Technical Note: SSH

Bas Meijer 2016

```
Mar 11 22:09:48 web sshd[2889]: Accepted certificate
ID "ansible_bas" signed by RSA CA
a7:e5:a4:65:5e:b2:de:0d:1b:d7:86:56:08:fc:70:1f
via /etc/ssh/ca_key.pub
```

Automation

- Automate deployment with Ansible
- Git stores every change in playbooks
- Adminstrator avoids change in interactive logons

```
'( umask 22 && mkdir -p "$( echo $HOME/.ansible/tmp/ansible-
tmp-1457871526.58-41244554513251 )" && echo "$( echo
$HOME/.ansible/tmp/ansible-tmp-1457871526.58-41244554513251 )"
)'tmp-1457871526.58-41244554513251 )" )'
```

- Ansible only needs SSH access.

- So it must be secure, right?

```
ssh-copy-id ansible@yourserver.com
```

SSH Issues

1. Insiders manipulate the SSH authorized_keys
2. Someone uses another key-pair
3. SSH key distribution is a pain, joiners/leavers
4. Misuse of ansible private key for interactive logon

authorized_keys manipulation

- I consider users adding pubkeys an anti-pattern
- Keys must be writable only by the root user but readable by the user requiring access (chattr +i).
- AuthorizedKeysFile /etc/ssh/authorized_keys/%u

```
ssh-copy-id ansible@yourserver.com
```

Use of another ssh key-pair

- authorized_keys restricted with options (rsync)
- abuse of other user’s keys without a passphrase
- The private key should be protected, by a passphrase or in hardware token.

```
[bas@sql ~]$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/bas/.ssh/id_rsa):
Created directory '/home/bas/.ssh'.
Enter passphrase (~~empty for no passphrase~~):
```

Manage key usage options

- One advantage of using certificates is that you don't have to distribute the public keys to the correct system for each user.

- Signing the public keys with a central PKI authority adds significant security. Limit user, host, options.

- This is not X.509, ssh-keygen does all of it.

```
ssh-keygen -f ca_key
ssh-keygen -s ca_key -I key_id -h -Z host.domain user_key.pub
```

Key distribution is a pain

- Distributing individual keys does not scale

- Only the CA public key should be once put on the system and mentioned in the sshd_config file

- Abandon local authorized_keys files

```
TrustedUserCAKeys /etc/ssh/ca_key.pub
AuthorizedKeysFile /dev/null
```

Someone leaves

- Signed public keys can have an expiry
- Revocation lists should be centrally managed.

```
ssh-keygen -s ca_key -I id -n bas -V +1M id_rsa.pub
```

Misuse the ansible private key for interactive logon

- Ansible should automate, not hotfix
- Encourage playbooks
- Encourage accountability
- Interactive shell should be logged out

```
echo logout > /home/ansible/.bash_profile
```