SSH Zugang zur Oracle Cloud

ORACLE

Germany Customer Success

Autor: Georg Völl

Inhaltsverzeichnis

Bilderverzeichnis

1 MANAGEMENT SUMMARY

Der administrative Zugang zur Oracle Cloud geschieht über ein Web-Interface bei dem Sie sich per Username und Passwort anmelden. Möchten Sie auf eine VM in der OPC zugreifen (z.B. eine DBaaS-Instanz), geschieht dies über „ssh“ und einem Public- und Private-Key-Pair.

In dieser Anleitung möchten wir Ihnen zeigen, wie ein Key-Pair im OpenSSH Format generieren, welches Sie anschließend nutzen können, um sich per ssh an einer Virtual Machine (VM) in der Oracle Cloud anmelden zu können. Den Public-Key laden Sie in die Cloud hoch und den Private-Key sichern Sie vor unerlaubten Zugriff lokal.

Als Voraussetzung zur Nutzung von „ssh“ muss der Port 22 in Ihrer Firmen-Firewall offen sein. Fragen Sie dafür bei Ihrem Firewall-Admin nach. Ein erstes Indiz, ob der Port offen ist, kann Ihnen das Tool „telnet“ liefern (unter Windows muss dieses Tool eventuell erst von Ihnen freigeschaltet werden). Probieren Sie aus, ob Sie mit diesem öffentlichen Server (kein Oracle Cloud relevanter Server) über Port 22 eine Verbindung aufbauen können:

```
telnet 217.160.122.230 22
```

Als Antwort sollte eine Zeile mit „Connected to kundenserver.de“ oder „Accepted“ erscheinen. Wenn dies nicht der Fall ist, wird Port 22 wahrscheinlich durch eine Firewall geblockt. Als Antwort erhalten Sie dann „Connection refused“ oder „Timeout“. Sie können „telnet“ mit <CTRL-C> abbrechen. Wenn eine Firewall den Port blockiert, benötigen Hilfe durch Ihren Firewall-Admin, der den Port 22 dann entweder generell öffnet oder für bestimmte IPs freigibt. Diese IP-Adressen (die öffentlichen IPs der VMs auf die Sie zugreifen möchten) müssen Sie ihm dann nennen. Eine Hilfe hierzu erhalten Sie in dem Link in der Zusammenfassung.

Die jeweils aktuellste Version dieses Dokumentes kann hier herunter geladen werden:

https://standby.cloud/download/pdf/ssh-german.pdf

2 GENERIEREN DES KEY-PAIRS

2.1 Windows

Unter Windows benötigen Sie das Tool „PuTTYgen“ um das Schlüsselpaar zu erzeugen.

Download Link für PuTTY und PuTTYgen:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Nach der Installation führen Sie das Tool PuTTYgen aus. In dem erscheinenden Fenster prüfen Sie, ob die Standard-Einstellungen „Type of key to generate“ auf „SSH-2 RSA“ und die Bit-Länge des Schlüssels mindestens 2048 betragen.

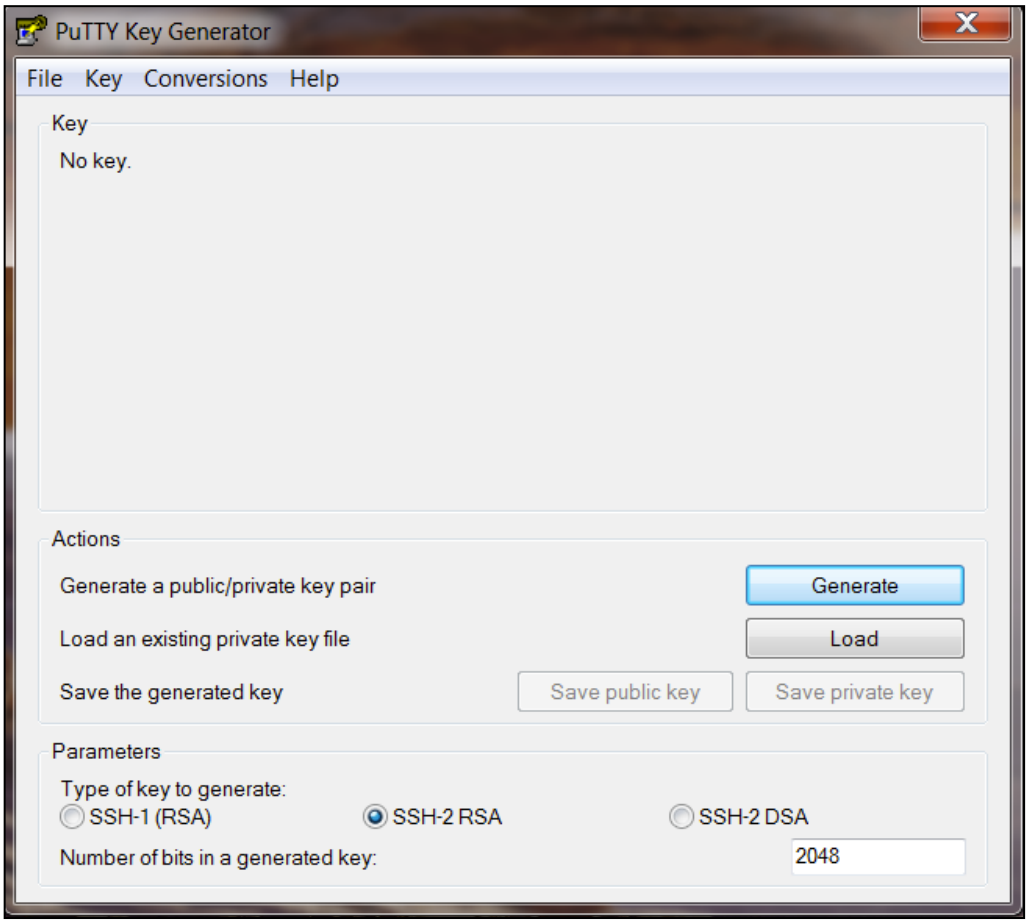

Abbildung 1: PuTTYgen Startfenster

Wenn die Einstellungen passen, klicken Sie auf den „Generate“ Button. Bewegen Sie dann die Maus solange über das Fenster, bis genügend Zufallszahlen generiert wurden.

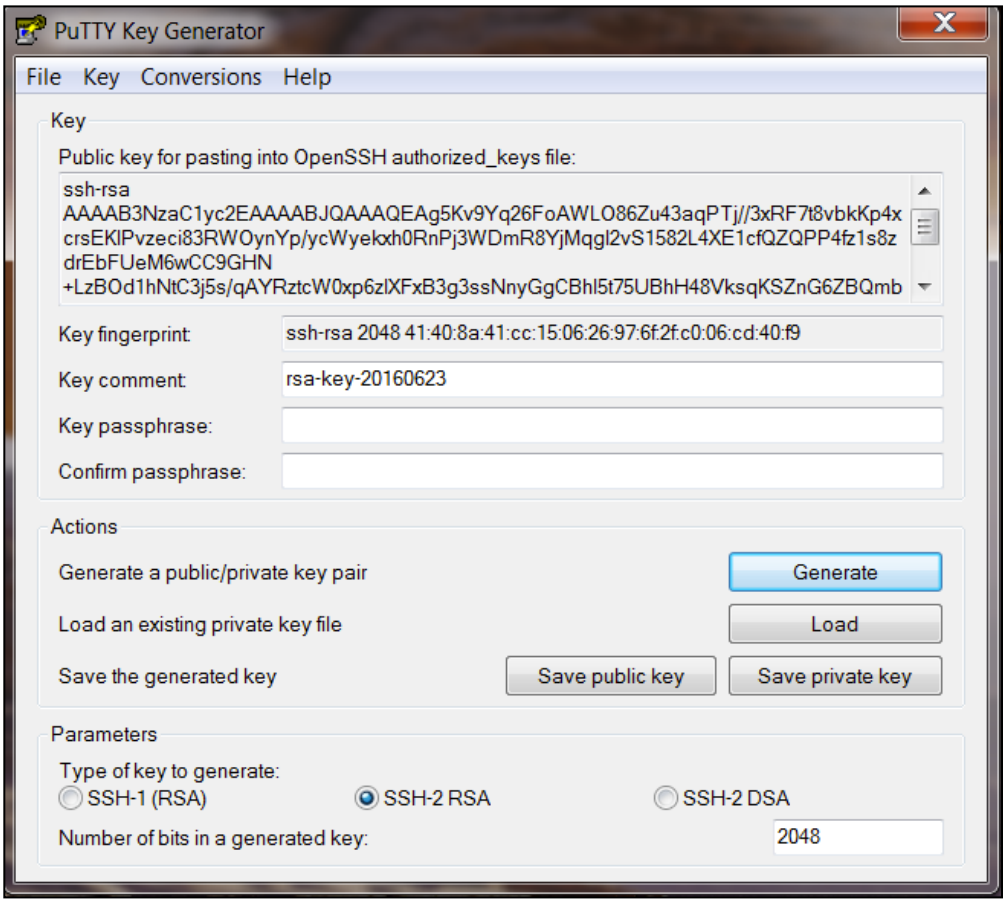

Abbildung 2: PuTTYgen Ergebnis

Im Feld „Key comment“ können Sie eine Beschreibung für den Key hinterlegen z.B. „OraCloudKey“. Optional können Sie im Feld „Key passphrase“ ein Kennwort hinterlegen, das Ihren privaten Schlüssel vor unerlaubtem Zugriff schützt, falls er in falsche Hände gerät. Dies wird von uns empfohlen. Bestätigen Sie das Kennwort im nächsten Feld und sichern anschließend die ezeugten Schlüssel:

- Öffnen Sie eine Textdatei, die Sie z.B. „OraCloud-Pub-OpenSSH.txt“ nennen und kopieren Sie den kompletten Inhalt aus dem Textfenster (beginnt mit „ssh-rsa“) in die Textdatei (dies ist der Public Key, der in die OPC geladen wird).

- Speichern Sie dann den Private-Key für die Nutzung mit PuTTY (anderes Format als OpenSSH). Betätigen Sie den „Save private key“ Button und speichern Sie den Key z.B. unter dem Namen „OraCloud-Priv.ppk“.

- Optional: Damit Sie auch von einem Unix / Linux aus auf die OPC zugreifen können, sichern Sie den OpenSSH Private-Key, in dem Sie im Menü unter „Conversions“ den Eintrag „Export OpenSSH key“ ausführen (dies ist der Private-Key für Unix) und sichern Sie ihn z.B. unter „OraCloud-Priv-OpenSSH“. Diesen privaten Schlüssel können Sie dann auf eine Unix-Maschine kopieren. Dort sollte er mit „chmod 600 OraCloud-Priv-OpenSSH“ vor unerlaubtem Zugriff geschützt werden.

2.1.1 Umwandeln eines OpenSSH Private Keys

Sie können einen OpenSSH Private Key (der z.B. in der OPC für Sie generiert wurde oder der mit Unix / Linux ssh-keygen - wie im nächsten Kapitel beschrieben - generiert wurde) mit dem Tool „PuTTYgen“ umwandeln, damit Sie ihn mit PuTTy verwenden können.

Starten Sie hierfür wieder PuTTYgen und drücken den „Load“ Button und laden den private key. Nach der Eingabe der Passphrase, sehen Sie das folgende Ergebnis:

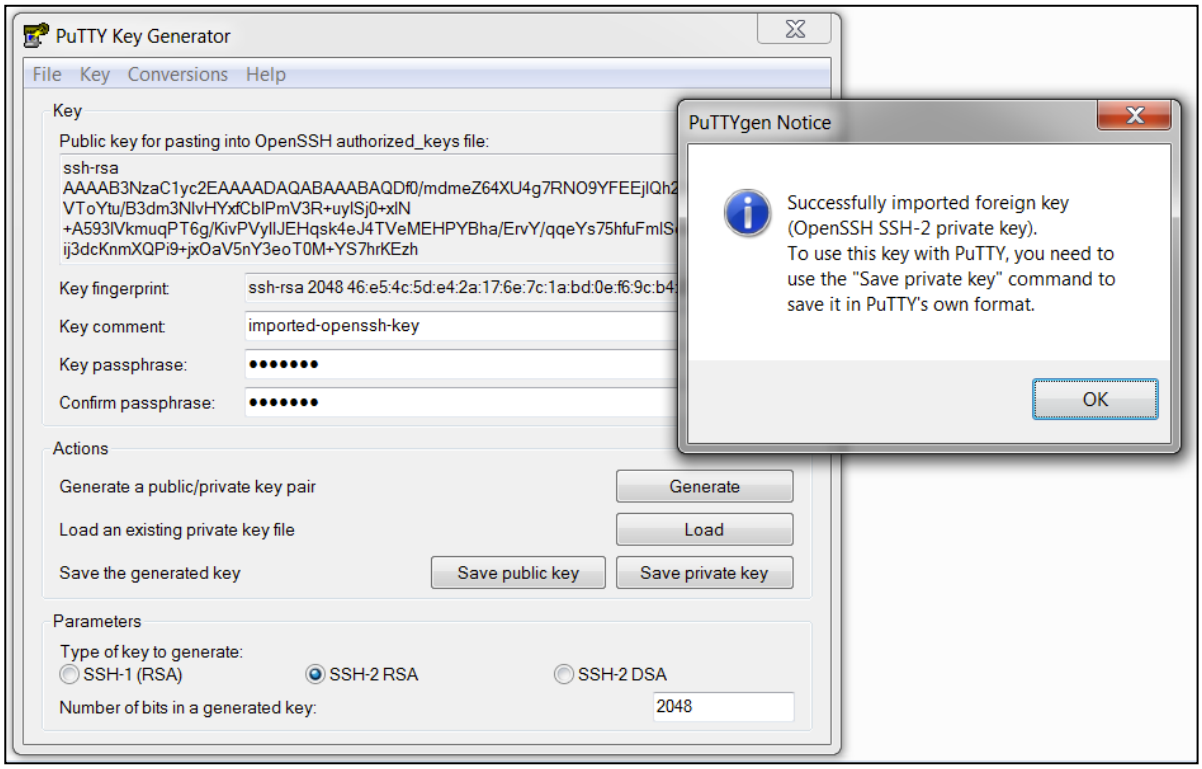

Abbildung 3: PuTTYgen Key konvertieren

Nach erfolgreichem Import, können Sie im „Key comment“ Feld noch einen sinnvolleren Namen als „imported-openssh-key“ eingeben. Drücken Sie anschließend den „Save private key“ Button und speichern Sie ihn mit der Endung „.ppk“.

2.2 Unix / Linux

Geben Sie in einem Terminalfenster das folgende Kommando ein:

```
ssh-keygen -t rsa -b 2048 -C OraCloudKey -f OraCloud
```

Der Parameter „-C“ ist optional: Sie können hier einen Kommentar abgeben z.B. auch für wen der Schlüssel sein soll (Beispiel: opc@compute1). Sie werden bei der Erstellung des Schlüsselpaares nach einer Passphrase gefragt. Geben Sie 2mal Return ein, bleibt die Passphrase leer. Mit diesem Kommando werden zwei Dateien erzeugt: „OraCloud“ (dies ist der Private Key) und „OraCloud.pub“ (dies ist der Public-Key zum Hochladen in die OPC). Wenn es Sie stört, dass der Private Key keine Endung hat, können Sie ein „.pem“ als Endung anhängen:

```
mv OraCloud OraCloud.pem
```

Mit dem Private Key melden Sie sich an der VM an – dies zeigen wir Ihnen im nächsten Kapitel.

3 SSH ZUGANG

Erstellen Sie bitte erst eine VM in der Oracle Cloud bevor Sie hier weiterlesen. Sie benötigen eine öffentliche IP Adresse, die Ihnen erst nach Erstellung der VM bekannt ist. Für eine VM unter IaaS (Oracle Compute Cloud Service) können Sie auch vorher eine öffentliche IP reservieren, die dann von der VM genutzt werden kann. Wenn Sie eine PaaS Instanz (z.B. DBaaS Instanz) einrichten möchten, kann diese reservierte öffentliche IP aber nicht genutzt werden. Die PaaS-Dienste bieten eigene Möglichkeiten eine IP zu reservieren.

Wir nutzen einen SSH Zugang und verwenden den Standard-User „opc“. Dieser User wird immer eingerichtet und kann per „sudo“ bzw. „sudo su - root“ als Root Administrator arbeiten.

3.1 Windows

Unter Windows benötigen Sie das Tool „PuTTY “ um einen SSH Zugang auf die VM in der Oracle Cloud herzustellen.

Download Link für PuTTY und PuTTYgen:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Installieren Sie PuTTY und führen es aus.

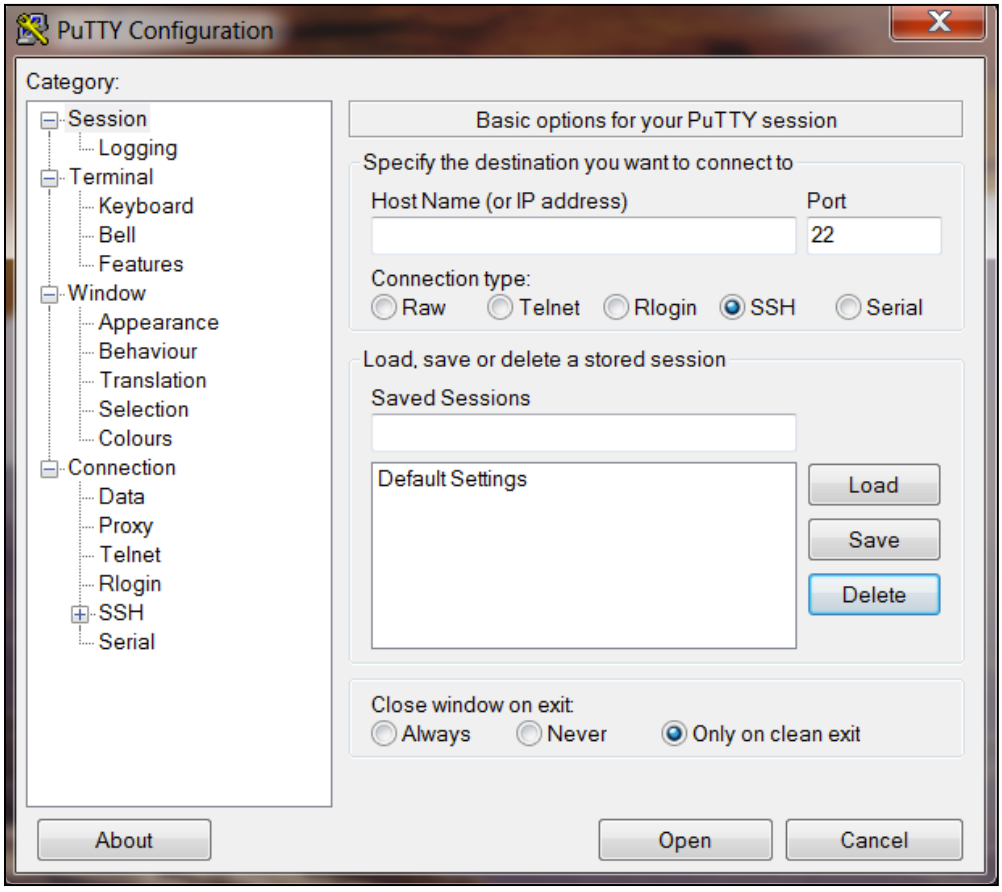

Abbildung 4: PuTTY

Tragen Sie im Feld „Host Name (or IP address)“ die öffentliche IP Adresse Ihrer VM ein. Im linken Menü-Baum klicken Sie auf „Data“ und tragen im Feld „Auto-login username“ den User „opc“ ein.

Klicken Sie dann wieder im linken Menü-Baum auf das Plus-Icon neben „SSH“. Klicken Sie auf „Auth“ und dann auf den Browse-Button um den Private-Key für PuTTY (z.B. OraCloud-Priv.ppk“) zu laden, den Sie im vorherigen Kapitel erstellt haben. Zum Schluss klicken Sie wieder auf den ersten Menü-Punkt im Baum „Session“, geben bei „Saved Sessions“ z.B. den Namen „Oracle Cloud“ ein und klicken den Button „Save“. Ihre Einstellungen werden dadurch gesichert.

Zum Testen der Verbindung drücken Sie den „Open“ Button. Es öffnet sich ein Terminalfenster, in dem Sie erst nach der Passphrase für Ihren Private-Key gefragt werden. Wenn Sie sich das erste Mal an Ihrer VM anmelden, werden Sie gefragt, ob Sie die Verbindung wirklich nutzen wollen (Host ist nicht bekannt - RSA Fingerprint wird danach gespeichert und diese Anfrage kommt nicht mehr). Antworten Sie hier mit „yes“.

Danach können Sie beliebige Kommandos absetzen.

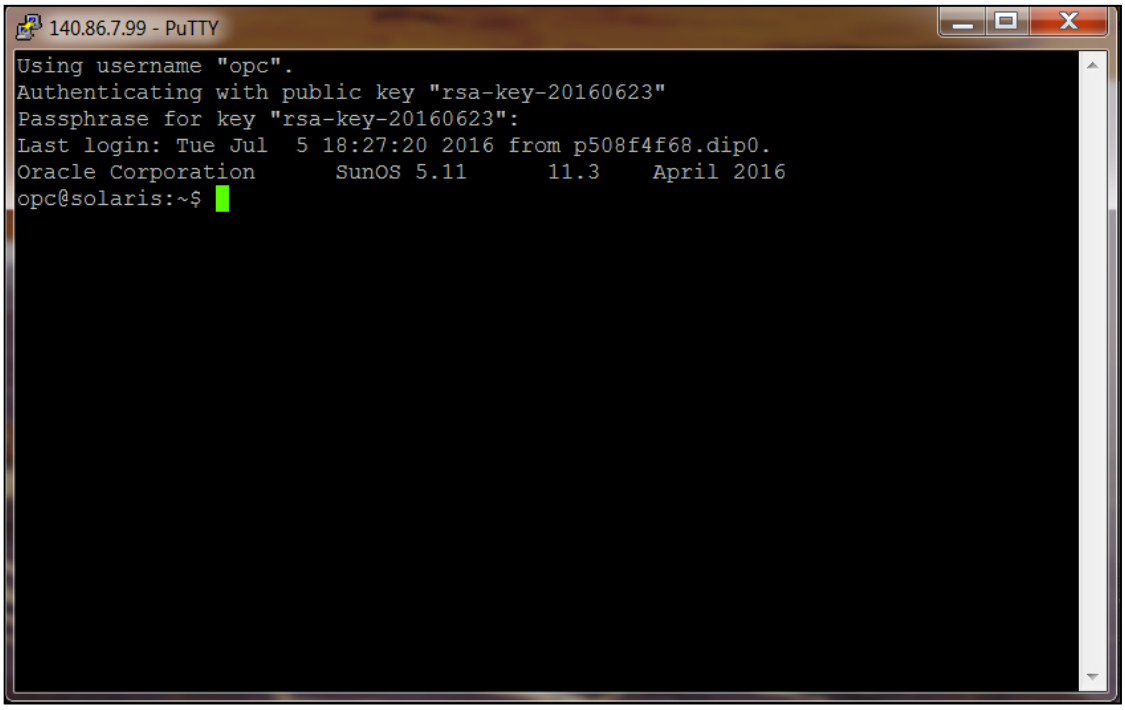

Abbildung 5: PuTTY Terminalfenster

Sie beenden die Terminal-Session, in dem Sie das Kommando „exit“ eingeben.

3.1.1 Ports tunneln mit PuTTY

Falls Sie auf einen Port zugreifen wollen, der in Ihrer Firmen-Firewall geblockt ist (gilt nicht für den SSH-Port 22 – der muss unbedingt offen sein), dann können Sie diesen über SSH mit Hilfe von PuTTY tunneln. Führen Sie alle Schritte der Konfiguration in PuTTY wie oben beschrieben durch und gehen dann zusätzlich auf das Feld „Connection->SSH->Tunnels“.

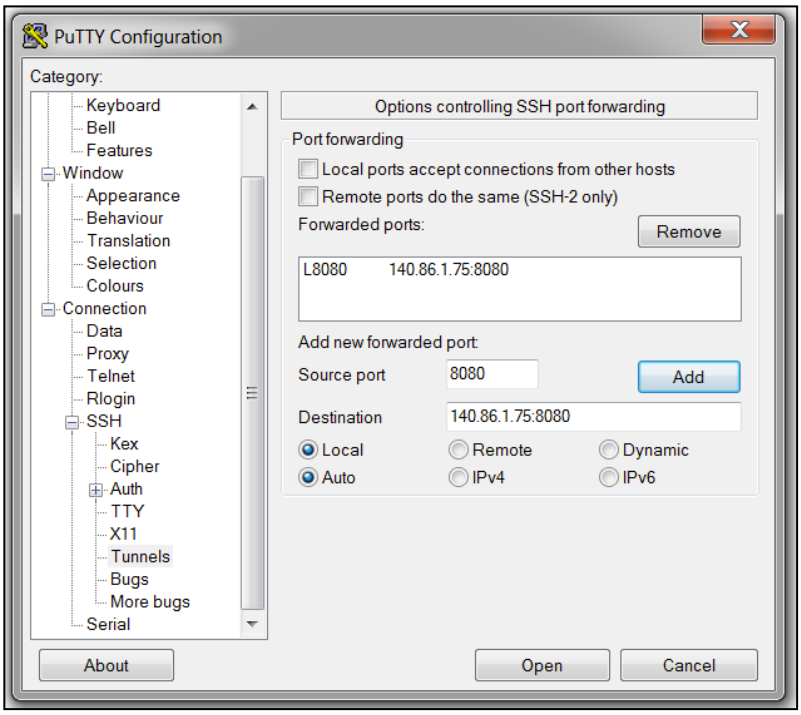

Abbildung 6: PuTTY SSH Port forwarding

Geben Sie bei „Source port“ den Port ein, den Sie tunneln möchten (z.B. 5500 für die Enterprise Manager DB Express Konsole“) und geben Sie bei Destination die IP Ihrer VM gefolgt von einem Doppelpunkt und dem gleichen Port ein. Drücken Sie anschließend den „Add“ Button und wiederholen Sie diesen Schritt ggf. für weitere Ports. Einige weitere Beispiele wären z.B. Port 8080 für Glassfish und Port 4848 für die Glashfish Admin Konsole.

Wenn die Verbindung mit PuTTY geöffnet ist, können Sie jetzt mit einem lokalen Browser diesen Port mit „localhost:<port>“ erreichen.

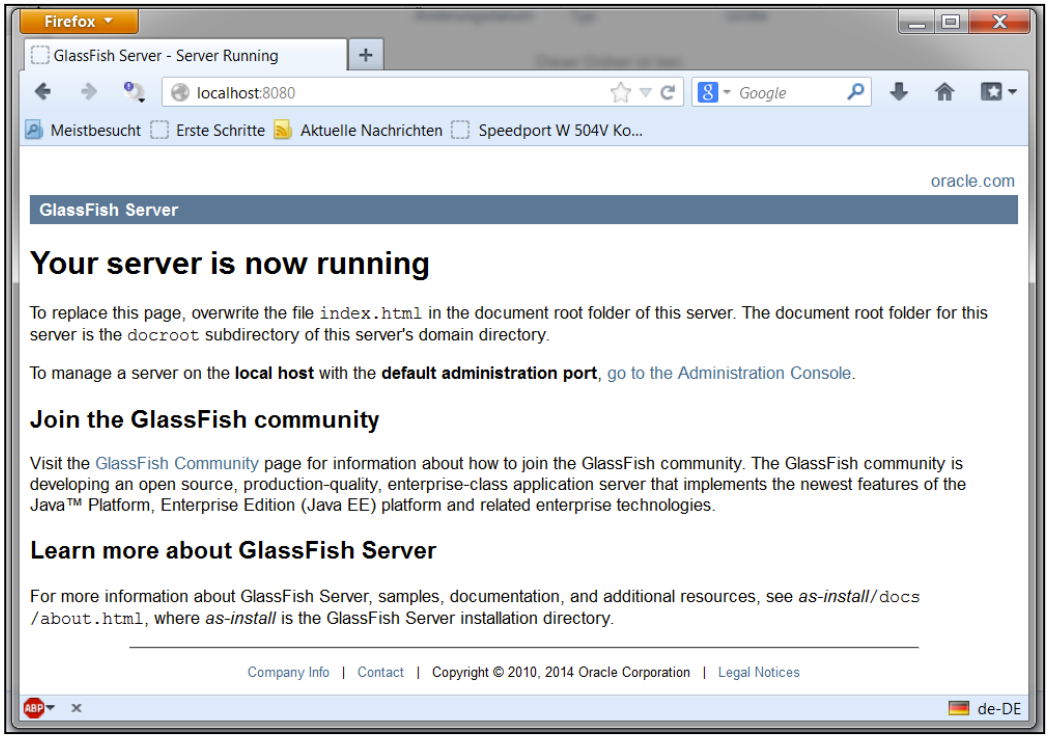

Abbildung 7: Localhost Port forwarding mit Firefox

3.2 Unix / Linux

Unter Unix rufen Sie im Terminalfenster das Kommando „ssh“ mit diesen Parametern auf:

ssh -X -i <PfadZumKey>/<IhrPrivateKey> opc@<IPderVM>

Der optionale Parameter „-X“ ermöglicht den Aufruf von X11 Fenstern auf der VM. Lassen Sie die Option weg, wenn Sie kein X11 benötigen.

Der private key muss mit „chmod“ (z.B. chmod 600 OraCloud-Priv-OpenSSH) vor unerlaubtem Zugriff geschützt sein. SSH verweigert sonst eine Nutzung.

Ersetzten Sie bitte vorher „<IPderVM>“ mit der öffentlichen IP Ihrer VM und geben bei Bedarf den Pfad zu Ihrem Private-Key mit an.

Wenn Sie sich das erste Mal an Ihrer VM anmelden, werden Sie gefragt, ob Sie die Verbindung wirklich nutzen wollen (Host ist nicht bekannt - RSA Fingerprint wird danach gespeichert und diese Anfrage kommt nicht mehr). Antworten Sie hier mit „yes“. Der Fingerprint der VM wird in der Datei „known_hosts“ im Verzeichnis „.ssh“ im User Home Verzeichnis gespeichert. Falls Sie bei Tests die gleiche IP mit anderen VMs erneut benutzen sollten, erkennt dies „ssh“ und vermutet einen Angriff. Löschen Sie dann den Fingerprint in der Datei.

Danach können Sie beliebige Kommandos absetzen.

```
The authenticity of host '140.86.8.16 (140.86.8.16)' can't be established.
RSA key fingerprint is 27:be:91:df:ca:1b:b3:b0:1d:17:37:4d:0e:ff:0a:a5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '140.86.8.16' (RSA) to the list of known hosts.
Oracle Corporation      SunOS 5.11      11.3    December 2015
opc@solaris:~$ pwd
/export/home/opc
opc@solaris:~$ exit
Abgemeldet
Connection to 140.86.8.16 closed.
```

Abbildung 8: Terminalfenster unter Unix

Sie beenden die Connection, in dem Sie das Kommando „exit“ eingeben.

3.2.1 Ports tunneln mit SSH

Wenn Sie ein Port-Forwarding mit „ssh“ durchführen wollen (damit in der Firmen-Firewall nicht zusätzlich zu ssh (Port 22) weitere Ports offen sein müssen), dann können Sie dies mit der Option –L vornehmen (Local Port Forwarding). Geben Sie z.B. das folgende Kommando ein, damit Sie mit Ihrem lokalen Browser bei Eingabe der URL „localhost:8080“ zur Default Seite von Glassfish kommen:

ssh -X -i <PfadZumKey>/<IhrPrivateKey> –L 8080:<IPderVM>:8080 opc@<IPderVM>

Natürlich muss ein Glassfish AppServer auf Ihrer VM laufen, damit Sie dies testen können. Die URL „localhost:<Port>“ funktioniert nur solange die SSH Verbindung besteht.

4 DATEIEN TRANSFERIEREN

Erstellen Sie bitte erst eine VM in der Oracle Cloud bevor Sie hier weiterlesen. Sie benötigen eine öffentliche IP Adresse, die Ihnen erst nach Erstellung der VM bekannt ist.

4.1 Windows

Unter Windows benötigen Sie das Tool „WinSCP“ um bequem Dateien zwischen Ihrer lokalen Maschine und der VM in der Oracle Cloud transferieren zu können.

Download Link für WinSCP:

https://winscp.net/eng/docs/lang:de

Installieren Sie WinSCP und führen es aus. Sie werden gefragt, ob Sie gespeicherte Verbindungen aus PuTTY importieren möchten – das erspart Ihnen die erneute Eingabe der Verbindungsdaten.

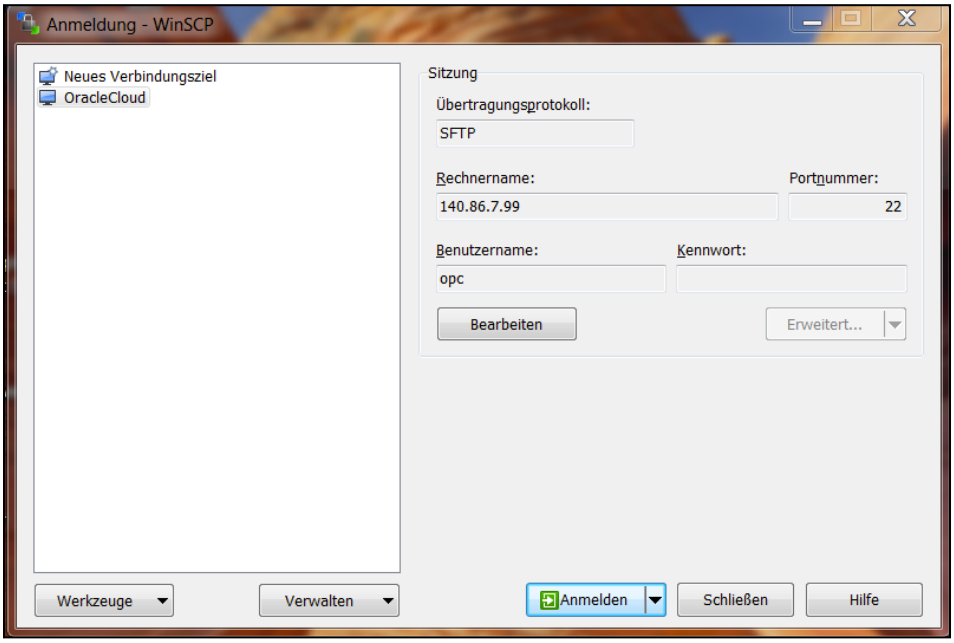

Abbildung 9: Anmeldung WinSCP

Klicken Sie auf den „Anmelden“ Button – danach werden Sie wieder nach der Passphrase gefragt.

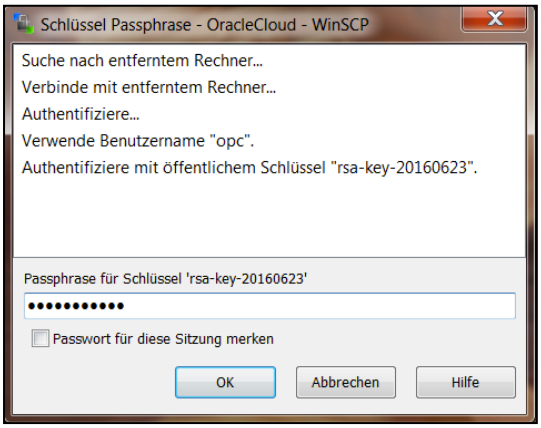

Abbildung 10: Passphrase Abfrage

Danach erhalten Sie in zwei Fenstern eine Auflistung Ihrer Dateien – im linken Fenster die lokalen Dateien und im rechten Fenster Ihre Dateien in der VM.

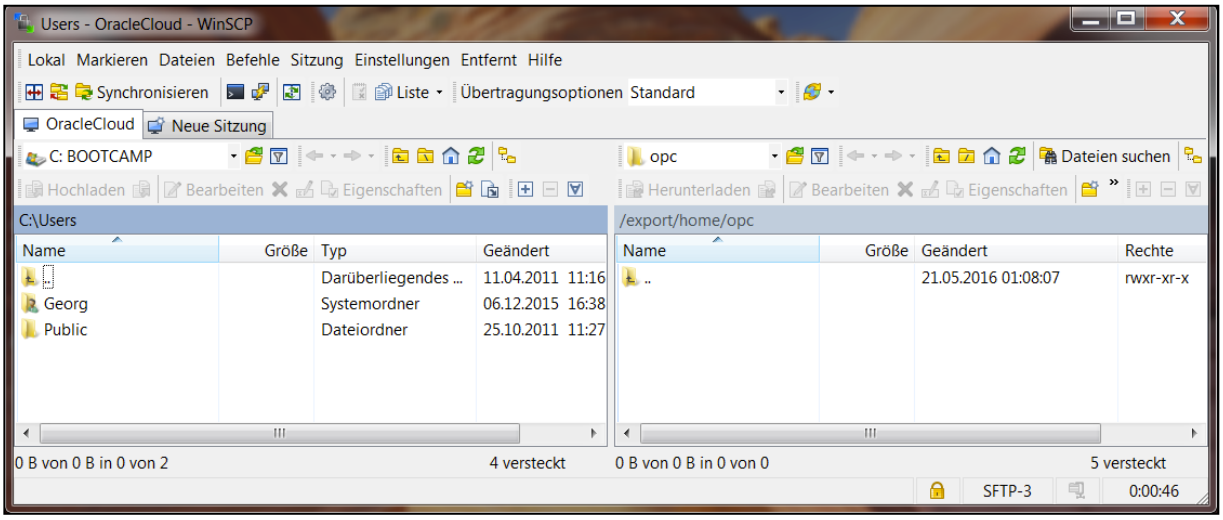

Abbildung 11: WinSCP

4.2 Unix / Linux

Unter Unix nutzen Sie das Tool „scp“ zum Transferieren der Dateien. Mit dem Parameter „-i“ geben Sie wieder Ihren Private-Key (evtl. mit Pfad) an. Wenn Sie Dateien in die Cloud hochladen wollen, geben Sie erst die hochzuladende Datei (z.B. workfiles.tar.gz) an, dann Username (opc) gefolgt von einem Klammeraffen und der öffentlichen IP der VM und dann mit einem Doppelpunkt getrennt das Zielverzeichnis in das die Datei kopiert werden soll.

```
scp -i OraCloud-Priv-OpenSSH.txt workfiles.tar.gz opc@140.86.6.8:/export/home/opc
```

Mit dem obigen Kommando kopieren Sie die Datei „workfile.tar.gz“ aus dem aktuellen lokalen Verzeichnis in die VM mit der IP 140.86.6.8 in der Cloud in das Home-Verzeichnis des Users OPC. Wenn Sie die letzten beiden Parameter verdrehen, kopieren Sie Dateien aus der Cloud nach Lokal:

```
scp -i OraCloud-Priv-OpenSSH.txt opc@140.86.6.8:/export/home/opc/workfiles.tar.gz .
```

Das obige Kommando kopiert die Datei „workfiles.tar.gz“ aus dem Home-Verzeichnis des Users OPC aus der VM in der Cloud in das aktuelle lokale Verzeichnis.

5 VERWALTUNG IHRER SCHLÜSSEL

Wir empfehlen zumindest für den wichtigsten User in der Oracle Cloud (User „opc“ oder in Ravello: User „ravello“) unbedingt einen Private Key mit einer Passphrase zu nutzen. Dieser User kann Root-Rechte erlangen und ist somit der mächtigste User auf der VM. Wenn der Private Key einmal in falsche Hände geraten sollte, so steht wenigstens noch die Passphase vor der ungewollten Nutzung. Wenn Sie die Passphrase einmal ändern müssen, können Sie dies z.B. mit dem Tool „ssh-keygen“ machen:

```
ssh-keygen -p -P <AltePassphrase> -N <NeuePassphrase> -f <PrivateKeyDatei>
```

Der Public Key wird auf der VM im Home-Verzeichnis des Users im Ordner „.ssh“ in der Datei „authorized_keys“ abgelegt. Sie können hier auch mehrere Public Keys ablegen, wenn z.B. mehrere Benutzer den User „opc“ nutzen sollen. Beim Erstellen der Instanz können Sie einen oder mehrere Keys angeben. In einigen Cloud Services z.B. „Database Cloud Service“ können Public Keys auch nach dem Erstellen der Instanz mit der Web-Oberfläche hinzugefügt werden. Das Script „inject-sshkeys.sh“ (Teil von opc-init) fügt dann neue Schlüssel zu „authorized_keys“ hinzu.

Im Compute Cloud Service können Sie zur Zeit nur bei der Erstellung einer neuen VM Instanz einen oder mehrere Schlüssel angeben. Nach Erstellung können Sie mit der Web-Oberfläche die Schlüssel nicht mehr ändern. Wenn dies einmal erforderlich sein sollte, können Sie aber z.B. einen weiteren Public Key an die bestehende Datei anhängen:

```
cat <NeuerPublicKey> >> .ssh/authorized_keys
```

Sie können die Datei „authorized_keys“ auch mit einem Editor z.B. „vi“ ändern. Wir empfehlen Ihnen hier dringend äußerst vorsichtig vorzugehen. Wenn Sie einen Fehler machen, kommen Sie eventuell nicht mehr auf Ihre VM.

6 API ACCESS UNTER OCI

Wenn Sie auf das REST API der Oracle Cloud Infrastructure (OCI) zugreifen möchten, benötigen Sie einen Public Key im PEM Format. Diesen können Sie aus einem bestehenden Private Key jederzeit mit „openssl“ erzeugen:

```
openssl rsa -pubout -in <PrivateKeyDatei> -out <PublicKeyPem>
```

Falls Sie noch keinen Private Key (z.B. mit ssh-keygen) erzeugt hatten, können Sie diesen auch mit openssl erstellen:

```
openssl genrsa -out <PrivateKeyDatei> 2048
```

Dokumentation des OCI REST API:

https://docs.cloud.oracle.com/iaas/Content/API/Concepts/usingapi.htm

Auch das OCI Command Line Interface benötigt diesen Key. Dokumentation:

https://docs.cloud.oracle.com/iaas/Content/API/Concepts/cliconcepts.htm

Weitere Informationen zum Erstellen der Keys erhalten Sie hier:

https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm

7 ZUSAMMENFASSUNG

Wir zeigten Ihnen, wie Sie das Schlüsselpaar zum Zugriff auf eine VM in der Oracle Cloud erzeugen können, wie Sie auf die VM Zugriff erlangen um dort Kommandos auszuführen und wie Sie Dateien transferieren.

Einen simplen Key-Generator können Sie hier finden:

http://ssh-keygen.voell.de/

Dort können Sie alle benötigten Keys per Web-Interface erstellen.

Zusätzliche Infos zu SSH und dem Zugriff auf eine VM in der Oracle Cloud:

https://apex.oracle.com/pls/apex/cmuetzli_de/r/47279/files/static/v58/02_Workshop-Prereq_SSH-Guide_v1.5_DE.pdf

Weitere Informationen zum Zugriff auf VMs bzw. Instanzen in der Cloud erhalten Sie im Handbuch zu den Oracle Public Cloud Services:

Using Oracle Compute Cloud Service (IaaS)

https://docs.oracle.com/cloud/latest/stcomputecs/STCSG/toc.htm

Lesen Sie hier Kapitel 2 (Enabling secure Access to Instances Using SSH) und ggf. Kapitel 8 und 9.

Infos zum Öffnen von Ports in der Firewall

https://docs.oracle.com/cloud/latest/stcomputecs/STCSG/GUID-DE568AAF-39CE-462C-B605-B96AE4036825.htm

Network Access (SSH Key Pair)

https://docs.oracle.com/en/cloud/paas/database-dbaas-cloud/csdbi/manage-network-access.html

SSH Tunnel

https://docs.oracle.com/en/cloud/paas/database-dbaas-cloud/csdbi/create-ssh-tunnel.html