itspeople

Tools für DBA‘s und Cloud-Nutzer: ssh – die Secure Shell

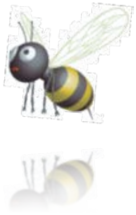
11. August 2017

Robert Marz

DOAG

Robert Marz

Kunde	Technical Architect mit datenbankzentrischem Weltbild
its-people	Portfoliomanager Datenbanken Blogredakteur
DOAG	Themenverantwortlicher „Cloud“ in der Datenbank Community



@RobbieDatabee

blog.its-people.de

Robert.Marz
@its-people.de

ssh – the secure shell

Netzwerkprotokoll

Verschlüsselt

Client-Server:

Client: ssh
Server: sshd

Open Source

OpenSSH

Versionen

1.x : veraltet, unsicher
2.x: aktuell

ssh – mächtige Tools

Defacto Standard für verschlüsselte Konsolenverbindungen

- Ersatz für telnet, rlogin, rsh, etc.
- Rechner zu Rechner
- SSL verschlüsselt

Kann viel mehr:

- Automatisches Login
- Netzwerktunnel (VPN im Eigenbau)
- Dateitransfer
- Remote-Filesystem
- Tunnelketten

Konfigurationsdateien

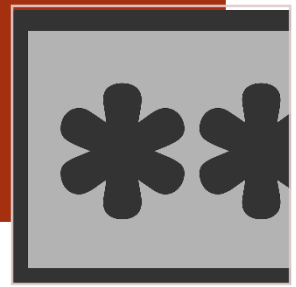
Global in /etc, per User in ~/.ssh

- Server (sshd)
  - sshd_config
  - authorized_keys*
  - sshrc
- Client (ssh)
  - config*
  - known_hosts*
  - Keys*
    - Private*
      - identity
      - id_dsa
      - id_rsa
      - …
    - Public*
      - identity.pub
      - id_dsa.pub
      - id_rsa.pub
      - …
  - sshrc
  - environment

Kennwort oder Schlüsselpaar?

- Merken
- Kurz
- Keylogger
- „Wandern“
+ Einfach

Kennwörter



+ Datei
+ Komplex
+ Privater Teil nur lokal
-„Komplizierter“

Schlüsselpaar

Konfigurationsdateien: known_hosts

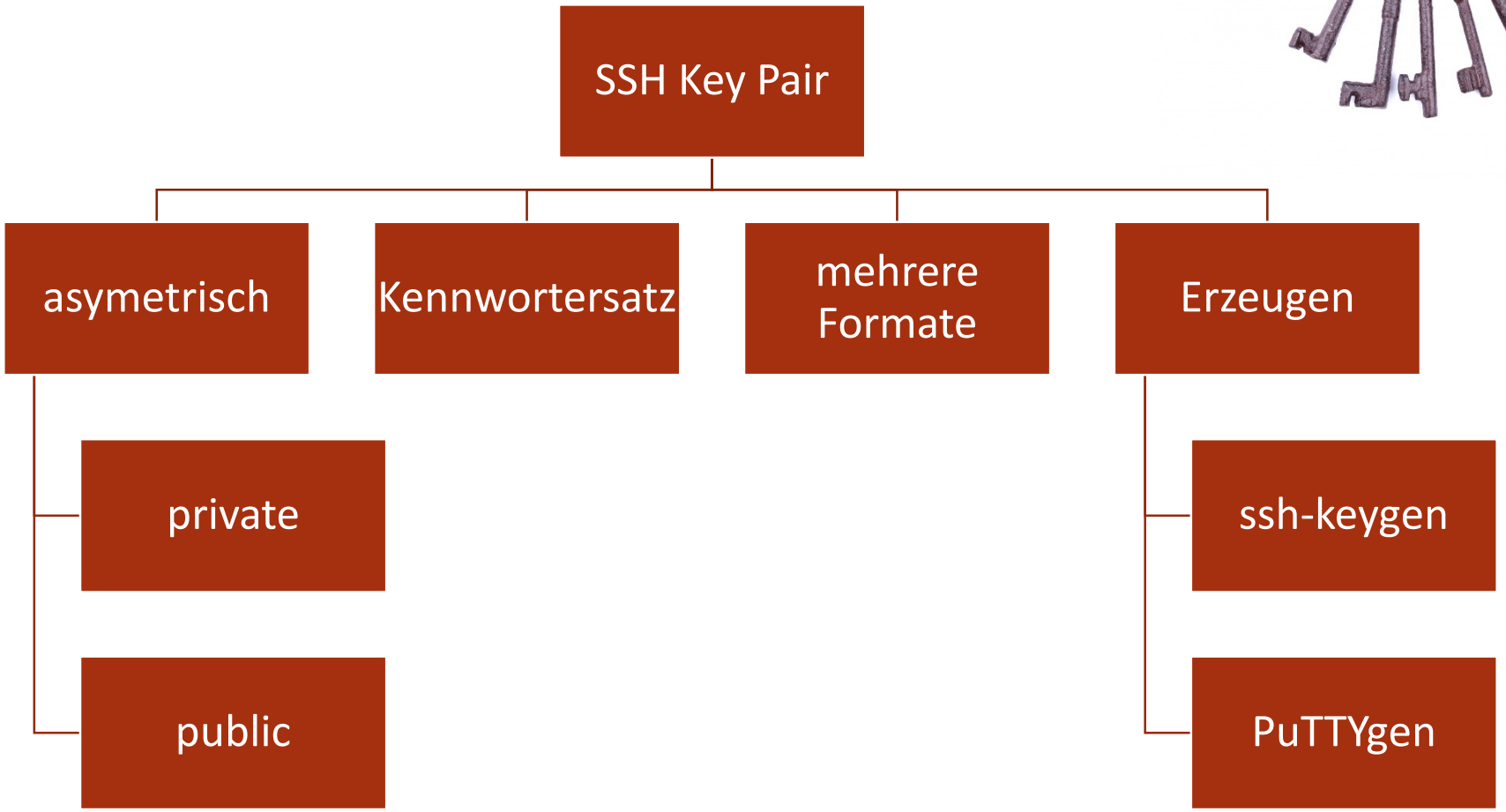
known_hosts (Client)

```
[rmarz@niteowl ~]$ ssh no-web
The authenticity of host 'no-web (10.145.176.14)' can't be established.
RSA key fingerprint is 49:29:a4:ac:5b:f0:6e:5c:83:40:68:a8:77:bc:32:e3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'no-web' (RSA) to the list of known hosts.
```

- Merkliste bekannte Server
- Vertrauensstellung (Achtung!)
  - Kennwortübertragung im Klartext
  - Bekannte Exploits

```
Warning: the RSA host key for 'no-web' differs from the key for the IP address '10.145.176.14'
Offending key for IP in /home/rmarz/.ssh/known_hosts:17
```

SSH Schlüssel



Der Public Key

Verteilen

ssh-copy-id
E-Mail
Cloud Web-Oberfläche

Dateiname (default)

identity.pub
id_dsa.pub
id_rsa.pub
Beliebig

Der Private Key

Dateiname (default)

identity
id_dsa
id_rsa

Beliebiger Dateiname

ssh –i /pfad/zum/private/key

Verlässt NIEMALS freiwillig den Rechner

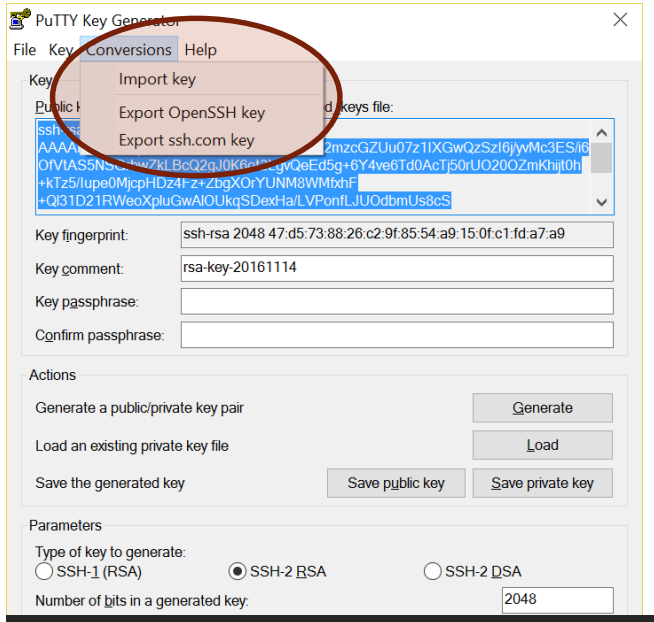
Privat und Geheim

Mit Kennwort verschlüsselbar

SSH Key Formate

openssh	Offizieller Standard Komplett verschlüsselt RFC 4716
Putty	Eigenes Format Public Key unverschlüsselt Mehrzeilig
ssh.com	Kommerzielle Variante Wenig verbreitet

Umwandlung mit Texteditor oder Tool




```
PuTTY Format:

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20161114"
AAAAB3NzaC1yc2EAAAABJQAAAQEAgOH2mzcGZUu07z1IXGwQzSzI6j/yvMc3ES/i
6OfVtAS5NSGrbwZkLBcQ2gJ0K6ot2LgvQeEd5g+6Y4ve6Td0AcTj50rUO20OZmKh
ijt0h+kTz5/Iupe0MjcpHDz4Fz+ZbgXOrYUNM8WMfxhF+Ql31D21RWeoXpluGwAl
OUkqSDexHa/LVPonfLJUOdbmUs8cS+e3Cdd6MDRJeXAoArxFZAfveRXK9RT0DBOc
gcIEv3/s9Vtyp5bg/NHsV40am/jUemDlSQIL/1ZBI4dKmGt4EV43tqSaZg3ylbEn
knAgDpCgBCs0VHpbRLbLJCR/9umS1TNklalkuqiYI2xEmJqOXQ==
---- END SSH2 PUBLIC KEY ----

######################################################################

openSSH-Format:

ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAgOH2mzcGZUu07z1IXGwQzSzI6j/yvMc3ES/
i6OfVtAS5NSGrbwZkLBcQ2gJ0K6ot2LgvQeEd5g+6Y4ve6Td0AcTj50rUO20OZmKhijt0h+kTz5/
Iupe0MjcpHDz4Fz+ZbgXOrYUNM8WMfxhF+Ql31D21RWeoXpluGwAlOUkqSDexHa/
LVPonfLJUOdbmUs8cS+e3Cdd6MDRJeXAoArxFZAfveRXK9RT0DBOcgcIEv3/s9Vtyp5bg/NHsV40am/
jUemDlSQIL/1ZBI4dKmGt4EV43tqSaZg3ylbEnknAgDpCgBCs0VHpbRLbLJCR/9umS1TNklalkuqiYI
2xEmJqOXQ== rsa-key-20161114
```

Konfigurationsdateien: authorized_keys

authorized_keys (Server)

erlaubt Zugriff

- auf den Server
- pro User

Optionen (Auszug)

- command
- Environment
- From
- no-pty
- restrict (verbietet alles)
- gezieltes erlauben möglich

```
# Comments allowed at start of line
ssh-rsa AAAAB3Nza...LiPk== user@example.net

from="*.sales.example.net,!pc.sales.example.net"
ssh-rsa AAAAB2...19Q== john@example.net

command="dump /home",no-pty,no-port-forwarding
ssh-dss AAAAC3...51R== example.net

permitopen="192.0.2.1:80",permitopen="192.0.2.2:
25" ssh-dss AAAAB5...21S==

tunnel="0",command="sh /etc/netstart tun0" ssh-
rsa AAAA...== jane@example.net

restrict,command="uptime" ssh-rsa
AAAA1C8...32Tv== user@example.net

restrict,pty,command="nethack" ssh-rsa
AAAA1f8...IrrC5== user@example.net
```

Netzwerk Tunnel

Mini VPN

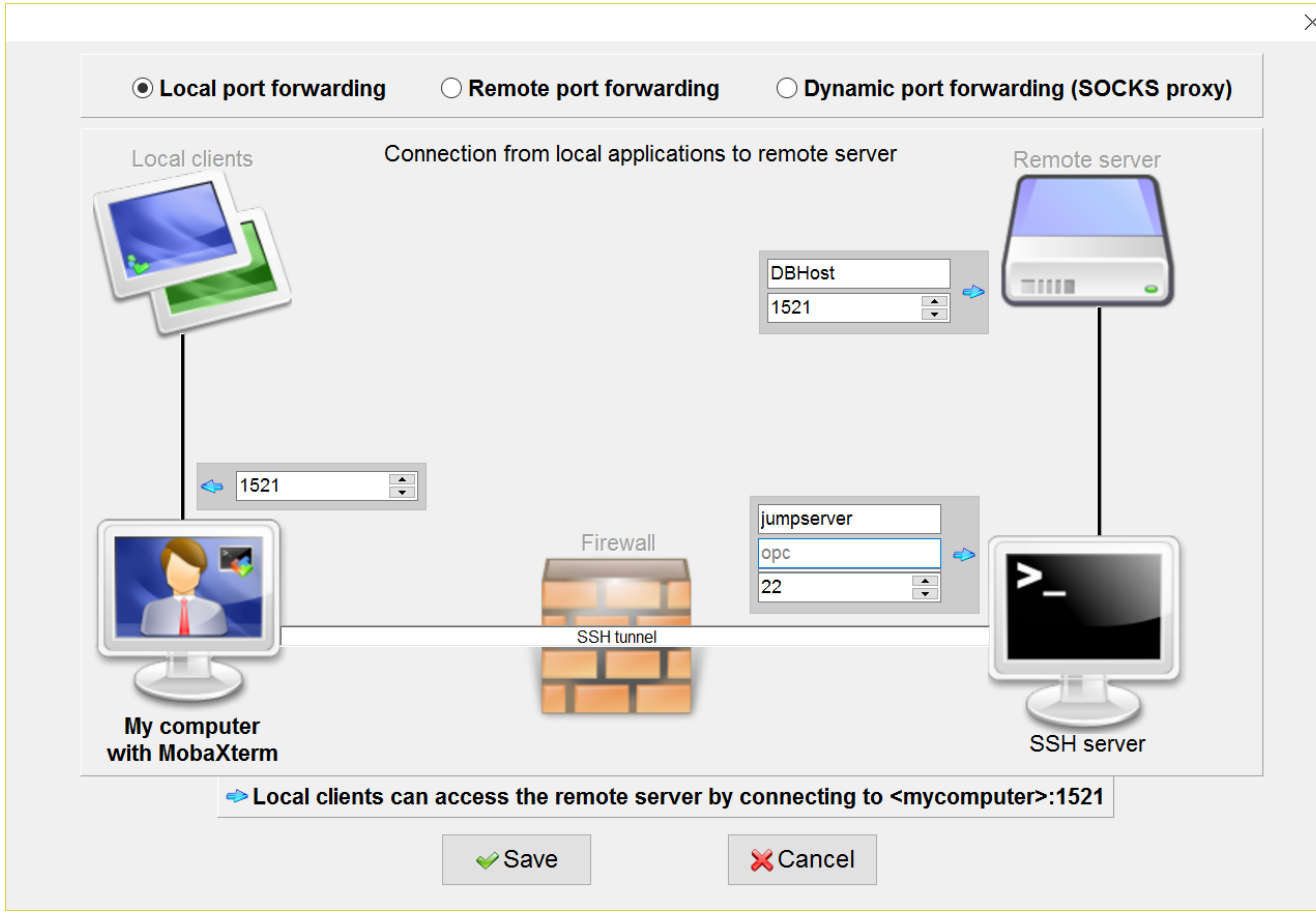
Parameter
- -L lport:zielrechner:dport
- -L 1521:127.0.0.1:1521

Tools

SQL Developer
SQLcl
MobaXterm

Spielart:

X11 Forwarding
SOCKS5-Tunnel
- https-Proxy
- Parameter -D portnummer



Sicherer Dateitransfer

scp

- Secure Copy

sftp

- Secure FTP

rsync -e ssh

- Remote Sync

tar

- ssh user@remote.host "tar czpf - /some/important/data" \
  | tar xzpf - -C /new/root/directory
- tar cpf - /some/important/data | ssh user@destination-machine \
  "tar xpf - -C /some/directory/"

Das Remotefilesystem sshfs

- Remote Filesystem
- lokales Einbinden
- Dauerhaft oder per Session
- Integration in Clients
  - (z.B.Midnight Commander)

Der ssh-agent

Speichert Keys

Entschlüsselt
Im RAM
Key Kennwort nur einmal eingeben

Key-Operationen

für Clients
Keine Weitergabe des Schlüssels

Linux:

ssh-agent
ssh-add

Windows:

PuTTY-Agent (pagent.exe)

Konfigurationsdateien: config

config (Client)

Aliase (host)

Shortcut für den ssh-Aufruf

Parameter

Gruppiert nach Host
- Wildcards möglich

Erster Treffer für Parameter gilt
- Von speziell zu allgemein

Beispiel

Hostname

User

IdentityFile

LocalForward

```
# Cloud Server
Host OraCloud*
    User opc
    IdentityFile ~/.ssh/OracleCloud-RobbieDatabee.ppk

Host OraCloud-DB12.2
    HostName 141.144.32.110
    LocalForward 1521 127.0.0.1:1521

Host OraCloud-DB12.1
    HostName 141.144.32.63
    LocalForward 6777 127.0.0.1:1521

# Home Router
Host schlumpf
    HostName schumpf.robbienet.local
    Port 8022
    User root
    IdentityFile ~/.ssh/nas01.key

# SSH via JumpServer
Host kunde1.abnahme
    HostName 192.168.42.116
    User orastred
    ProxyCommand  ssh rmarz@jumpserver.kunde.com nc %h %p 2> /dev/nul

# default values
Host *
    ForwardX11 no
    ForwardX11Trusted yes
    User rmarz
    Port 22
    Protocol 2
    ServerAliveInterval 60
    ServerAliveCountMax 30
```

Konfigurationsdateien: config - Beispiel

```
# Dieser Aufruf:
ssh -i ~/.ssh/id_ovm_manager_prod.ppk -p 10000 admin@ovm-manager.gis-ffm.mycompany.com

    # Wird duch diesen Eintrag in der ~/.ssh/config
    Host ovmcli
        Hostname ovm-manager.gis-ffm.mycompany.com
        User admin
        IdentityFile ~/.ssh/id_ovm_manager_prod.ppk
        Port 10000

            # Dauerhaft zu diesem Aufruf:
            ssh ovmcli
```

SSH Implementierungen

Unix / Linux

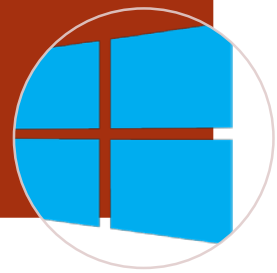
- Nativ

OSX (Mac)

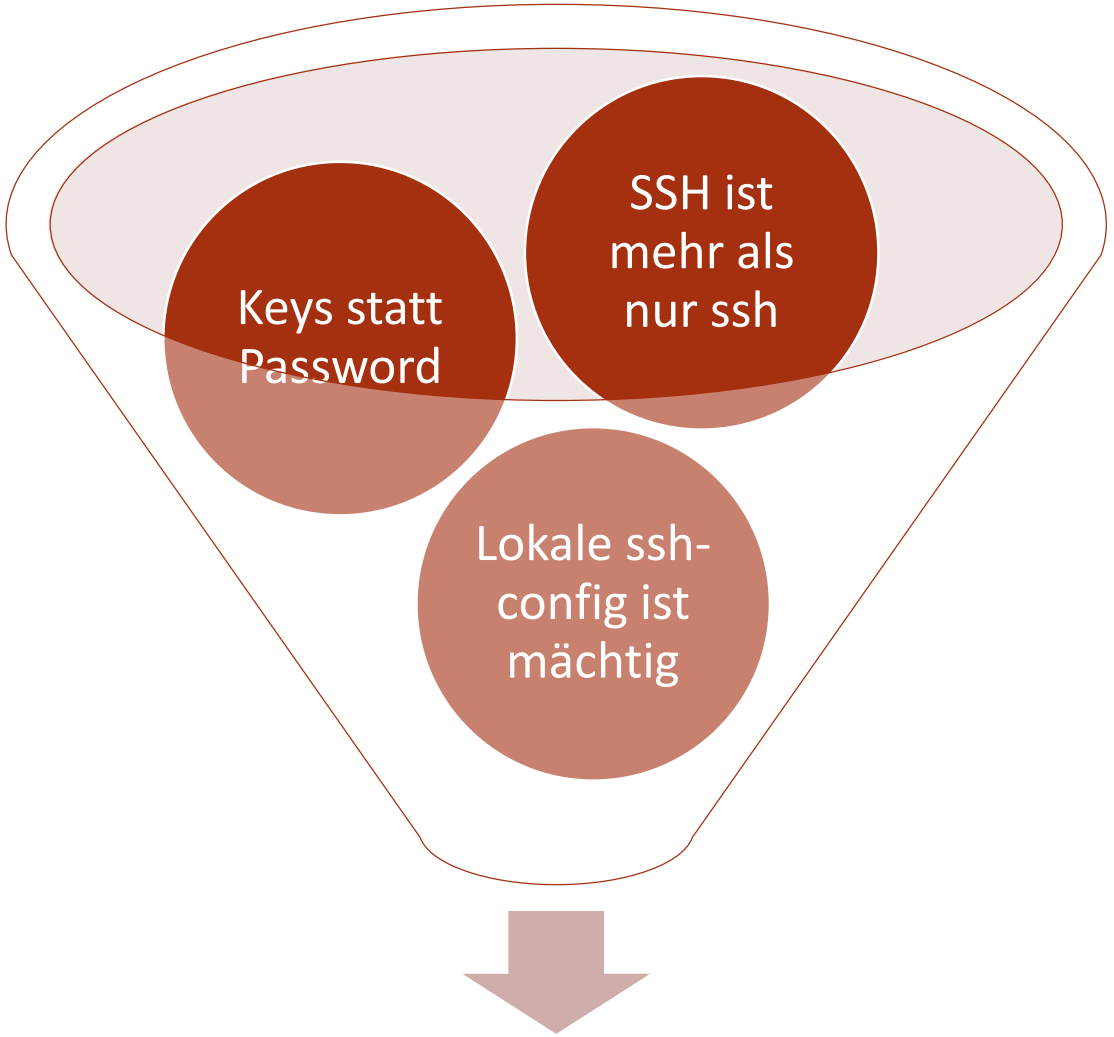
- Nativ

Windows

- Clients, z.B.
  - PuTTY
  - MobaXterm
  - mRemoteNG
  - Bash/Linux für Windows 10
  - PowerShell/Win32-OpenSSH von MS
- Server, z.B.
  - Bash/Linux für Windows 10
  - PowerShell/Win32-OpenSSH von MS



Fazit



Viel Spaß beim Ausprobieren!

Herzlichen Dank für Ihre Aufmerksamkeit !

we make the difference
www.its-people.de

Fragen ?

its-people GmbH

Frankfurt	Tel. 069 2475 2100
Hamburg	Tel. 040 2360 8808
Köln	Tel. 0221 1602 5204
München	Tel. 089 5484 2401

its-people ERP Beratungsgesellschaft mbH

Frankfurt	Tel. 069 2475 1980

www.its-people.de **info@its-people.de**