



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

17. November, 2016

Robert Marz



Robert Marz

Kunde

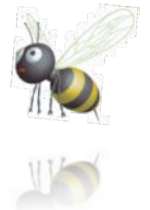
Technical Architect
mit datenbankzentrischem Weltbild

its-people

Portfoliomanager Datenbanken
Blogredakteur

DOAG

Themenverantwortlicher „Cloud“
in der Datenbank Community



@RobbieDatabee



blog.its-people.de



Robert.Marz
@its-people.de

its-people auf der DOAG 2016

- Quo vadis datum?
Data Lineaging in gewachsenen Warehouse-Strukturen
 - Jens Behring
 - Dienstag, 15.11. 13:00 Uhr Helsinki
- CSV mit reinem SQL und der Magie von JSON_TABLE einlesen
 - Robert Marz
 - Dienstag, 15.11 14:00 Uhr Oslo
- Eine Karte sagt mehr als 1000 Worte
 - Sven Brömer
 - Mittwoch 16.11. 12:00 Uhr Oslo
- Scripting mit SQLcl
Batchscripts auf einem neuen Level
 - Sabine Heimsath, Robert Marz
 - Mittwoch, 16.11. 14:00 Uhr Kopenhagen
- Panel:
Der DBA in der Cloud
 - Moderator Robert Marz
 - Donnerstag, 17.11. 10:00 Uhr Kiew
- **Werkzeuge für DBAs und Cloudnutzer: ssh**
 - **Robert Marz**
 - **Donnerstag, 17.11. 16:00 Uhr Oslo**

<http://www.its-people.de/doag-2016.html>



DOAG 2017 Datenbank

30.-31. Mai 2017 in Düsseldorf

datenbank.doag.org

Ab sofort Vortrag
einreichen!



ssh – the **secure shell**

Netzwerkprotokoll

Verschlüsselt

Client-Server:

Client: ssh

Server: sshd

Open Source

OpenSSH

Versionen

1.x : veraltet, unsicher

2.x: aktuell

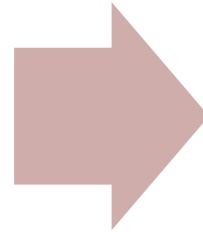


ssh – mächtige Tools



Defacto Standard für verschlüsselte Konsolenverbindungen

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



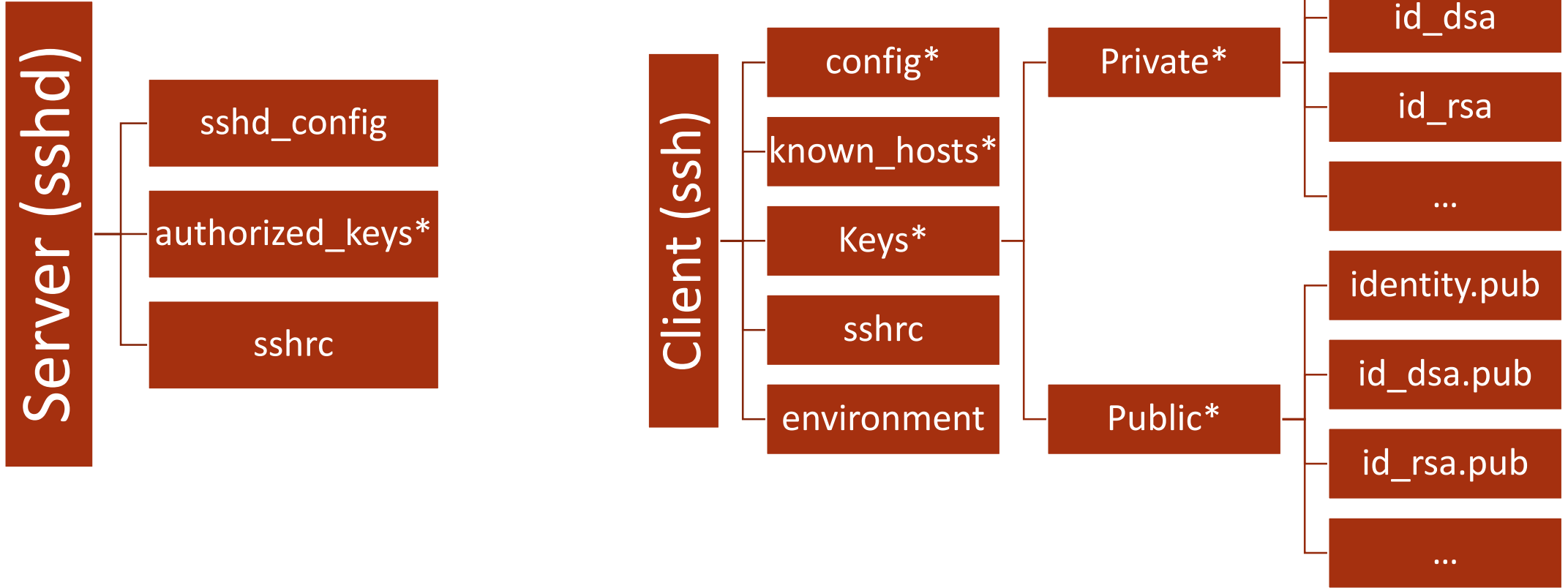
Kann viel mehr:

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



Konfigurationsdateien

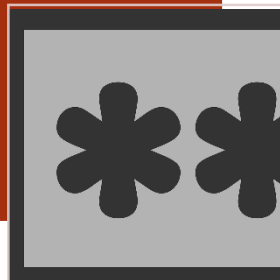
Global in /etc, per User in ~/.ssh



Kennwort oder Schlüsselpaar?

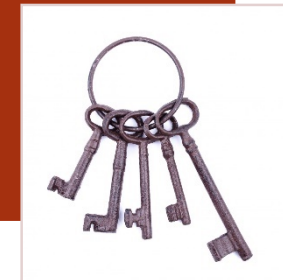
- Merken
- Kurz
- Keylogger
- „Wandern“
- Einfach

Kennwörter



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

Schlüsselpaar



Konfigurationsdateien: known_hosts



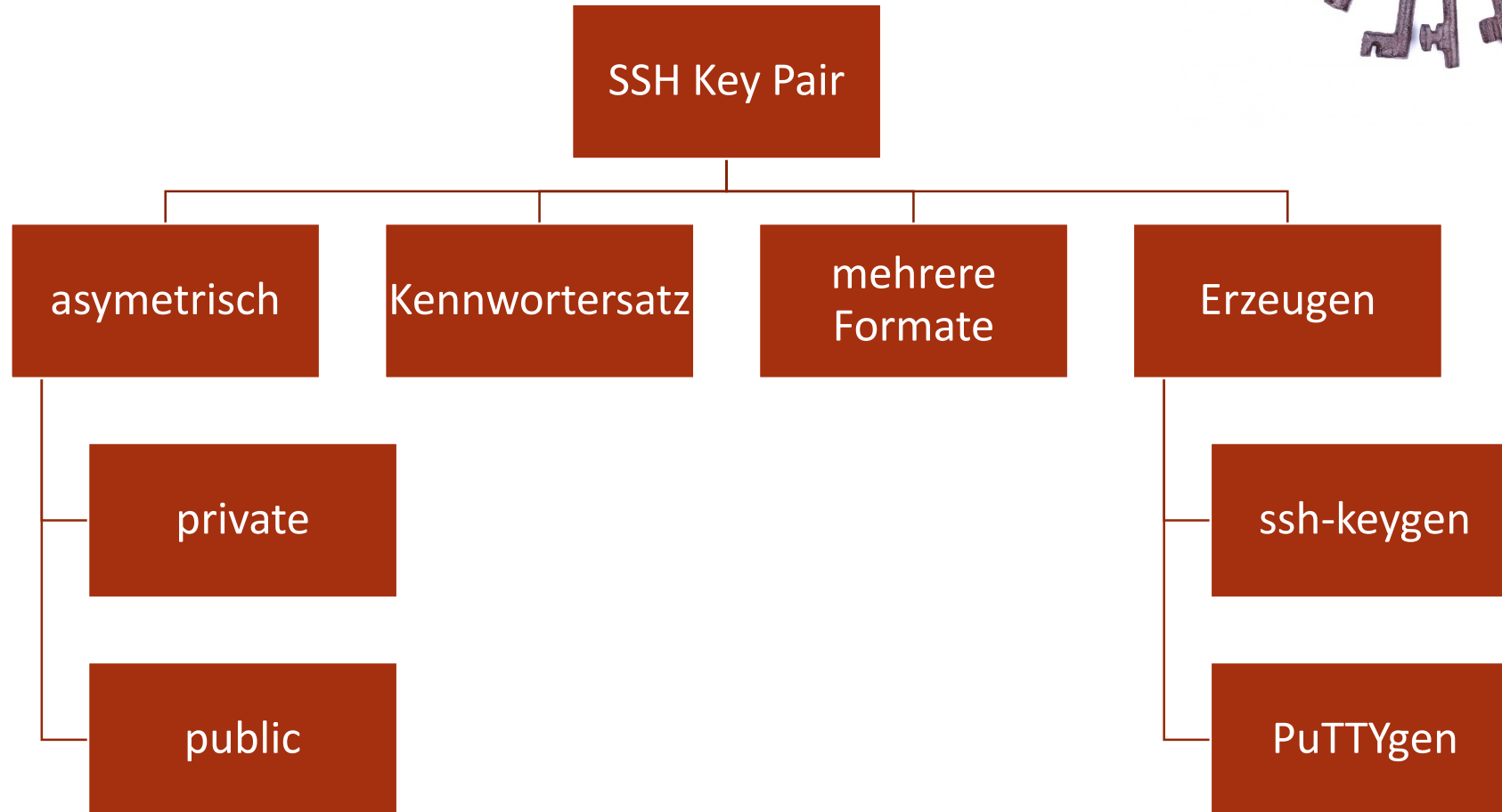
known_hosts (Client)

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

```
[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.
```

```
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](#)

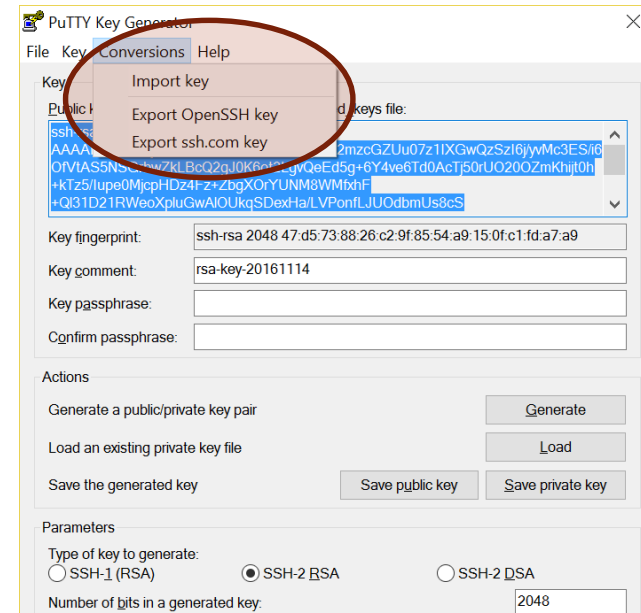
Putty

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
60fvTAS5NSGrbwZkLBcQ2gJ0K6ot2LgvQeEd5g+6Y4ve6Td0AcTj50rU0200ZmKh
ijt0h+kTz5/Iupe0MjcpHDz4Fz+ZbgX0rYUNM8WmfxfH+Q131D21RWeoXpluGwAl
OUkqSDexHa/LVPonfLJUodbmUs8cS+e3Cdd6MDRJeXAoArxFZafveRXX9RT0DB0c
gcIEv3/s9Vtyp5bg/NHsV40am/jUemDLSQIL/1ZBI4dKmGt4EV43tqSaZg3ylbEn
knAgDpCgBCs0VHpbRLbLJCR/9umS1TNkla1kuqiYI2xEmJq0XQ==
---- END SSH2 PUBLIC KEY ----

#####

openSSH-Format:

ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAgoH2mzcGZUu07z1IXGwQzSzi6j/yvMc3ES/
i60fvTAS5NSGrbwZkLBcQ2gJ0K6ot2LgvQeEd5g+6Y4ve6Td0AcTj50rU0200ZmKhijt0h+kTz5/
Iupe0MjcpHDz4Fz+ZbgX0rYUNM8WmfxfH+Q131D21RWeoXpluGwAlOUkqSDexHa/
LVPonfLJUodbmUs8cS+e3Cdd6MDRJeXAoArxFZafveRXX9RT0DB0cgcIEv3/s9Vtyp5bg/NHsV40am/
jUemDLSQIL/1ZBI4dKmGt4EV43tqSaZg3ylbEnknAgDpCgBCs0VHpbRLbLJCR/9umS1TNkla1kuqiYI
2xEmJq0XQ== 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

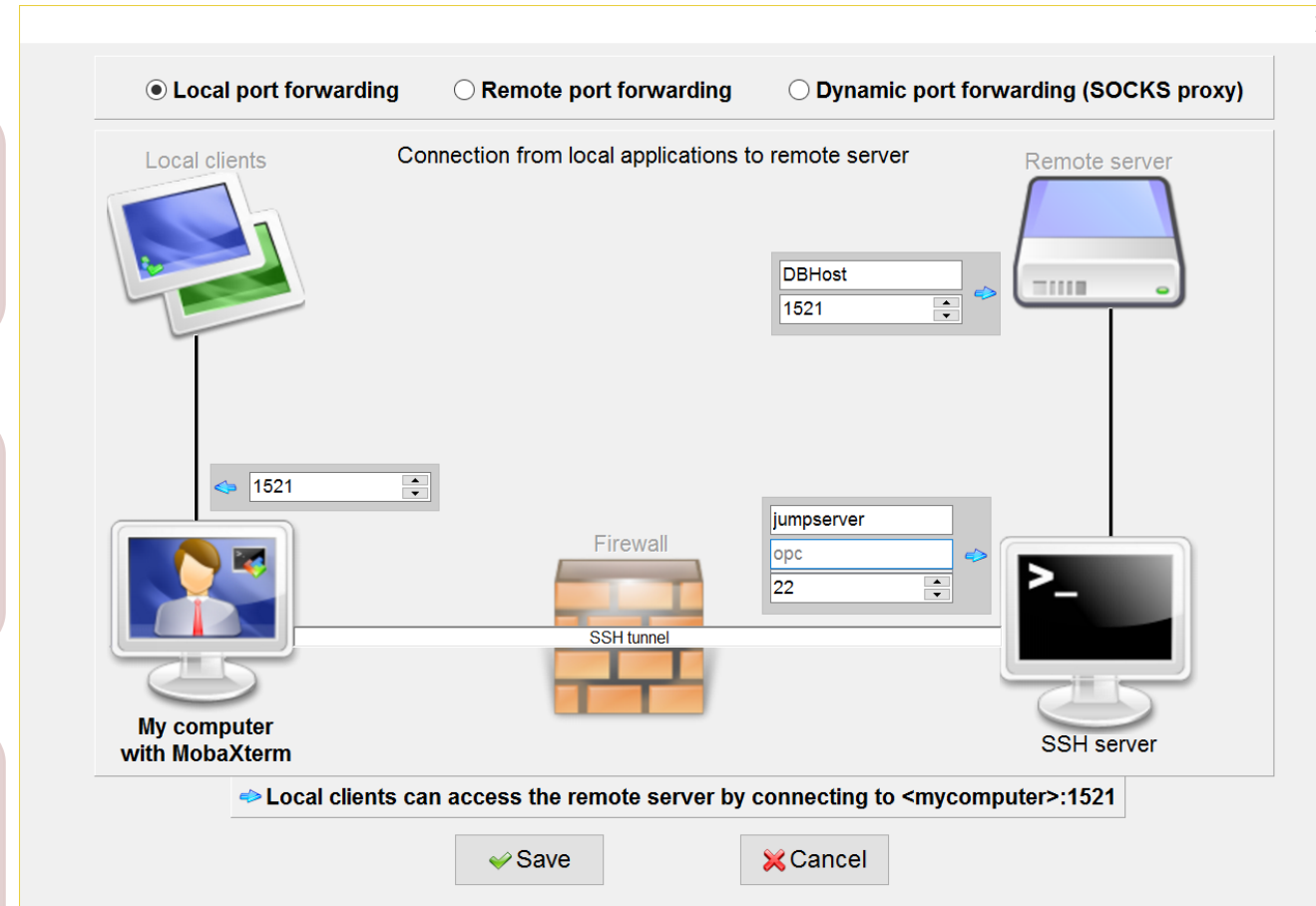
Parameter
 -L lport:zielrechner:dport
 -L 1521:127.0.0.1:1521

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

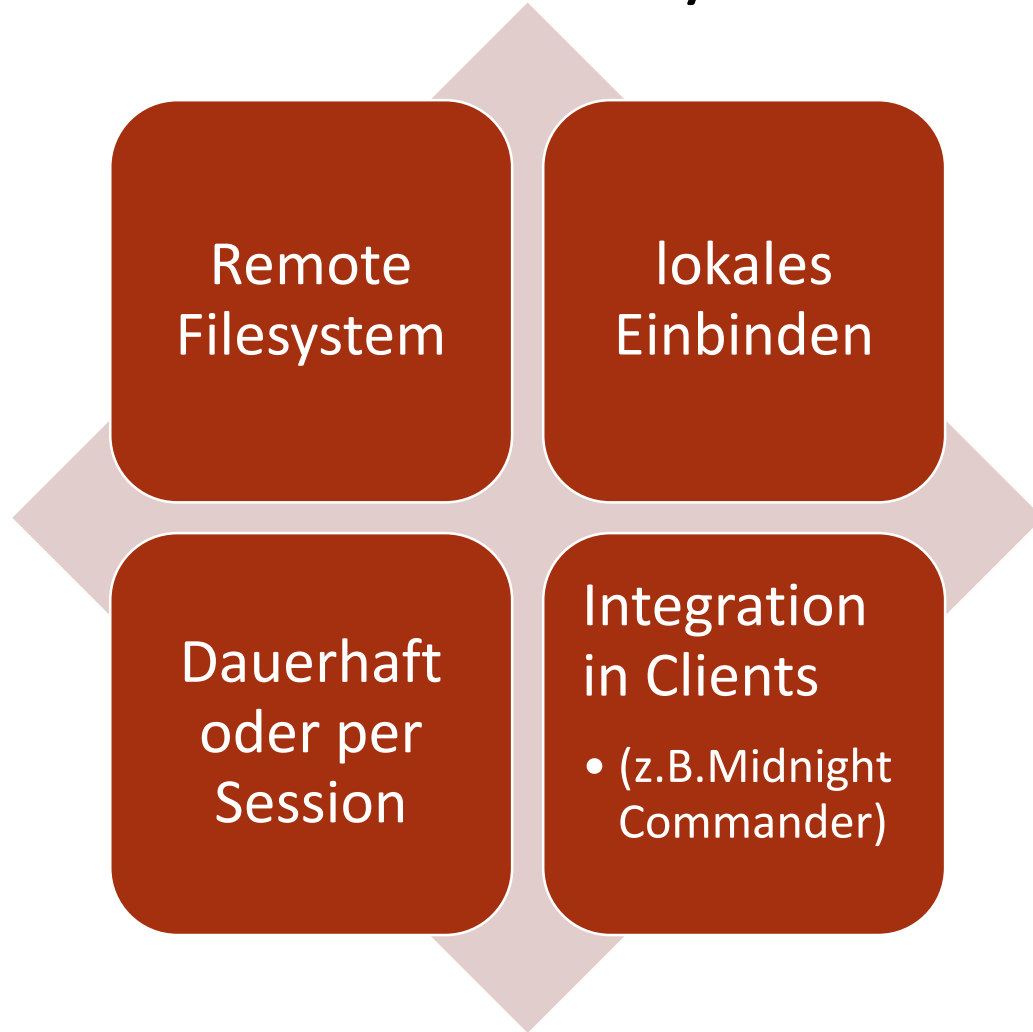
- Remote Sync

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



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
	Pro Host (Wildcards möglich)
Beispiel	Hostname User IdentityFile LocalForward

```

1 ### default for all ##
2 Host *
3     ForwardX11 no
4     ForwardX11Trusted yes
5     User rmarz
6     Port 22
7     Protocol 2
8     ServerAliveInterval 60
9     ServerAliveCountMax 30
10
11 ## override as per host ##
12 Host OraCloud*
13     User opc
14     IdentityFile ~/.ssh/
15         OracleCloud-RobbieDatabee.ppk
16
17 Host OraCloud-DB12.2
18     HostName 141.144.32.110
19     LocalForward 1521 127.0.0.1:1521
20
21 Host OraCloud-DB12.1
22     HostName 141.144.32.63
23     LocalForward 6777 127.0.0.1:1521
24
25 ## Home Router ##
26 Host schlumpf
27     HostName schumpf.robkienet.local
28     Port 8022
29     User root
30     IdentityFile ~/.ssh/nas01.key
31
32 # SSH via JumpServer
33 Host kunde1.abnahme
34     HostName 192.168.42.116
35     User orastred
36     ProxyCommand ssh rmarz@jumpserver.kunde.com
37         nc %h %p 2> /dev/null
  
```

SSH Implementierungen

- Nativ

Unix /
Linux



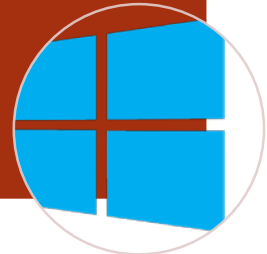
- Nativ

OSX (Mac)

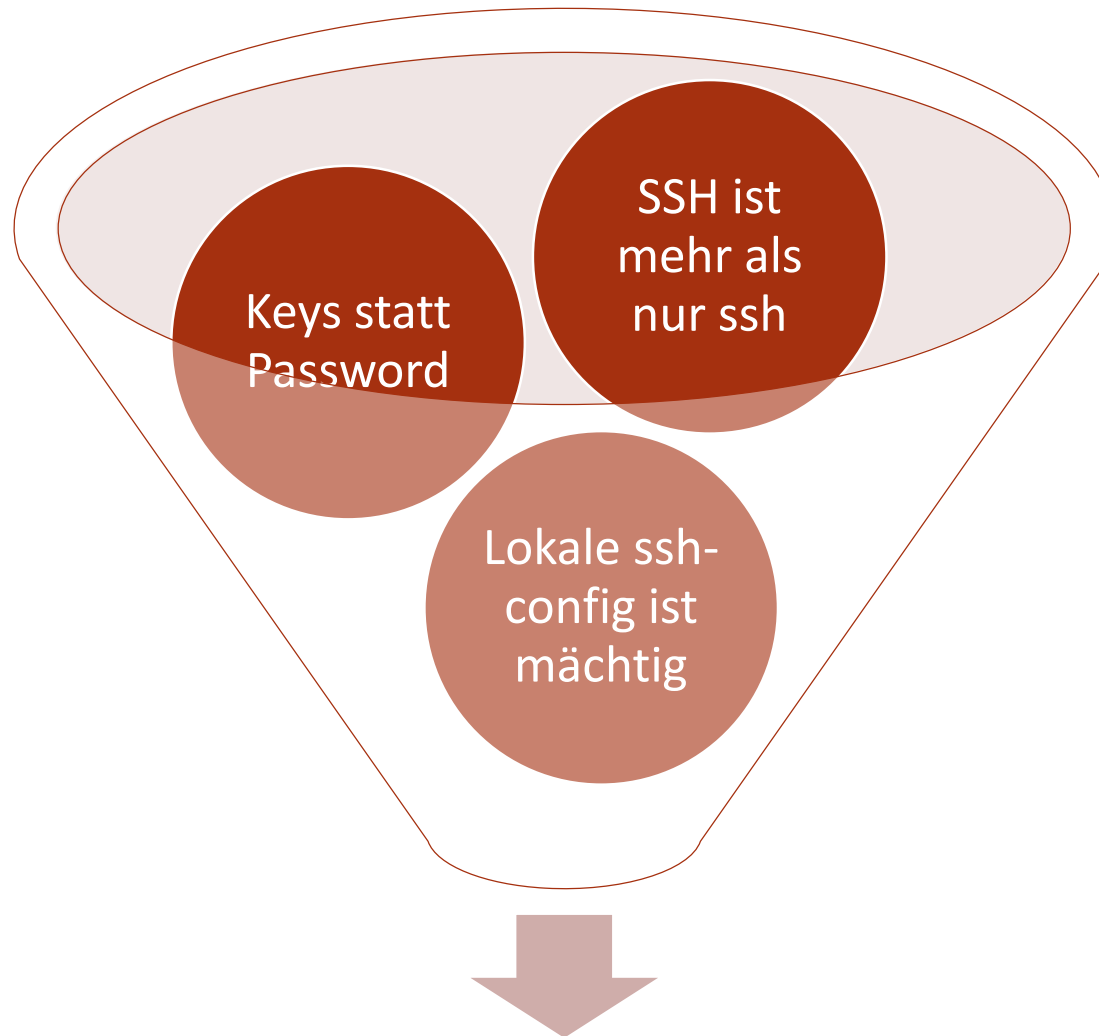


- PuTTY
- MobaXterm
- mRemoteNG
- - ...
- Bash/Linux für Windows 10
 - PowerShell/Win32-OpenSSH von MS
 - Client und Server

Windows



Fazit



Viel Spaß beim Ausprobieren!



Herzlichen Dank für Ihre Aufmerksamkeit !

we make the difference
www.its-people.de

Fragen ?



its-people GmbH

Frankfurt
Hamburg
Köln
München

Tel. 069 2475 2100
Tel. 040 2360 8808
Tel. 0221 1602 5204
Tel. 089 5484 2401

its-people ERP Beratungsgesellschaft mbH

Frankfurt

Tel. 069 2475 1980

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