ORACLE

Protecting Database Cloud Services with Bastion Service

Business challenge

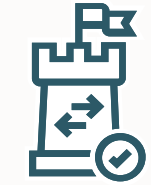
In the shared responsibility model of PaaS Services like Database Cloud Service, DBCS, or Exadata Cloud Services, ExaCS, the service consumers are granted OS access, and have some responsibilities requiring access to the Linux OS, as user oracle or with group membership equal to the oracle user.

The services is created with the opc account, authenticated with a private/public ssh keypair. User opc is configured to offer sudo root.

From a governance perspective, organizations is required to enforce the usage of named users, and not common accounts Linux like opc or oracle, for the purpose of accountability and auditability

Central governance, with central user CRUD, is the preferred opting, avoiding fragmented user management

Oracle Cloud Infrastructure, Bastion Service



- Provides restricted and time-limited secure access to resources that don't have public endpoints and require strict resource access controls
- With Oracle Cloud Infrastructure (OCI) Bastion service, customers can enable access to private hosts without deploying and maintaining a jump host.
- Gaining improved security posture with identity-based permissions and a centralized, audited, and time-bound SSH session
- Oracle OCI Bastion Service utilizes Oracle OCI IAM, removing the need for user governance eon Linux host, centralizing all user governance, RBAC access to one single instance of Oracle OCI IAM

References

- Oracle OCI Bastion Services
  https://docs.oracle.com/en-us/iaas/Content/Bastion/Concepts/bastionoverview.htm
- Oracle OCI Identity Domains
  https://docs.oracle.com/en-us/iaas/Content/Identity/getstarted/identity-domains.htm

Solution proposal I

Traditional Linux user governance

Deploy user management at Linux level

DBCS and ExaCS runs on Oracle Enterprise Linux, OEL, supporting standard Linux user management/user governance

From a Linux perspective the following will partly support the common requirements:

- Don’t share the opc private key, no one is allowed to use ssh with the opc private key.

Each user signing in to the Linux node has their own private key. The oracle account is public and

Shared oracle account

- Each user signing in to the Linux node has their own private key. The oracle account is public and the users public key are stored in ~/.ssh/authorized_keys

Individual accounts

- For each suer a personal account is created with the users public key in the users authorized keys file, or the user is authenticated via LDAP over Linux PAM
- The users Linux account is assigned to the required groups at Linux level to provide access to the oracle software owner and grid software owner

Solution proposal II

Use Oracle OCI Bastion Service

All access to DBCS or ExaCS Linux vm is tunnelled though the Bastion Services

The Bastion Service resides in a compartment, and only OCI users with access, though OCI policies, to the compartment and the bastion Service will be able to create a bastion ssh session to the linux vm.

The bastion service is configured with a private/public ssh key pair, with the public key in the authorized_keys file of the oracle user. The opc account private key is not used.

The VCN network is configured so the only permittable access over port 22 is from the private endpoint of the bastion host

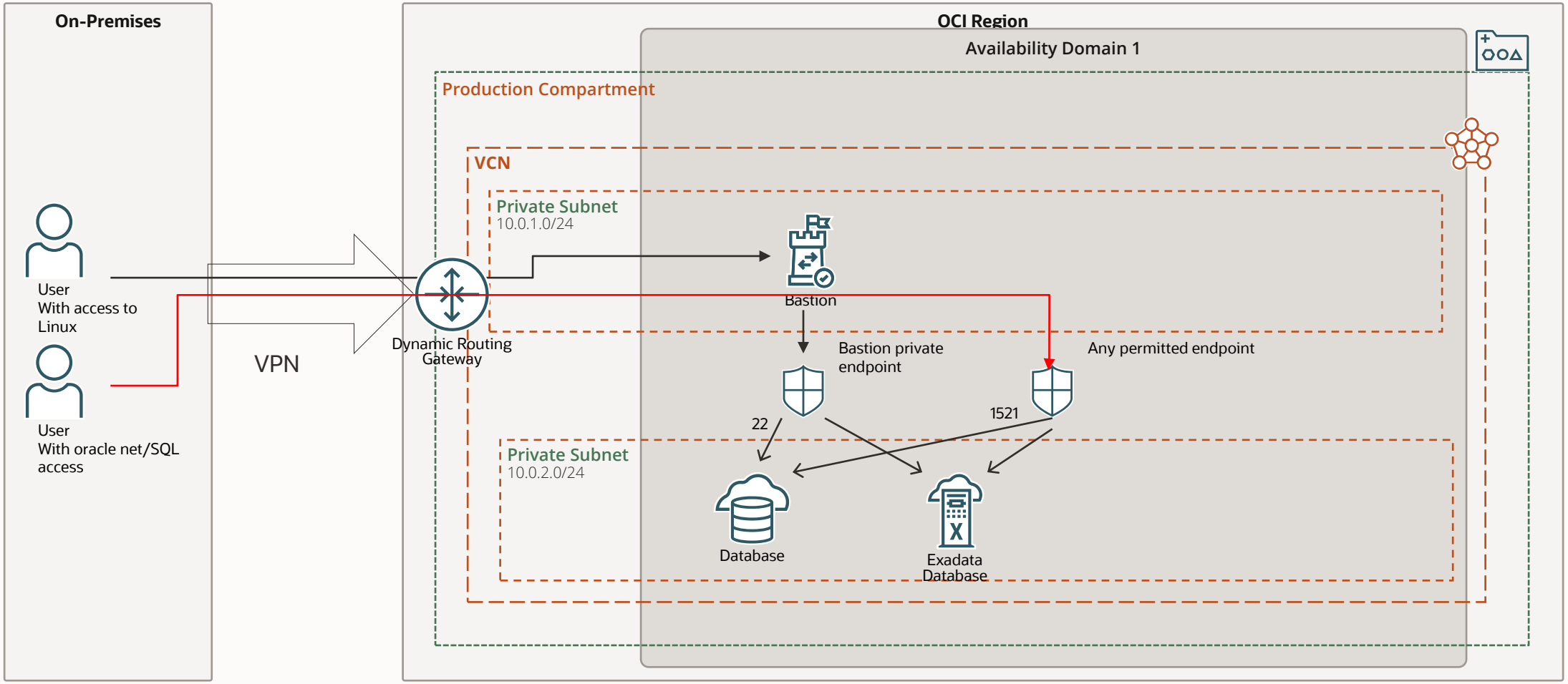
Oracle net/SQL traffic over port 1521/1522 is permitted from the private subnet

Bastion Service support two types of ssh tunnel:

- Managed SSH Session, for compute nodes with the OCI agent running
- SSH Port forwarding session, for compute nodes, like DBCS and ExaCS, whithout running OCI agent

Network configuration

Traffic flow



Traffic flow

The DBCS or ExaCS instances resided in a separate subnet, 10.0.2.0/24, and Network Security Groups, NSG, is configured for permitting ingress/egress traffic.

With a NSG, the only permitted traffic over port 22 to the DBCS instance or ExaCS instance s from the private endpoint of the Bastion Service, resides in the 10.0.1.0/24 subnet

Oracle Net traffic is configured based on the application and oracle net/SQL traffic requirements, in the example, only from the 10.0.1.0/24 subnet

Bastion Configuration and usage

Bastion Service is a two step process

- Create the Bastion Service, which created the private endpoint in the subnet
- Create a private ssh key pair pr. user that needs access. Upload the public key to ~/.ssh/authorized_keys in the oracle account on the DBCS or ExaCS server

- For each time access is needed, create a Bastion Session. The Bastion Session is valid for 3 hours, The bastion session generates a new ssh private/public key pair, used for ssh connection to the Bastion Service
- The private key for authentication of the oracle Linux account is tunnelled through the Bastion Session

Bastion Service Creation

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion?region=eu-frankfurt-1

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Search

- Home
- Compute
- Storage
- Networking
- Oracle Database
- Databases
- Analytics & AI
- Developer Services
- Identity & Security
- Observability & Management
- Hybrid
- Migration
- Billing & Cost Management
- Governance & Administration
- Marketplace

Compartments
Federation
Authentication Settings

Data Protection
Overview
Classification Results
Targets
Recipes
Settings

Responder Activity
Detector Recipes
Responder Recipes
Managed Lists
Data Masking
Settings

Security Zones
Overview
Recipes

Security Advisor

Threat Intelligence
Overview
Threat Indicator Database

Firewalls
Network Firewalls
Network Firewall Policies

Overview
Certificates
Certificate Authorities
CA Bundles

Scanning
Vulnerability Reports
Scanning Reports
Targets
Scan Recipes

Vault

Managed Access
Access Requests
Approval Templates
Resource Settings

Bastion

Compliance

Audit

Access Governance

Help
Security Overview
Security Services and Features
Security Testing Policy
Security Best Practices
Government Cloud Services
All Security Documentation
Identity and Access Management

Access Governance

List scope

Compartment

Choose a compartment

https://cloud.oracle.com/security/bastion

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion?region=eu-frankfurt-1

This account has missing or expired metadata information. Some functionality might be restricted. To resolve this issue, go to the Account Admin Tool in the Console to update the information or contact Oracle Support.

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Identity & Security

- Identity
- Data Protection
- Cloud Guard
- Security Zones
- Security Advisor
- Threat Intelligence
- Firewalls
- Web Application Firewall
- Certificates
- Scanning
- Vault
- Managed Access
- Bastion
- Compliance
- Audit
- Access Governance

List scope

Compartment

ios_no

oraemeasec (root)/Advisory/ios_no

Filters

State

Any state

Tag filters add | clear

Bastions *in* ios_no *Compartment*

Bastions let you create and manage sessions that provide authenticated users with ephemeral, timebound access to resources in the tenancy. Bastions establish secure bridge connections from preconfigured IP addresses to supported target hosts that do not have a public IP address, such as compute instances running an OpenSSH server or autonomous transaction processing databases that support SSH tunneling to an arbitrary port.

Create bastion

Name	State	Bastion type	Created
privatenet	Deleted	Standard	Mon, Oct 17, 2022, 20:25:04 UTC
iosjump	Active	Standard	Sat, Feb 26, 2022, 17:36:37 UTC

Showing 2 Items 1 of 1

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion?region=eu-frankfurt-1

This account has missing or expired metadata information. Some functionality might be restricted. To resolve this issue, go to the Account Admin Tool in the Console to update the information or contact Oracle Support.

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Identity & Security

- Identity
- Data Protection
- Cloud Guard
- Security Zones
- Security Advisor
- Threat Intelligence
- Firewalls
- Web Application Firewall
- Certificates
- Scanning
- Vault
- Managed Access
- Bastion
- Compliance
- Audit
- Access Governance

List scope

Compartment: ios_no

oraemeasec (root)/Advisory/ios_no

Filters

State: Any state

Tag filters add | clear

Bastions *in* ios_no *Compartmen*

Bastions let you create and manage sessions that provide authe
IP address, such as compute instances running an OpenSSH s

Create bastion

Name
privatenet
iosjump

Create bastion

Help

Bastion name

dbbastion

Configure networking

Target virtual Cloud network in **ios_no** (Change Compartment)

iotnet

Target subnet in **ios_no** (Change Compartment)

iotprivate

CIDR block allowlist

10.3.0.0/24 ×

Example: 11.0.0.0/24

The IP addresses or address ranges that you want to allow to connect to target resources through SSH connections created through sessions hosted by this bastion.

Show advanced options

Create bastion | Cancel

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion?region=eu-frankfurt-1

This account has missing or expired metadata information. Some functionality might be restricted. To resolve this issue, go to the Account Admin Tool in the Console to update the information or contact Oracle Support.

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Identity & Security

- Identity
- Data Protection
- Cloud Guard
- Security Zones
- Security Advisor
- Threat Intelligence
- Firewalls
- Web Application Firewall
- Certificates
- Scanning
- Vault
- Managed Access
- Bastion
- Compliance
- Audit
- Access Governance

List scope

Compartment

ios_no

oraemeasec (root)/Advisory/ios_no

Filters

State

Any state

Tag filters add | clear

Bastions *in* ios_no *Compartment*

Bastions let you create and manage sessions that provide authenticated users with ephemeral, timebound access to resources in the tenancy. Bastions establish secure bridge connections from preconfigured IP addresses to supported target hosts that do not have a public IP address, such as compute instances running an OpenSSH server or autonomous transaction processing databases that support SSH tunneling to an arbitrary port.

Create bastion

Name	State	Bastion type	Created
dbbastion	Active	Standard	Tue, Oct 25, 2022, 10:43:03 UTC
privatenet	Deleted	Standard	Mon, Oct 17, 2022, 20:25:04 UTC
iosjump	Active	Standard	Sat, Feb 26, 2022, 17:36:37 UTC

Showing 3 Items 1 of 1

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion/bastions/ocid1.bastion.oc1.eu-frankfurt-1.amaaaaaaupfargiaagg2k5ndzglenayjaxqryrusuawkjqhgocrhvxbuphaa?region=eu-frankfurt-1

This account has missing or expired metadata information. Some functionality might be restricted. To resolve this issue, go to the Account Admin Tool in the Console to update the information or contact Oracle Support.

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Security » Bastion » dbbastion

B

ACTIVE

dbbastion

Edit | Add tags | Move resource | Delete bastion

Bastion information | Tags

OCID: ...buphaa Show Copy

Created: Tue, Oct 25, 2022, 10:43:03 UTC

Target virtual Cloud network:

Target subnet:

Maximum session time-to-live (TTL): 3 hours, 00 minutes

CIDR block allowlist: 10.3.0.0/24

Compartment: oraemeasec (root)/Advisory/ios_no

Private endpoint IP address: 10.3.4.100

Bastion type: Standard

Resources

Sessions

Metrics

Filters

State

All

Sessions

Create session

Name	Session type	Target resource	Target port	Username	State	Session TTL	Started
Loading							

Showing 0 Items 1 of 1

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion?region=eu-frankfurt-1

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Identity & Security

- Identity
- Data Protection
- Cloud Guard
- Security Zones
- Security Advisor
- Threat Intelligence
- Firewalls
- Web Application Firewall
- Certificates
- Scanning
- Vault
- Managed Access
- Bastion
- Compliance
- Audit
- Access Governance

List scope

Compartment

ios_no

oraemeasec (root)/Advisory/ios_no

Filters

Bastions *in* ios_no *Compartment*

Bastions let you create and manage sessions that provide authenticated users with ephemeral, timebound access to resources in the tenancy. Bastions establish secure bridge connections from preconfigured IP addresses to supported target hosts that do not have a public IP address, such as compute instances running an OpenSSH server or autonomous transaction processing databases that support SSH tunneling to an arbitrary port.

Create bastion

Name	State	Bastion type	Created
dbbastion	Active	Standard	Tue, Oct 25, 2022, 10:43:03 UTC
privatenet	Deleted	Standard	Mon, Oct 17, 2022, 20:25:04 UTC
iosjump	Active	Standard	Sat, Feb 26, 2022, 17:36:37 UTC

Showing 3 Items 1 of 1

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion/bastions/ocid1.bastion.oc1.eu-frankfurt-1.amaaaaaaupfargiaagg2k5ndzglenayjaxqryrusuawkjqhgocrhvxbuphaa?region=eu-frankfurt-1

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Security » Bastion » dbbastion

B

ACTIVE

dbbastion

Edit | Add tags | Move resource | Delete bastion

Bastion information | Tags

OCID: ...buphaa Show Copy

Created: Tue, Oct 25, 2022, 10:43:03 UTC

Target virtual Cloud network: iotnet

Target subnet: iotprivate

Maximum session time-to-live (TTL): 3 hours, 00 minutes

CIDR block allowlist: 10.3.0.0/24

Compartment: oraemeasec (root)/Advisory/ios_no

Private endpoint IP address: 10.3.4.100

Bastion type: Standard

Resources

Sessions

Metrics

Filters

State

All

Sessions

Create session

Name	Session type	Target resource	Target port	Username	State	Session TTL	Started
No items found.							

Showing 0 Items 1 of 1

Terms of Use and Privacy Cookie Preferences

T
B

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion/bastions/ocid1.bastion.oc1.eu-frankfurt-1.amaaaaaaupfargiaagg2k5ndzglenayjaxqryrusuawkjqhgo...

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Security » Bastion » dbbastion

B

ACTIVE

dbbastion

Edit | Add tags | Move resource | Delete bastion

Bastion information | Tags

OCID: ...buphaa Show Copy

Created: Tue, Oct 25, 2022, 10:43:03 UTC

Target virtual Cloud network: iotnet

Target subnet: iotprivate

Maximum session time-to-live (TTL): 3 hours, 00 minutes

CIDR block allowlist: 10.3.0.0/24

Compartment: oraemeasec (root)/Advisory/ios_no

Private endpoint IP address: 10.3.4.100

Bastion type: Standard

Resources

Sessions

Metrics

Filters

State

All

Sessions

Create session

Name	Session type	Target resource	Target port	Username	State	Session TTL	Started
No items found.							

Showing 0 Items 1 of 1

Bastion Session Creation

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion/bastions/ocid1.bastion.oc1.eu-frankfurt-1.amaaaaaaupfargiaagg2k5ndzglenayjaxqryrusuawkjqhgocrhvxbuphaa?region=eu-frankf...

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Security » Bastion » dbbastion

B

ACTIVE

dbbastion

Edit | Add tags | Move resource | Delete bastion

Bastion information | Tags

OCID: ...buphaa Show Copy

Created: Tue, Oct 25, 2022, 10:43:03 UTC

Target virtual Cloud network: iotnet

Target subnet: iotprivate

Maximum session time-to-live (TTL): 3 hours, 00 minutes

CIDR block allowlist: 10.3.0.0/24

Compartment: oraemeasec (root)/Advisory/ios_no

Private endpoint IP address: 10.3.4.100

Bastion type: Standard

Resources

Sessions

Metrics

Filters

State

All

Sessions

Create session

Name	Session type	Target resource	Target port	Username	State	Session TTL	Started
No items found.							

Showing 0 Items 1 of 1

Terms of Use and Privacy Cookie Preferences

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion/bastions/ocid1.bastion.oc1.eu-frankfurt-1.amaaaaaaupfargiaagg2k5ndzglenayjaxqryrusuawkjqhgo...

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Security » Bastion » dbbastion

B

ACTIVE

dbbastion

Edit | Add tags | Move resource

Bastion information | Tags

OCID: ...buphaa Show Copy

Created: Tue, Oct 25, 2022, 10:43:0

Target virtual Cloud network: iotne

Target subnet: iotprivate

Maximum session time-to-live (TTL

Resources

Sessions

Metrics

Filters

State

All

Sessions

Create session

Name	Session type

Create session

Help

Bastion name

dbbastion

Session type

SSH port forwarding session

Session name

dbtestsession

Connect to the target host by using:

IP address | Instance name

IP address

10.3.4.182

Port

22

Add SSH key

Choose SSH key file | Paste SSH key | Generate SSH key pair

Download the private key so that you can connect to the instance using SSH. It will not be shown again.

Save private key | Save public key

Show advanced options

Create session | Cancel

Terms of Use and Privacy | Cookie Preferences

ssh-key-2022-10-25.key

Show all

Bastion | Oracle Cloud Infrastruct

cloud.oracle.com/security/bastion/bastions/ocid1.bastion.oc1.eu-frankfurt-1.amaaaaaaupfargiaagg2k5ndzglenayjaxqryrusuawkjqhgo...

ORACLE Cloud | Cloud Classic | Search resources, services, documentation, and Marketplace | Germany Central (Frankfurt)

Security » Bastion » dbbastion

B

ACTIVE

dbbastion

Edit | Add tags | Move resource | Delete bastion

Bastion information | Tags

OCID: ...buphaa Show Copy

Created: Tue, Oct 25, 2022, 10:43:03 UTC

Target virtual Cloud network: iotnet

Target subnet: iotprivate

Maximum session time-to-live (TTL): 3 hours, 00 minutes

CIDR block allowlist: 10.3.0.0/24

Compartment: oraemeasec (root)/Advisory/ios_no

Private endpoint IP address: 10.3.4.100

Bastion type: Standard

Resources

Sessions

Metrics

Filters

State

All

Sessions

Create session

Name	Session type	Target resource	Target port	Username	State	Session TTL	Started
dbtestsession	Port forwarding	10.3.4.182	22	-	Active	3 hours, 00 minutes	Tue, Oct 25, 2022, 12:38:01 UTC

Showing 1 Item 1 of 1

Terms of Use and Privacy Cookie Preferences

ssh access to target resource via ssh tunnel

Bastion Session Creation

Start the ssh-agent

```
eval `ssh-agent`
```

Upload the users own private key

```
ssh-add myprivatekey.key
```

Upload the private key created by the bastion session

```
ssh-add bastion-session.key
```

Create a resident ssh tunnel to the target, through the Bastion Service

```
ssh -N -4 -L 8222:10.3.4.182:22 -p 22 ocid1.bastionsession.oc1.eu-frankfurt-
1.a*****@host.bastion.eu-frankfurt-1.oci.oraclecloud.com
```

Connect to the target over the ssh tunnel

ssh tunnel example

```
[ios@ios3 ~]$ ssh-add -l
The agent has no identities.
[ios@ios3 ~]$ ssh-add .ssh/iosstd
Identity added: .ssh/iosstd (.ssh/iosstd)
[ios@ios3 ~]$ ssh-add .ssh/ses.key
Identity added: .ssh/ses.key (.ssh/ses.key)
[ios@ios3 ~]$ ssh-add -l
2048 SHA256:zoFfJmFc0GzGZR/7j8tG/+8fswxLnUR0IvTWB9LvtaY .ssh/iosstd (RSA)
2048 SHA256:qS+sUTND8xnghyB2vFsuZ2ggc79juxOXfRTjB9nYtqI .ssh/ses.key (RSA)
[ios@ios3 ~]$ ssh -4 -N -L 8222:10.3.4.182:22 -p 22 ocidl.bastionsession.ocl.eu-frankfurt-1.amaaaaaaupfargia
jmymczp2rbe6qxthyg24jg4klyanpmyl77q457xhw33q@host.bastion.eu-frankfurt-1.oci.oraclecloud.com
```

```
[ios@ios3 cloud_scripts]$
[ios@ios3 cloud_scripts]$
[ios@ios3 cloud_scripts]$
[ios@ios3 cloud_scripts]$ ssh oracle@localhost -p 8222
Last login: Tue Oct 25 12:51:07 2022
[oracle@ios ~]$ uname -a
Linux ios 4.14.35-2047.510.5.5.el7uek.x86_64 #2 SMP Fri Jan 28 08:33:42 PST 2022 x86_64 x86_64 x86_64 GNU/Linux
[oracle@ios ~]$ exit
logout
Connection to localhost closed.
[ios@ios3 cloud_scripts]$
```

Example script for creating bastion service session, Managed SSH Session with OCI CLI

```
#!/bin/bash
#
# Example script that creates a managed ssh session with the bastion service
#
PYENV=/home/ios/py38
OCIPROFILE=oraemeasec
BASTIONOSID="ocid1.bastion.oc1.eu-frankfurt-1.amaaaaaaupfargial6ibktqk7xmz6kywqkcwsxrmqrdqjsyyf24qvwcqnbpq"
SSHKEYDIR="/home/ios/.ssh/"
SSHPUBFILE="bastion_pub"
SSHPRIVATEFILE="bastion.pem"
DISPLAYNAME="iosjumpv3-session"
RESOURCEID="ocid1.instance.oc1.eu-frankfurt-1.antheljsupfargic47fjgar7f34zdiccsv5wmrfsv4bnkfnyindlh6ew46ka"
OSUSERNAME=opc
RESOURCEPORT=22
RESOURCEIPADDRESS="10.3.4.86"
OCIREGION="eu-frankfurt-1"
TIMETOLIVE=1800
TEMPFILE=/home/ios/tempCreateSession.json
#
# Activate python env for OCI config
#
source py38env/bin/activate
```

```
#
# build inputfile for session creation
#
echo '{
  "bastionId": "'${BASTIONOSID}'",
  "displayName": "'${DISPLAYNAME}'",
  "keyType": "PUB",
  "maxWaitSeconds": 0,
  "sessionTtl": "string",
  "session-ttl-in-seconds": '${TIMETOLIVE}',
  "sshPublicKeyFile": "'${SSHKEYDIR}${SSHPUBFILE}'",
   "target-resource-details": {
        "session-type": "MANAGED_SSH",
        "target-resource-id": "'${RESOURCEID}'",
        "target-resource-operating-system-user-name": "'${OSUSERNAME}'",
        "target-resource-port": '${RESOURCEPORT}',
        "target-resource-private-ip-address": "'${RESOURCEIPADDRESS}'"
      },
  "waitForState": [
    "SUCCEEDED"
  ],
  "waitIntervalSeconds": 60
}'  >$TEMPFILE
```

```
#
# Create the session
#
#CSTATUS=`oci bastion session create --profile $OCIPROFILE --bastion-id --from-json "file://${TEMPFILE}"`
CSTATUS=`oci bastion session create --profile $OCIPROFILE --from-json "file://${TEMPFILE}"`
#echo $CSTATUS | jq '.data."lifecycle-state"' |  grep
'ACCEPTED\|CANCELED\|CANCELING\|IN_PROGRESS\|SUCCEEDED\|ACTIVE\|CREATING' >/dev/null
echo $CSTATUS | jq '.data."lifecycle-state"' |  grep
'ACCEPTED\|CANCELED\|CANCELING\|IN_PROGRESS\|SUCCEEDED\|ACTIVE\|CREATING'
if [ $? -ne  0 ]
then
  echo $CSTATUS
  echo ""
  echo "Creation of session failed"
  exit 1
fi
#
# check if creation failed
#
ASTATUS=`echo $CSTATUS | jq '.data."lifecycle-state"' | sed 's/"//g'`
if [ "$ASTATUS" = "FAILED" ]
then
  echo $CSTATUS
  echo "Creation of session failed"
  exit 2
fi
```

```
#
# grab the ID of the session, and check if it is active
#
ID=`echo $CSTATUS | jq '.data.id' | sed 's/"//g'`
echo "ID: "$ID
if [  "$ASTATUS" != "ACTIVE" ]
then
    echo "waiting for session creation (approx 60 sec.)"
    for I in 1 2 3 4 5 6
    do
      sleep 10
      ASTATUS=`oci --profile $OCIPROFILE bastion session get --session-id $ID | jq '.data."lifecycle-state"' | sed 's/"//g' `
      if [ "$ASTATUS" = "ACTIVE" ]
      then
        echo "bastion service is ready"
        break
      fi
      echo "Creation status: "${ASTATUS}
    done
     if [ "$ASTATUS" != "ACTIVE" ]
      then
        echo "bastion service is not yet available "
        echo "Please verify with command: "
        echo "oci --profile $OCIPROFILE bastion session get --session-id $ID"
        exit 1
      fi
fi
```

```
#
#  Connect to the session
#
ssh -i ${SSHKEYDIR}${SSHPRIVATEFILE} -o ProxyCommand="ssh -i  ${SSHKEYDIR}${SSHPRIVATEFILE} -W %h:%p -p 22
${ID}@host.bastion.${OCIREGION}.oci.oraclecloud.com" \
 -p ${RESOURCEPORT} ${OSUSERNAME}@${RESOURCEIPADDRESS}
```