



# Configure Conditional DNS forwarding between OCI and AD Domain

## Table of contents

Configure Conditional DNS forwarding between OCI and AD Domain .....	3
Introduction .....	3
Scope of the Document .....	3
Summary and Considerations .....	4
What is conditional DNS forwarding? .....	5
Implementation .....	6
Task 1: Setup OCI DNS endpoint .....	8
CREATE A NEW SUBNET .....	8
CREATE DNS ENDPOINT .....	9
Task 2: Create DNS forwarding rules in OCI .....	12
Task 3: Configure Conditional DNS forwarders in AD DNS Server .....	13
CREATE A REVERSE LOOKUP ZONE AND PTR RECORD .....	14
CONFIGURE CONDITIONAL FORWARDER .....	17
Conclusion .....	20
Authors and Contributors .....	21

## Configure Conditional DNS forwarding between OCI and AD Domain

### Introduction

DNS is undoubtedly one of the critical functions in the IT infrastructure. Given the current trends, organizations are deploying and managing IT environments across multiple clouds spanning geo-locations. This multi-cloud deployment requires a robust DNS query resolution mechanism that can simplify DNS resolution across distributed environments. One such mechanism and, I guess, historically well-adopted mechanism is the DNS forwarding that allows you to create forwarding rules based on specific Domain or CIDR requests. This document will walk you through the steps on how to implement DNS forwarding between OCI and AD domain DNS servers.

Oracle Cloud VMware Solution is deployed in Oracle Cloud Infrastructure regions and uses the native OCI DNS service. It leverages OCI DNS service to obtain and resolve the name resolution queries for the OCVS VMware SDDC appliances and OCI endpoints. Once the VMware SDDC is up and running, you can onboard OCVS VMware SDDC appliances and application workloads to the organization's DNS Servers. This will allow you to query your existing organization's AD domain and resolve the VMware SDDC appliance's DNS queries for specific use cases. These use cases can be configuring VMware SRM, VMware Tanzu, and VMware Horizon or resolving application endpoints within the native OCI cloud and vice versa. To achieve this task, we will use one of the DNS features, Conditional DNS forwarding. In this how-to guide, I will walk you through the steps and important details about configuring conditional DNS forwarding between the OCI DNS service and the active directory DNS server.

Below are some key objectives we will achieve with this implementation guide.

- Ability to resolve OCI endpoints with the clients deployed in OCVS VMware SDDC.
- Ability to resolve application workloads deployed in OCVS VMware SDDC.
- Ability to resolve OCI Endpoints, OCVS VMware SDDC workloads (VMs), and On-prem workloads.

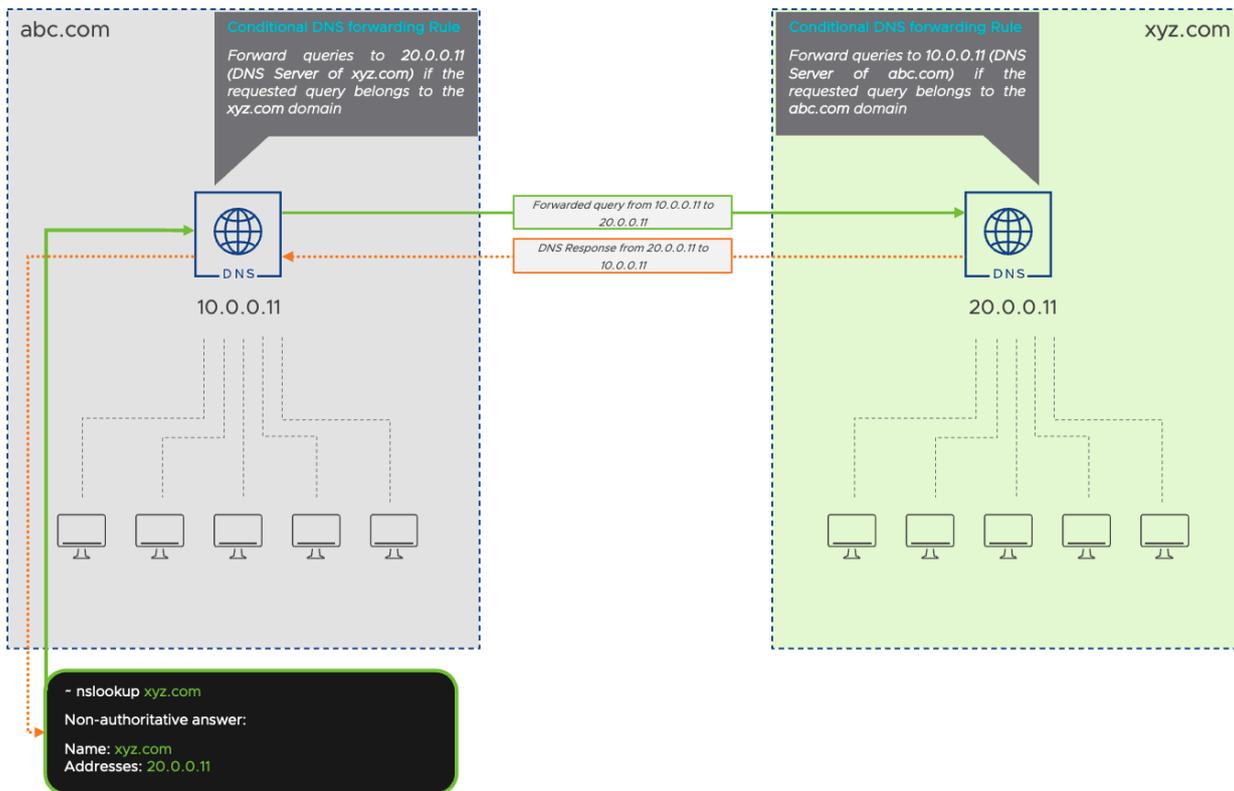
### Scope of the Document

This document requires a basic understanding of DNS, VMware SDDC, and Oracle Cloud Infrastructure.

## Summary and Considerations

<b>Use Case</b>	Resolving DNS queries within the OCI, OCVS VMware SDDC workloads, and on-prem environment.
<b>Pre-requisites</b>	Below are some of the pre-requisites to configuring conditional DNS forwarder:
<b>General Considerations/Recommendations</b>	
<b>Performance Considerations</b>	There are no specific performance considerations except creating a separate subnet in OCI to host DNS endpoints. Also, it ensures that all the DNS servers in the AD domain are healthy.
<b>Network Considerations/Recommendations</b>	
<b>Document Reference</b>	<a href="#">Oracle Cloud Documentation - DNS in Your Virtual Cloud Network</a>
<b>Last Updated</b>	January 2023

## What is conditional DNS forwarding?



Conditional DNS forwarding is a method to direct DNS queries related to a specific domain to another DNS server. This is done by creating conditional DNS forwarders or rules on the DNS server. This is a simple and reliable method to resolve DNS queries belonging to an external domain.

For example, as illustrated in the above diagram, we have two domains, **abc.com** and **xyz.com**. Clients belonging to **abc.com** reach out to their DNS server, which is **10.0.0.11**. Similarly, clients belonging to **xyz.com** reach out to their DNS server, which is **20.0.0.11**. However, in a scenario where clients from the **abc.com** domain will not be able to resolve queries related to **xyz.com** because it does not have any DNS records of the **xyz.com** domain and vice versa.

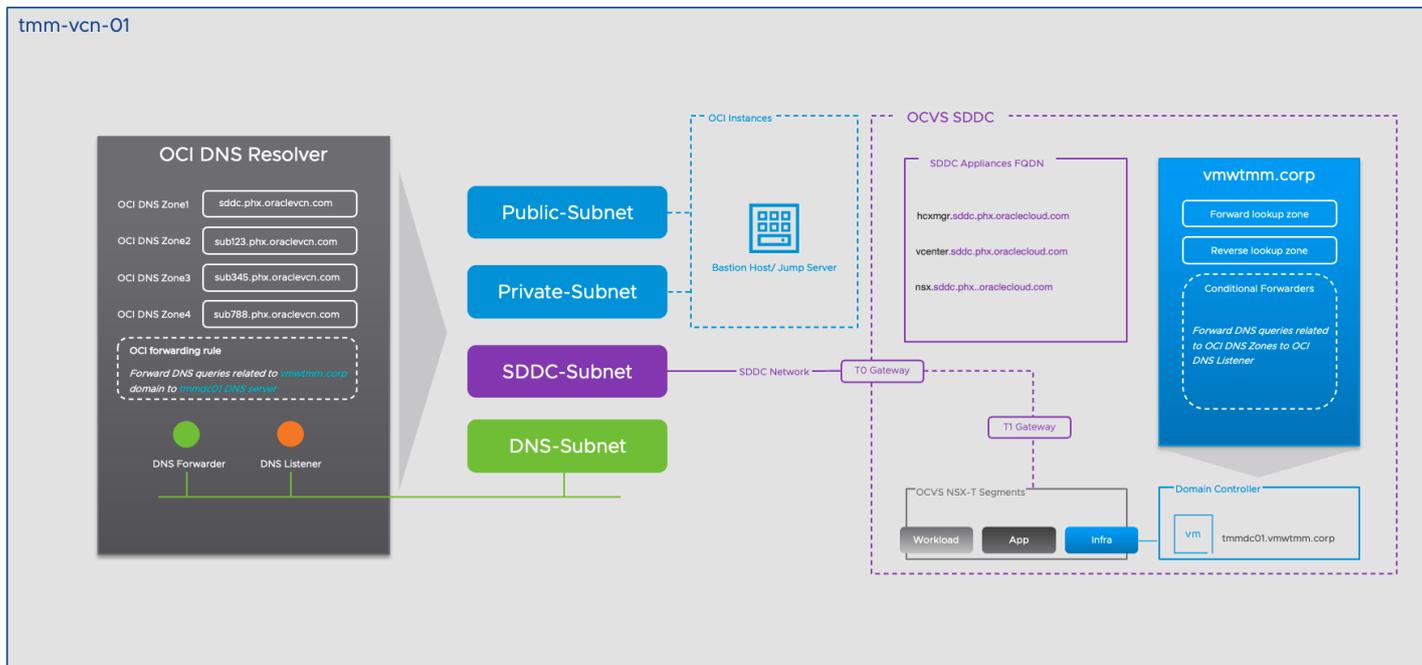
To resolve this issue, you can configure a conditional DNS forwarder to point external DNS server to resolve queries belonging to a specific domain. This DNS server is expected to have the DNS records of the requested domain.

As shown in the above diagram, a conditional DNS forwarder is configured on the **abc.com** DNS server that can be understood as "Forward queries from **abc.com** to **20.0.0.11 (DNS Server of xyz.com)** if requested query belongs to the **xyz.com** domain". Similarly, a conditional DNS forwarder is configured on the **xyz.com** DNS server that can be understood as "Forward queries from **xyz.com** to **10.0.0.11 (DNS Server of abc.com)** if requested query belongs to the **abc.com** domain".

## Implementation

In the below section, we will look at the implementation steps to configure conditional DNS forwarding between the OCI DNS endpoint and our custom AD domain.

Before you begin



Before we begin the implementation, let us quickly understand the setup. The OCVS is a native tenant of OCI and leverages OCI infrastructure for compute, networks, and storage. I assume you do have a basic understanding of OCVS networking, so I will not touch base on all the details related to OCVS networking. However, I will explain how OCI DNS is playing its role in the OCVS SDDC environment.

**Subnets**, subnets are logical networks that you can create within the VCN. There can be two types of subnets: public and private.

**DNS Resolver**, Each VCN has its default OCI DNS resolver. The OCI DNS resolver associates a respective DNS private zone for each subnet in the VCN. All the instances in the OCI point to DNS resolver as their DNS server endpoint. The default DNS server IP address is hidden from the users, and we eventually get a masked IP address when we query the DNS server endpoint.

**tmm-vcn-01**

[Move resource](#)
[Add tags](#)
[Delete](#)

[VCN Information](#)
[Tags](#)

---

**Compartment:** vmware  
**Created:** Fri, Nov 25, 2022, 13:59:47 UTC  
**IPv4 CIDR Block:** 45.0.0.0/16  
**IPv6 Prefix:** No value

**OCID:** ...Zoeyna [Show Copy](#)  
**DNS Resolver:** tmm-vcn-01  
**Default Route Table:** [Default Route Table for tmm-vcn-01](#)  
**DNS Domain Name:** tmmvcn01.oraclevcn.com

**OCI DNS Zones**, As illustrated in the below diagram, we have four subnets: **Public, Private, SDDC subnets, and a new DNS subnet** (Need to create manually as a part of the implementation step). Each of these subnets has its own DNS zone to keep the DNS records documented.

**tmm-vcn-01**

Edit Move resource Add tags Delete

Private View Information Tags

OCID: ...bjsryq Show Copy Created: Fri, Nov 25, 2022, 13:59:48 UTC  
Protected: Yes ⓘ Compartment: vmware

## Private Zones in vmware Compartment

Private zones contain DNS data only accessible from within a VCN, such as private IP addresses.

Create Zone

Zone Name	Zone Type	Protected ⓘ	Created
subnettmmdns.tmmvcn01.oraclevcn.com → DNS zone for DNS Subnet	Primary	Yes	Wed, Jan 4, 2023, 15:41:58 UTC
sub12141309171.tmmvcn01.oraclevcn.com → DNS zone for ESXi Hosts	Primary	Yes	Wed, Dec 14, 2022, 13:14:42 UTC
sub11251359391.tmmvcn01.oraclevcn.com → DNS zone for Private Subnet	Primary	Yes	Fri, Nov 25, 2022, 13:59:51 UTC
sub11251359390.tmmvcn01.oraclevcn.com → DNS zone for Public Subnet	Primary	Yes	Fri, Nov 25, 2022, 13:59:50 UTC
sddc.phx.oci.oraclecloud.com → DNS zone for SDDC Appliances	Primary	No	Wed, Dec 14, 2022, 13:27:20 UTC
4.12.0.45.in-addr.arpa → Reverse Lookup zone	Primary	No	Wed, Dec 14, 2022, 13:27:25 UTC

The screenshot shows a hierarchical view of DNS zones in OCI. The root zone is vcenter-tmm-sddc-01.sddc.phx.oci.oraclecloud.com. Underneath it, there are three sub-zones: tmm-sddc-01-1.sub12141309171.tmmvcn01.oraclevcn.com, tmm-sddc-01-2.sub12141309171.tmmvcn01.oraclevcn.com, and tmm-sddc-01-3.sub12141309171.tmmvcn01.oraclevcn.com. Red arrows point from the root zone to the sub-zones, with labels: 'vCenter FQDN from OCI SDDC Subnet DNS Zone' pointing to the first sub-zone and 'ESXi FQDN from OCI DNS Zone' pointing to the second sub-zone.

**SDDC DNS Zone**, a separate OCI DNS zone, is created when we deploy a new OCVS SDDC. This zone contains the DNS records for all the VMware SDDC appliances. Also, a new separate OCI DNS zone is created to store the ESXi host's DNS records.

DNS - sddcloud.com

Move resource Add tags Delete

Zone Information Tags

Zone Scope: Private  
 Zone Type: Primary  
 Private View: [tmm-vcn-01](#)  
 Nameservers: vcn-dns.oraclevcn.com

Created: Wed, Dec 14, 2022, 13:27:20 UTC  
 OCID: ...zj6w3a [Show](#) [Copy](#)  
 Compartment: vmware  
 Protected: No ⓘ

Records

Publish Changes

Add Record Actions Search...

Domain	TTL	Type	RDATA	Protected	State
hcxmgr-trn.coci.oraclecloud.com	900	A	45	No	Unmodified
hcxmgr-trn.coci.oraclecloud.com	900	A	46	No	Unmodified
nsx-tmm-01.oraclecloud.com	900	A	45	No	Unmodified
nsx-tmm-01.oraclecloud.com	900	A	46	No	Unmodified
sddc.phx.vcn	86400	NS	vcn	Yes	Protected
sddc.phx.vcn	86400	SOA	vcn	Yes	Protected
vcenter-trn.coci.oraclecloud.com	900	A	45	No	Unmodified
vcenter-trn.coci.oraclecloud.com	900	A	46	No	Unmodified

**OCI DNS Endpoint**, The OCI DNS resolver masks its IP address for security reasons. So, if you want to interact with OCI DNS resolver, you must create two DNS endpoints, a DNS forwarder and a DNS listener. Both of these DNS endpoints have a network interface with which other services can communicate.

## Task 1: Setup OCI DNS endpoint

As explained in the earlier section, 'DNS Resolver', the DNS resolver hides its IPv4 interface for security reasons. To interact with the DNS resolver, you must create DNS endpoints. There are two types of DNS endpoints that you will need to configure. These two DNS endpoints are the DNS forwarder and DNS listener.

Depending on the DNS forwarding rule, the DNS forwarder will be used to forward DNS queries to an external DNS server. Similarly, the DNS listener will be used to receive DNS queries from an external domain. Below are the implementation steps for creating DNS endpoints.

### CREATE A NEW SUBNET

Create a new private subnet to host DNS endpoint IP interfaces. This is not mandatory, and you can use any existing private subnet within the VCN, but it is highly recommended to create a new subnet for DNS management to simplify the network management.

1. Login to OCI console.
2. Click on the Hamburger menu on the top left side.
3. Go to **Networking** and Select **Virtual Cloud Network**.
4. Select the appropriate VCN.
5. Scroll down to the Subnet Section.
6. Click **Create Subnet**.
7. Provide the following details.
  - a. Subnet **name**.
  - b. Select the appropriate **compartment**.
  - c. Select Subnet Type, and Select this as **Regional (Recommended)**
  - d. Select the IPv4 block. Make sure you pick a CIDR block from the VCN CIDR block and ensure that it does not override with any other CIDR block in your environment.

**Create Subnet**

Name 1

Create In Compartment 2  
vmware

Subnet Type 3  
 **Regional (Recommended)**  
 Instances in the subnet can be created in any availability domain in the region. Useful for high availability.  
 **Availability Domain-specific**  
 Instances in the subnet can only be created in one availability domain in the region.

IPv4 CIDR Block 4  
 IPv4 CIDR Block  
 Example: 10.0.0.0/24

- e. Select the appropriate route table.
- f. Select the Subnet access as **Private Subnet**.
- g. Keep the **'Use DNS hostnames in this subnet'** check box enabled under DNS resolution section.
- h. Select the appropriate security rule.
- i. Click **Create Subnet**.

**Note:** Configure the appropriate route table and security list to enable communication between the OCI DNS subnet and the OCVS custom DNS server. Ensure you can telnet to port 53 in both directions.

**Create Subnet**

Route Table Compartment in **vmware** 5 [\(Change Compartment\)](#)  
 Default Route Table for tmm-vcn-01

Subnet Access 6  
 **Private Subnet**  
 Prohibit public IP addresses for Instances in this Subnet  
 **Public Subnet**  
 Allow public IP addresses for Instances in this Subnet

DNS Resolution  
 **Use DNS hostnames in this SUBNET** ⓘ  
 Allows assignment of DNS hostname when launching an Instance

DNS Label  
 Generated from subnet name if not specified  
 Only letters and numbers, starting with a letter. 15 characters max.

DNS Domain Name *Read-only*  
 <dns-label>.tmmvcn01.oraclevcn.com

Dhcp Options Compartment in **vmware** 7 [\(Change Compartment\)](#)  
 Select DHCP options

Security Lists 8  
 You can associate up to 5 network security lists with the subnet.  
 Security List Compartment in **vmware** [\(Change Compartment\)](#)  
 Default Security List for tmm-vcn-01

[+ Another Security List](#)

[Create Subnet](#) [Cancel](#)

## CREATE DNS ENDPOINT

Create DNS forwarder and DNS listener on OCI DNS resolver.

1. Select the appropriate VCN.
2. Click **DNS Resolver**.

tmm-vcn-01

Move resource Add tags Delete

VCN Information Tags

Compartment: vmware  
 Created: Fri, Nov 25, 2022, 13:59:47 UTC  
 IPv4 CIDR Block: 45.0.0.0/16  
 IPv6 Prefix: No value

OCID: ...2oeyna Show Copy **1**  
 DNS Resolver: [tmm-vcn-01](#)  
 Default Route Table: [Default Route Table for tmm-vcn-01](#)  
 DNS Domain Name: tmmvcn01.oraclevcn.com

3. Under the resources section. Click on **Endpoints**.
4. Click on Create Endpoint.

Networking > Virtual Cloud Networks > tmm-vcn-01 > Private Resolver Details

tmm-vcn-01

Edit Move resource Add tags

Private Resolver Information Tags

OCID: ...b5d4da Show Copy  
 Dedicated Virtual Cloud Network: [tmm-vcn-01](#)  
 Protected: Yes ⓘ

A private DNS resolver handles DNS queries within your VCN based on private views and private DNS zones. A private DNS zone has similar capabilities to an Internet DNS zone, but provides resolution through a VCN. VCN creation includes a dedicated DNS resolver and a default private view with system-resolved DNS. You will have to create views and zones that the resolver can use to direct internal traffic.

Resources

Associated Private Views (0)  
 Rules (3) **1**  
**Endpoints (2)**  
 Work Requests (0)

Endpoints

The private endpoints use **2** forwarding and listening to DNS queries to or from another VCN.

Create Endpoint **2**

Name	State	Subnet
<a href="#">tmmdnsforwarder</a>	● Active	<a href="#">Subnet-tmm-dns</a>
<a href="#">tmmdnslistener</a>	● Active	<a href="#">Subnet-tmm-dns</a>

5. Create **DNS Listener**.
  - a. Provide a friendly name.
  - b. Select the **Subnet**.
  - c. Select the Endpoint type and Select **Listening**.
  - d. Provide a **Listening IP address**.
  - e. **Create Endpoint**.

**Create Endpoint** [Help](#)

Name:  1

Choose a subnet in VMware [\(change commitment\)](#) 2  
Subnet-tmm-dns

Endpoint type:  Listening  Forwarding 3  
An IP address in the subnet used to listen for queries. If a listening address is not provided then it will be assigned by the system. An IP address in the subnet that queries may be forwarded from. If a forwarding address is not provided then it will be assigned by the system.

Listening IP Address:  4  
Optional  
Please enter a valid IP address.  
 Use Network Security Group to control traffic: Optional  
Select up to a maximum of (5) network security groups.

5

6. Create a **DNS forwarder**.
  - a. Provide a friendly name.
  - b. Select the **Subnet**.
  - c. Select the Endpoint type and Select **Forwarding**.
  - d. Provide a **Forwarding IP address**.
  - e. **Create Endpoint**.

**Create Endpoint** [Help](#)

Name:  1

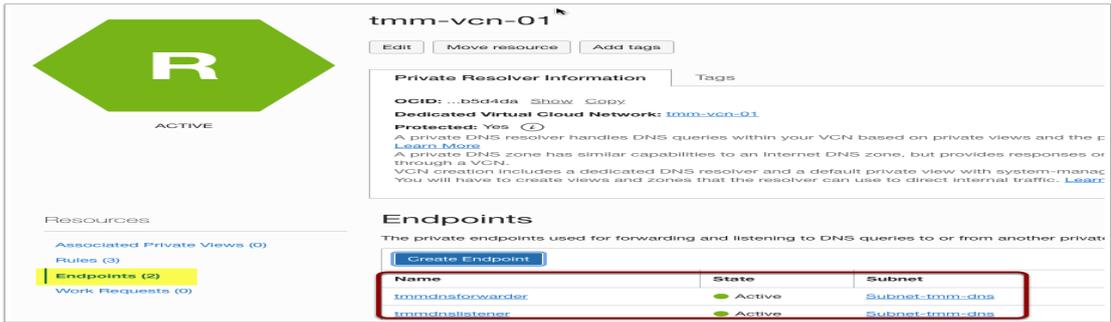
Choose a subnet in VMware [\(change commitment\)](#) 2  
Subnet-tmm-dns

Endpoint type:  Listening  Forwarding 3  
An IP address in the subnet used to listen for queries. If a listening address is not provided then it will be assigned by the system. An IP address in the subnet that queries may be forwarded from. If a forwarding address is not provided then it will be assigned by the system.

Listening IP Address:  4  
Optional  
Please enter a valid IP address.  
 Use Network Security Group to control traffic: Optional  
Select up to a maximum of (5) network security groups.

5

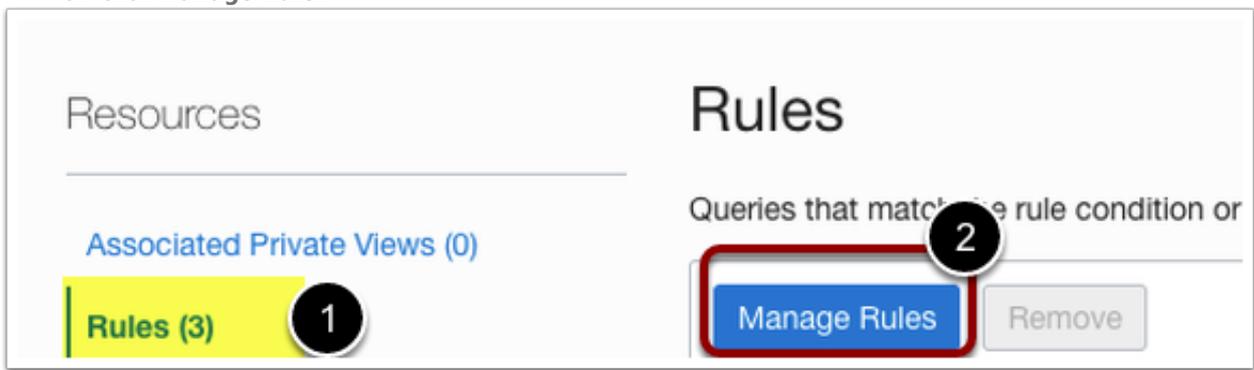
After the successful creation of both endpoints, you should be able to see the endpoint list as below.



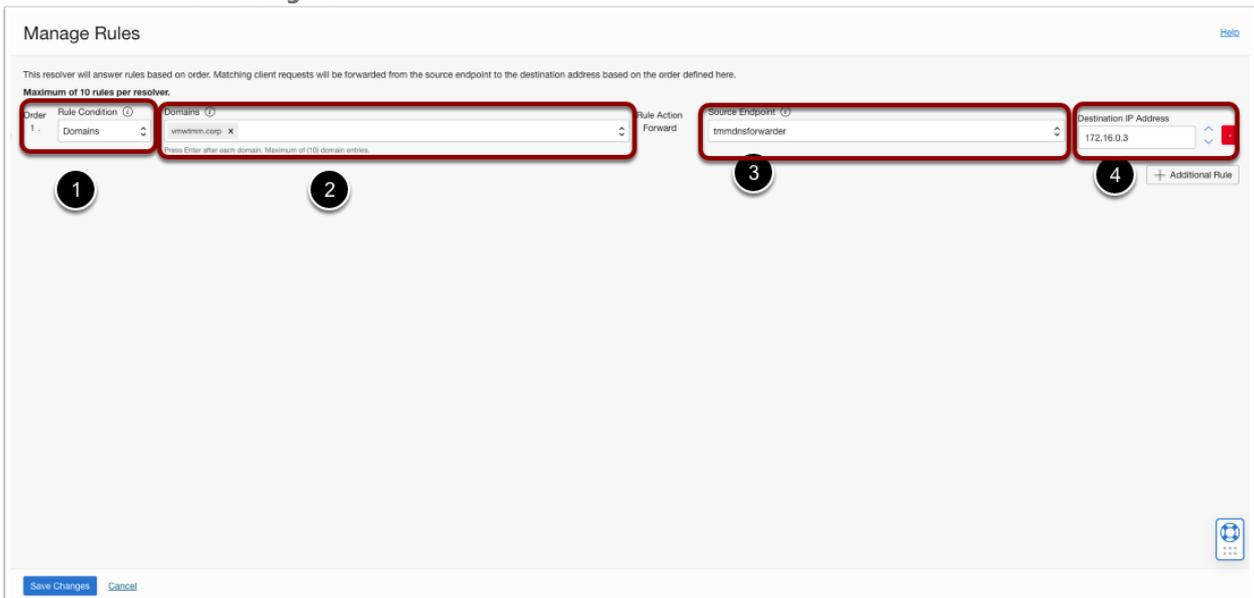
## Task 2: Create DNS forwarding rules in OCI

Now we have DNS endpoints that can act as the interface to communicate with OCI DNS resolver. In the OCI DNS resolver, create a new DNS forwarding rule to forward DNS queries that belongs to your custom domain to an external DNS server. This will allow OCI instances to resolve DNS queries that belong to your custom domain.

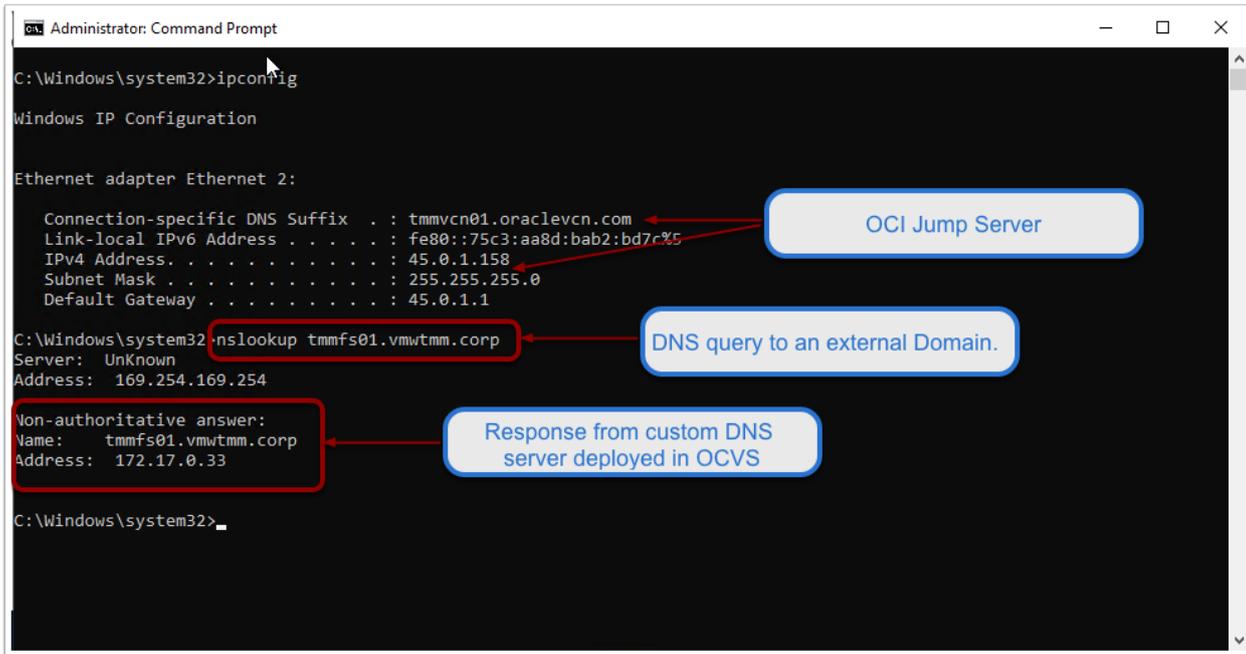
1. Go to the DNS resolver.
2. Under Resources Section, Click on **Rules**.
3. Click **Manage Rule**.



4. Provide Rule Condition, Select **Domain**.
5. **Provide Domain Name.**
6. Select **DNS Forwarder** as the source endpoint.
7. Enter the **Destination IP address**. This is the custom DNS Server IP address in the OCVS environment.
8. Click **Save Changes**.



After the successful completion of this task, you should be able to resolve DNS queries from OCI instances to the custom domain deployed in the OCVS environment.



### Task 3: Configure Conditional DNS forwarders in AD DNS Server

Before getting into the implementation details of configuring the conditional DNS forwarder, let us review OCI DNS zones in detail. Here, I will take an example of one of my OCVS SDDC lab instances and explain how VMware SDDC appliances, such as vCenter, NSX Manager, and HCX, get their FQDN address from OCI DNS.

tmm-vcn-01

Edit Move resource Add tags Delete

Private View Information Tags

OCID: ...bjsryq Show Copy Created: Fri, Nov 25, 2022, 13:59:48 UTC  
 Protected: Yes ⓘ Compartment: vmware

Private Zones in vmware Compartment

Private zones contain DNS data only accessible from within a VCN, such as private IP addresses.

Create Zone

Zone Name	Zone Type	Protected ⓘ	Created
<a href="#">subnettmdns.tmmvcn01.oraclevcn.com</a> → DNS zone for DNS Subnet	Primary	Yes	Wed, Jan 4, 2023, 15:41:58 UTC
<a href="#">sub12141309171.tmmvcn01.oraclevcn.com</a> → DNS zone for ESXi Hosts	Primary	Yes	Wed, Dec 14, 2022, 13:14:42 UTC
<a href="#">sub11251359391.tmmvcn01.oraclevcn.com</a> → DNS zone for Private Subnet	Primary	Yes	Fri, Nov 25, 2022, 13:59:51 UTC
<a href="#">sub11251359390.tmmvcn01.oraclevcn.com</a> → DNS zone for Public Subnet	Primary	Yes	Fri, Nov 25, 2022, 13:59:50 UTC
<a href="#">sddc.phx.oci.oraclecloud.com</a> → DNS zone for SDDC Appliances	Primary	No	Wed, Dec 14, 2022, 13:27:20 UTC
<a href="#">4.12.0.45.in-addr.arpa</a> → Reverse Lookup zone	Primary	No	Wed, Dec 14, 2022, 13:27:25 UTC

As you can see in the above diagram, we have a number of DNS zone under the VCN DNS resolver. Each subnet in the VCN corresponds to its respective DNS zone and stores DNS records belonging to instances deployed in those subnets. Let us learn more about each of these zones and understand the DNS records stored in each of these zones.

#### 1. sddc.phx.oci.oraclecloud.com

This zone stores the DNS records of all the VMware SDDC appliances, such as vCenter, HCX, and NSX Manager endpoints.

FQDN	Type	RDATA
vcenter-tmm-sddc- 01. <b>sddc.phx.oci.oraclecloud.com</b>	A	45.0.12.2
nsx-tmm-sddc- 01. <b>sddc.phx.oci.oraclecloud.com</b>	A	45.0.12.3
hcxmgr-tmm-sddc- 01. <b>sddc.phx.oci.oraclecloud.com</b>	A	45.0.12.4

**2. sub1241309171.tmmvcn01.oraclevcn.com**

This zone stores the DNS records of all the ESXi hosts.

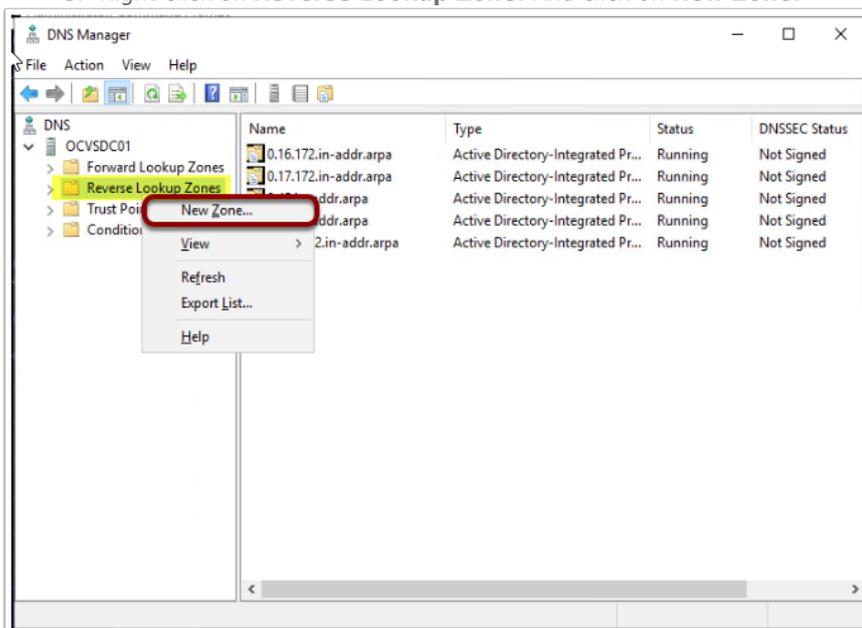
FQDN	Type	RDATA
tmm-sddc-01-1. <b>sub1241309171.tmmvcn01.oraclevcn.com</b>	A	45.0.8.27
tmm-sddc-01-2. <b>sub1241309171.tmmvcn01.oraclevcn.com</b>	A	45.0.8.46
tmm-sddc-01-3. <b>sub1241309171.tmmvcn01.oraclevcn.com</b>	A	45.0.8.71

Similarly, there are other OCI DNS zones that stores DNS records of OCI instances and the different service endpoints. We need to configure a conditional DNS forwarder for all the OCI zones that we want to resolve from our custom AD domain. In the case of OCVS SDDC endpoints, we will need to configure conditional DNS forwarders for '**sddc.phx.oci.oraclecloud.com**' and '**sub1241309171.tmmvcn01.oraclevcn.com**' in the customer AD DNS server.

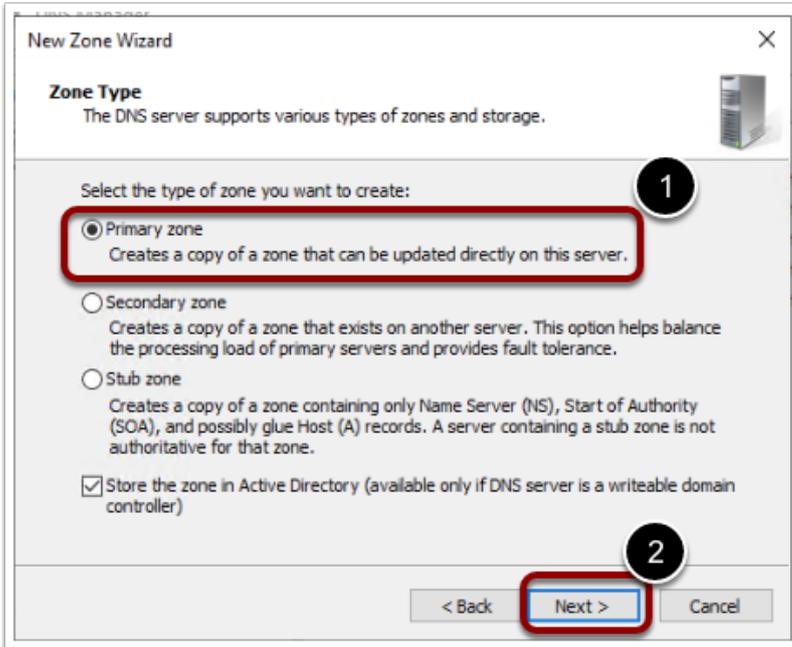
**CREATE A REVERSE LOOKUP ZONE AND PTR RECORD**

First, we will create a reverse lookup zone for the OCI DNS listener endpoint. In this example, the OCI DNS listener IP address is 45.0.2.10, and its FQDN is 'tmmdnslistener.subnettmmdns.tmmvcn01.oraclevcn.com'. We will use the reverse lookup zone to create a PTR record so that conditional forwarders can resolve the OCI DNS endpoint.

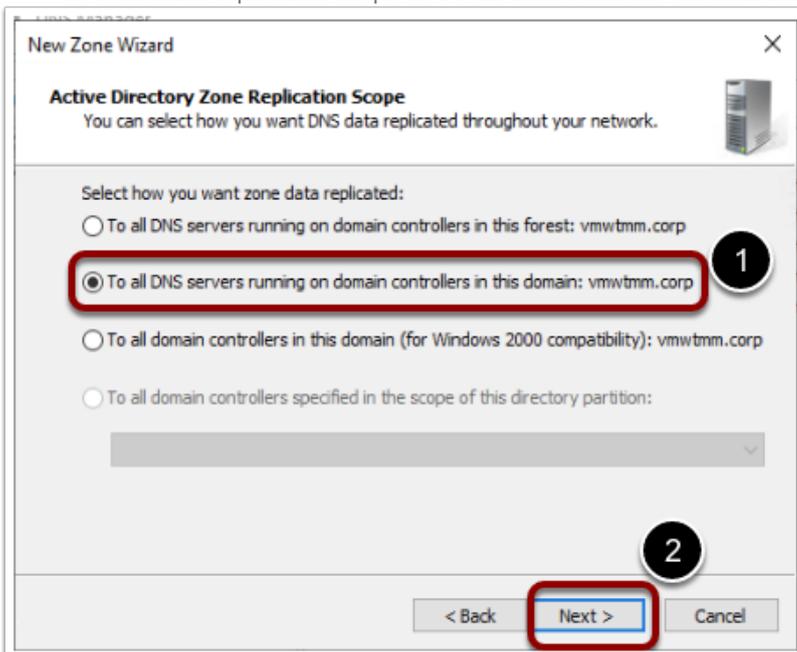
1. Login to the DNS server.
2. Explore the DNS application.
3. Right-click on **Reverse Lookup Zone**. And click on **New Zone**.



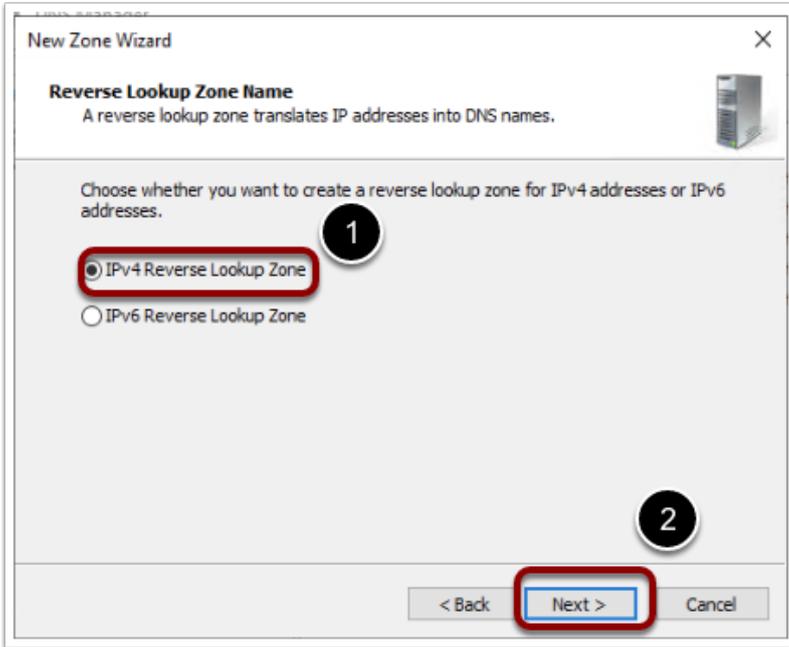
4. Select **Primary Zone** and click Next.



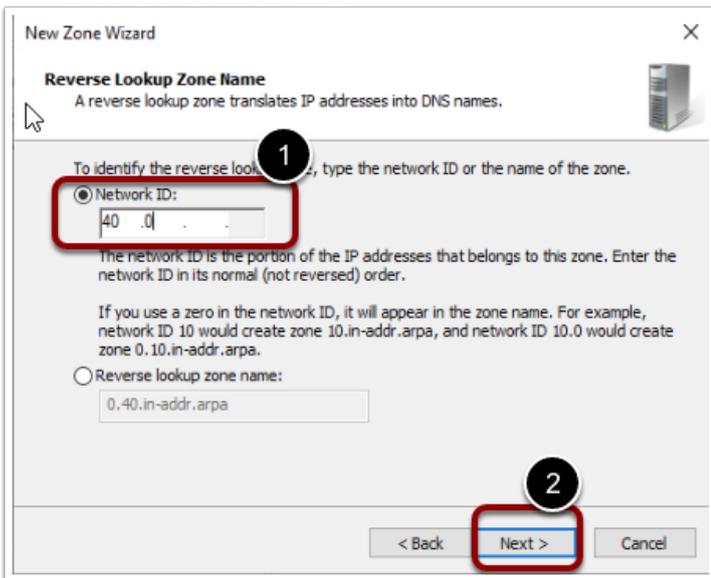
5. Select the replication scope as **To all DNS servers on domain controllers in this domain: *domainname***.



6. Select reverse lookup zone as **IPv4 reverse lookup zone**.



7. Provide the network ID.

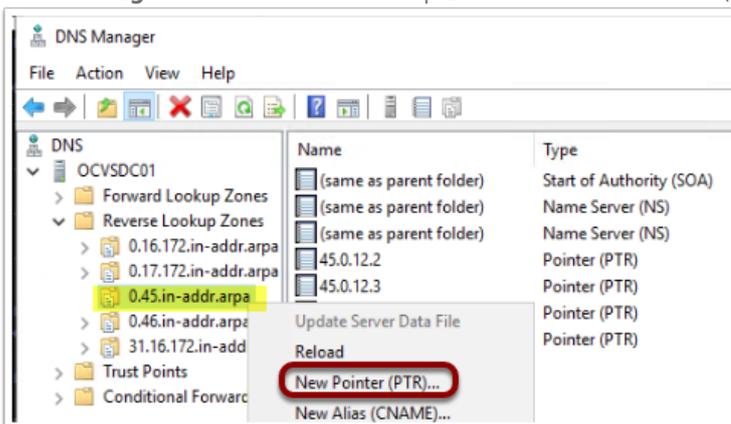


8. Enable **Allow only secure dynamic updates** option.

9. Finish.

Now create a PTR record for OCI DNS endpoint in the newly created reverse lookup zone.

10. **Right-click** on reverse lookup zone. Select New Pointer (PTR)



11. You can grab the OCI DNS listener endpoint IP address and FQDN from the OCI DNS resolver.

Domain	TTL	Type	RDATA
subnettmdns.tmmvcn01.oraclevcn.com	86400	NS	vcn-dns.oraclevcn.com.
subnettmdns.tmmvcn01.oraclevcn.com	86400	SOA	vcn-dns.oraclevcn.com. hostmaster.oracle.com. 3 3600 3600 3600 10
tmdnsforwarder.subnettmdns.tmmvcn01.oraclevcn.com	300	A	45.0.2.177
tmdnslistener.subnettmdns.tmmvcn01.oraclevcn.com	300	A	45.0.2.10

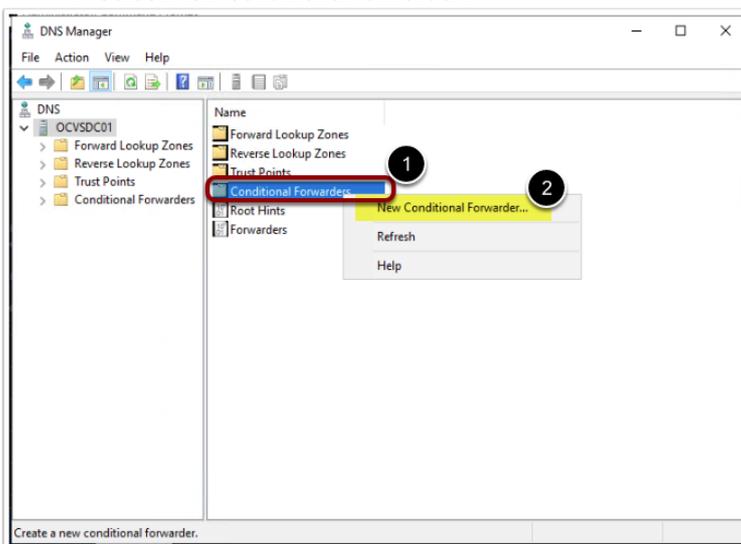
The 'New Resource Record' dialog box is shown with the following fields:

- Host IP Address: 45.0.2.10
- Fully qualified domain name (FQDN): 10.2.0.45.in-addr.arpa
- Host name: tmdnslistener.subnettmdns.tmmvcn01.oraclevcn.com

The 'OK' button is highlighted.

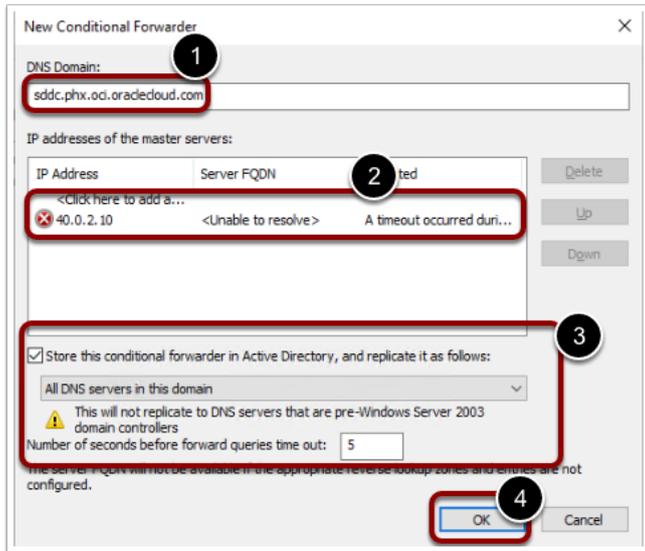
## CONFIGURE CONDITIONAL FORWARDER

1. Login to the DNS server.
2. Explore the DNS application.
3. Right-click on the conditional forwarder.
4. Select New Conditional forwarder.



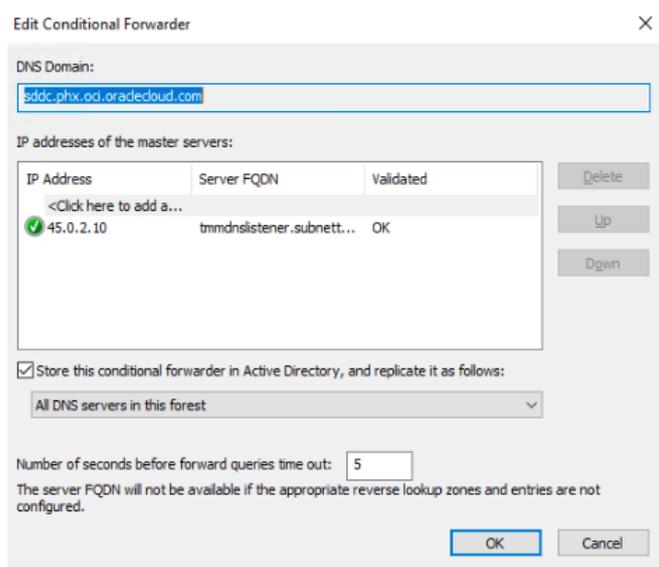
5. Provide following details
  - a. **DNS zone name:** This is the OCI DNS zone that you want to resolve
  - b. Provide **OCI DNS Listener IP address.** Please note that the first attempt will fail to resolve the IP address and return a failure message <Unable to resolve>, as shown in the picture below. But continue with the process.
  - c. Store this on all the DNS servers in the domain.
  - d. Click OK.

## Configure Conditional DNS forwarding between OCI and AD Domain



### Note:

After finishing this task, Go to conditional DNS forwarder and its properties. Edit the conditional DNS forwarder, and you will see that now the OCI DNS endpoint is able to resolve its IP address. If you are still getting <Unable to resolve> error message, then please verify the reverse lookup zone and OCI DNS endpoint PTR records.



After completion of this step, you should be able to resolve DNS queries related to the '**sddc.phx.oci.oraclecloud.com**' OCI DNS zone.

FQDN	Type	RDATA
vcenter-tmm-sddc- 01. <b>sddc.phx.oci.oraclecloud.com</b>	A	45.0.12.2
nsx-tmm-sddc- 01. <b>sddc.phx.oci.oraclecloud.com</b>	A	45.0.12.3
hcxmgr-tmm-sddc- 01. <b>sddc.phx.oci.oraclecloud.com</b>	A	45.0.12.4

Test 'nslookup' queries on all the SDDC appliances to verify whether the conditional DNS forwarder is working. If it is not working, please ensure that you have the correct routes and firewall settings configured to allow communication between the OCI DNS endpoint and the AD Domain DNS server over port 53.

```
Administrator: Command Prompt
C:\Users\Administrator>nslookup vcenter-tmm-sddc-01.sddc.phx.oci.oraclecloud.com
Server: localhost
Address: 127.0.0.1

Non-authoritative answer:
Name: vcenter-tmm-sddc-01.sddc.phx.oci.oraclecloud.com
Address: 45.0.12.2

C:\Users\Administrator>nslookup nsx-tmm-sddc-01.sddc.phx.oci.oraclecloud.com
Server: localhost
Address: 127.0.0.1

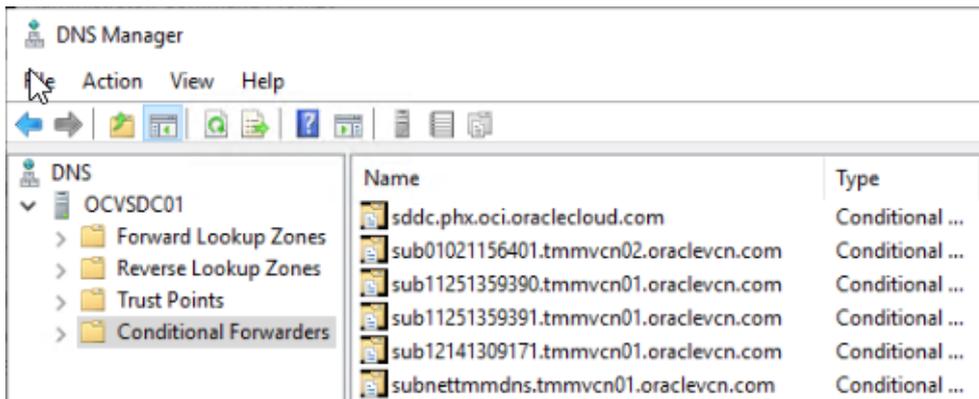
Non-authoritative answer:
Name: nsx-tmm-sddc-01.sddc.phx.oci.oraclecloud.com
Address: 45.0.12.3

C:\Users\Administrator>nslookup hcxmgr-tmm-sddc-01.sddc.phx.oci.oraclecloud.com
Server: localhost
Address: 127.0.0.1

Non-authoritative answer:
Name: hcxmgr-tmm-sddc-01.sddc.phx.oci.oraclecloud.com
Address: 45.0.12.4

C:\Users\Administrator>
```

Repeat the same process for all the OCI DNS zones that you want to resolve from AD Domain DNS Sever.



## Conclusion

DNS is an essential part of IT infrastructure. Given the multi-cloud deployment, resolving DNS queries that may belong to different DNS zones and domains becomes even more important. Many VMware solutions such as VMware SRM, HCX, Horizon, and VMware Tanzu require DNS resolution of SDDC appliances such as vCenter and NSX Manager. Conditional DNS forwarders between different DNS zones and domain certainly simplifies DNS management across the multi-cloud implementation.

## Authors and Contributors

A list of authors and contributors should be listed here in the following format:

- [Jatin Purohit](#), Sr. Technical Marketing Manager, VMware

Also, I would like to thank and acknowledge [Steve Dockar](#) (WW OCVS Field Solution Architect Director) for publishing a wonderful blog post "[Its always DNS...](#)" on his blog <https://notthe.blog/> . In addition to this, there are some great blog posts explaining different networking use cases on OCVS. Check out the details [here](#).

