c:f4:d3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'avisit03,10.1.1.82' (RSA) to the list of known hosts.
total 896
drwxr-xr-x 26 oracle dba 4096 Feb 27 18:49 .
drwxr-xr-x 6 root root 4096 May 30 2006 ..
-rw----- 1 oracle dba 2640 Feb 15 09:39 .ICEauthority
drwx----- 5 oracle dba 4096 May 21 2006 .Trash
-rw----- 1 oracle dba 120 Feb 15 09:39 .Xauthority
-rw-r--r-- 1 oracle dba 76 May 24 2006 .alias
-rw----- 1 oracle dba 16019 Jun 1 2006 .bash_history
...
...
```

In this example avisit01 is the primary server and avisit03 is the standby server

On the standby server:

```
[oracle@avisit03]$ ssh avisit01 ls -al
The authenticity of host 'avisit01 (10.1.1.81)' can't be established.
RSA key fingerprint is 40:bb:ea:96:48:7d:22:fa:36:a6:8e:e7:37:7c:f4:d3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'avisit01,10.1.1.81' (RSA) to the list of known hosts.
total 896
drwxr-xr-x 26 oracle dba 4096 Feb 27 18:49 .
drwxr-xr-x 6 root root 4096 May 30 2006 ..
-rw----- 1 oracle dba 2640 Feb 15 09:39 .ICEauthority
drwx----- 5 oracle dba 4096 May 21 2006 .Trash
-rw----- 1 oracle dba 120 Feb 15 09:39 .Xauthority
-rw-r--r-- 1 oracle dba 76 May 24 2006 .alias
-rw----- 1 oracle dba 16019 Jun 1 2006 .bash_history
...
...
```

In this example avisit01 is the primary server and avisit03 is the standby server

Secure shell configuration is now completed.

For more information on SSH, please consult the *man* pages in Unix or Linux.