SOP for Hybrid DNS

✓ Endorsed.

Scope

This page provides the standard operating procedures which include possible actions to be followed in the event of Hybrid DNS Requests for domain resolution or sharing it across multiple accounts.

Current Architecture:

Please refer to the document to understand the existing Hybrid DNS setup.

SOP for centralized domain DNS requests

Currently the Private Hosted Zone *(phz)* for aws.bhp.com has been setup in Core Networking account. Any requests destined for aws.bhp.com, whether generated from on-premise or other Spoke networking account, will be handled within the AWS Core Networking account.

The rules defined in outbound endpoints forward the traffic towards the servers currently being hosted under shared service account. (These servers are planned to move to the Core networking accounts in future)

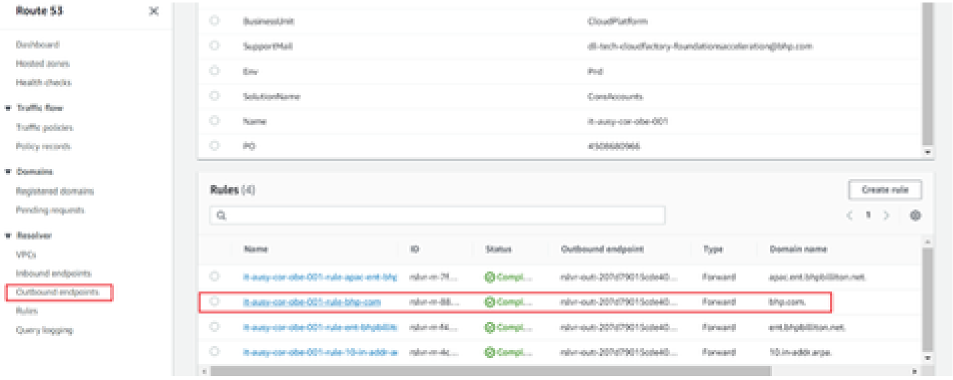
The rules for the outbound endpoints are shared amongst all the spoke accounts using Resource Access Manager.

SOP for queries generated from AWS Cloud Spoke Accounts:

If there is any issue in the connection for the DNS resolution for PHZ in AWS, verify the below steps in Core Network Account :

1. Verify VPC settings and set following settings to true in the Spoke Account VPC from where the query is initiated :
   - enableDnsHostnames
   - enableDnsSupport

   Kindly work with the AWS Squad to get the setting enabled.
2. Go to Route 53 domain and then to Outbound endpoints, verify there should be a rule pointing to *"bhp.com."*".

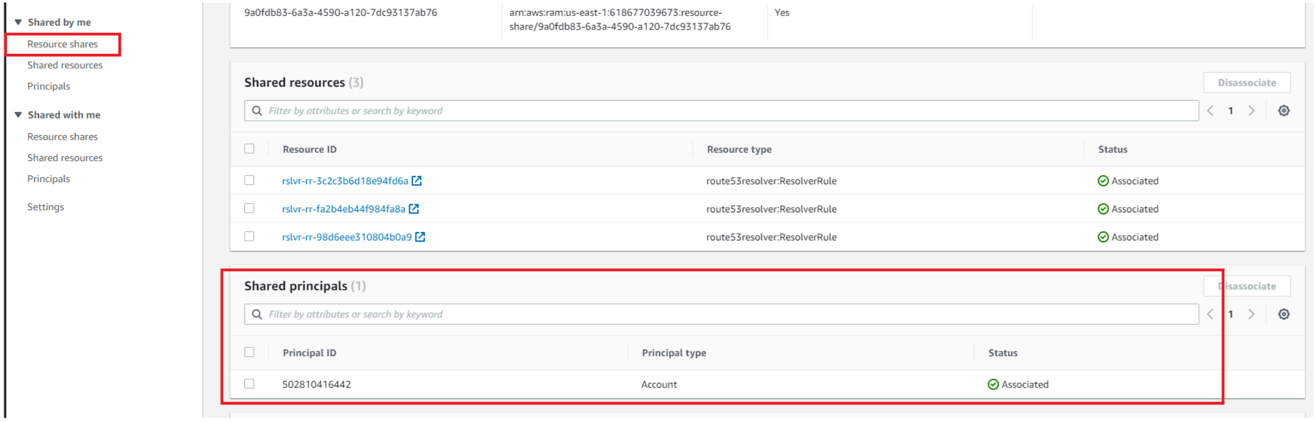


BusinessUnit	CloudPlatform
SupportMail	dl-tech-cloudfactory-foundationsacceleration@bhp.com
Env	Prd
SolutionName	CoreAccounts
Name	it-ausy-cor-obe-001
PO	4508680966

Rules (4)

Name	ID	Status	Outbound endpoint	Type	Domain name
it-ausy-cor-obe-001-rule-apac-ent-bhp	rslvr-rr-79...	Compl...	rslvr-out-207d79015cde40...	Forward	apac.ent.bhpbilliton.net.
it-ausy-cor-obe-001-rule-bhp-com	rslvr-rr-88...	Compl...	rslvr-out-207d79015cde40...	Forward	bhp.com.
it-ausy-cor-obe-001-rule-ent-bhpbillit	rslvr-rr-f4...	Compl...	rslvr-out-207d79015cde40...	Forward	ent.bhpbilliton.net.
it-ausy-cor-obe-001-rule-10-in-addr-a	rslvr-rr-4c...	Compl...	rslvr-out-207d79015cde40...	Forward	10.in-addr.arpa.

3. Go to the RAM and verify if the spoke VPC is associated with the resolver rules via RAM.



9a0fdb83-6a3a-4590-a120-7dc93137ab76 | arn:aws:ram:us-east-1:618677039673:resource-share/9a0fdb83-6a3a-4590-a120-7dc93137ab76 | Yes

Shared resources (3)

Filter by attributes or search by keyword

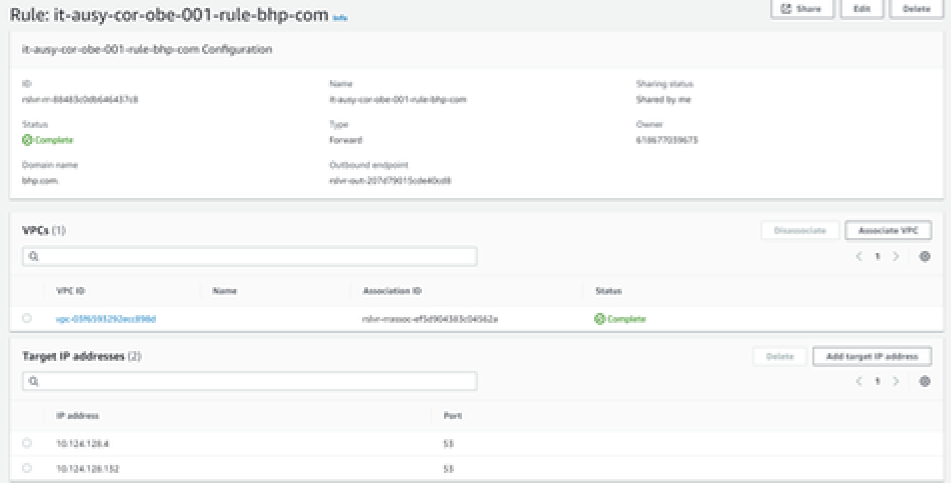
Resource ID	Resource type	Status
rslvr-rr-3c2c3b6d18e94fd6a	route53resolver:ResolverRule	Associated
rslvr-rr-fa2b4eb44f984fa8a	route53resolver:ResolverRule	Associated
rslvr-rr-98d6eee310804b0a9	route53resolver:ResolverRule	Associated

Shared principals (1)

Filter by attributes or search by keyword

Principal ID	Principal type	Status
502810416442	Account	Associated

4. Verify the Outbound Endpoint forwarding Rule should have an appropriate entry for alias bhp.com forwarding the rule to the appropriate resolver instance, currently: 10.124.128.4, 10.124.128.132 on Port 53.



Rule: it-ausy-cor-obe-001-rule-bhp-com

it-ausy-cor-obe-001-rule-bhp-com Configuration

ID rslvr-rr-88483c0db646437c8	Name it-ausy-cor-obe-001-rule-bhp-com	Sharing status Shared by me
Status Complete	Type Forward	Owner 618677039673
Domain name bhp.com	Outbound endpoint rslvr-out-207d79015cde40cd8	

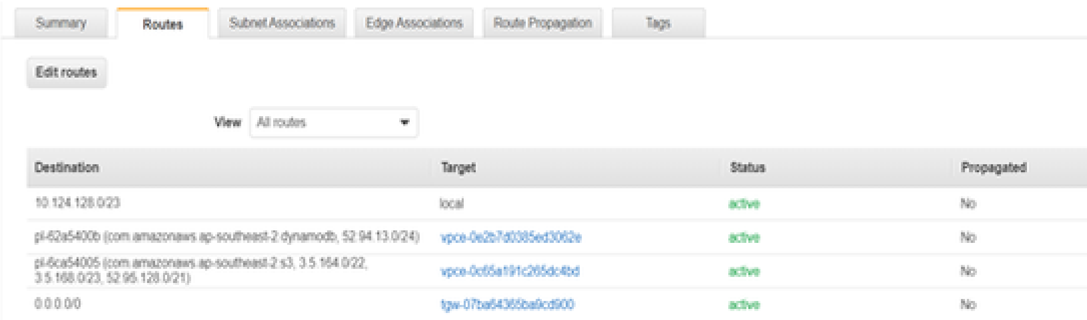
VPCs (1)

VPC ID	Name	Association ID	Status
vpc-03f6593292ecc898d		rslvr-rrassoc-ef5d904383c04562a	Complete

Target IP addresses (2)

IP address	Port
10.124.128.4	53
10.124.128.132	53

5. Verify that all the Target Instances(domain resolvers)are up and running. If anyone of them are corrupted , kindly reach out to AWS Squad to get them fixed .
6. The traffic generated from the spoke accounts will be following the route towards transit gateway, verify the VPC route tables should have appropriate route for the Transit gateway in the Spoke Account.

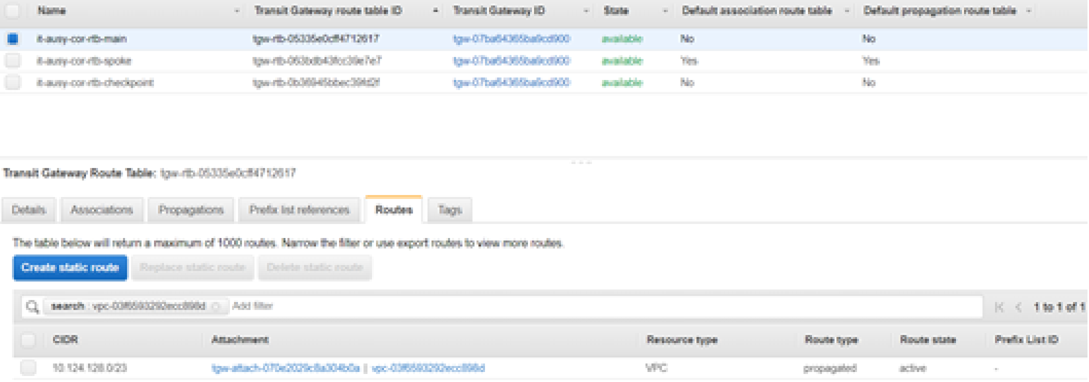


View: All routes

Destination	Target	Status	Propagated
10.124.128.0/23	local	active	No
pl-62a5400b (com.amazonaws.ap-southeast-2.dynamodb, 52.94.13.0/24)	vpce-0e2b7d0385ed3062e	active	No
pl-6ca54005 (com.amazonaws.ap-southeast-2.s3, 3.5.164.0/22, 3.5.168.0/23, 52.95.128.0/21)	vpce-0c65a191c265dc4bd	active	No
0.0.0.0/0	tgw-07ba64365ba9cd900	active	No

If in case no route present on VPC, reach out to AWS squad for updating the route table to point the default route to the TGW : https://gitlab.com/bhp-cloudfactory/aws-foundations/terraform-landscape-guardrails

7. Verify that the transit gateway route should have propagated routes for the VPC where the instances are being hosted . If no propagation routes present , go to the TGW route table , go to the propagation and add an entry for the destination CIDR as shown below.



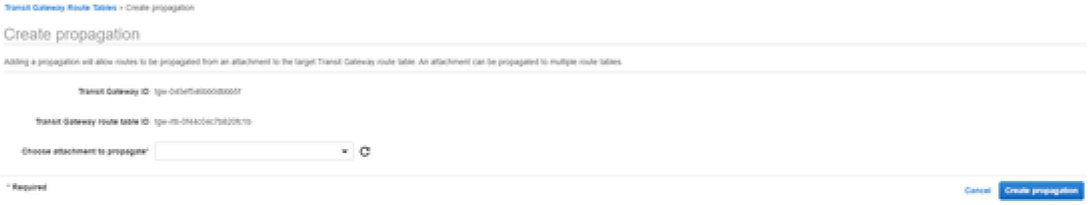
	Name	Transit Gateway route table ID	Transit Gateway ID	State	Default association route table	Default propagation route table
■	it-ausy-cor-rtb-main	tgw-rtb-05335e0cf84712617	tgw-07ba64365ba9cd900	available	No	No
□	it-ausy-cor-rtb-spoke	tgw-rtb-063bdb43fcc39e7e7	tgw-07ba64365ba9cd900	available	Yes	Yes
□	it-ausy-cor-rtb-checkpoint	tgw-rtb-0b36945bbec39fd2f	tgw-07ba64365ba9cd900	available	No	No

Transit Gateway Route Table: tgw-rtb-05335e0cf84712617

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

search : vpc-03f6593292ecc898d   Add filter   1 to 1 of 1

CIDR	Attachment	Resource type	Route type	Route state	Prefix List ID
10.124.128.0/23	tgw-attach-070e2029c8a304b0a | vpc-03f6593292ecc898d	VPC	propagated	active	-



Transit Gateway Route Tables > Create propagation

Create propagation

Adding a propagation will allow routes to be propagated from an attachment to the target Transit Gateway route table. An attachment can be propagated to multiple route tables.

Transit Gateway ID [illegible]

Transit Gateway route table ID [illegible]

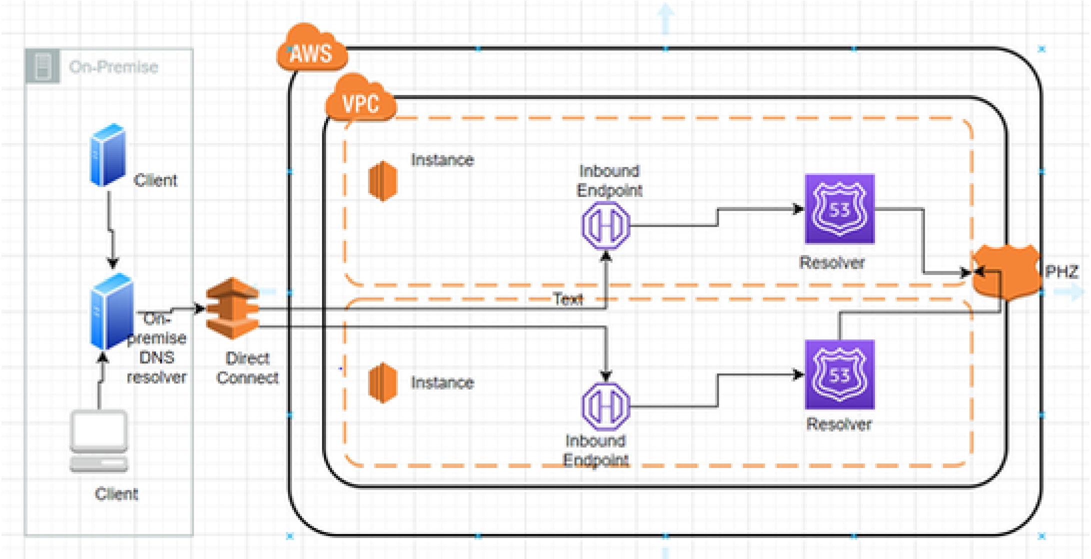
Choose attachment to propagate*

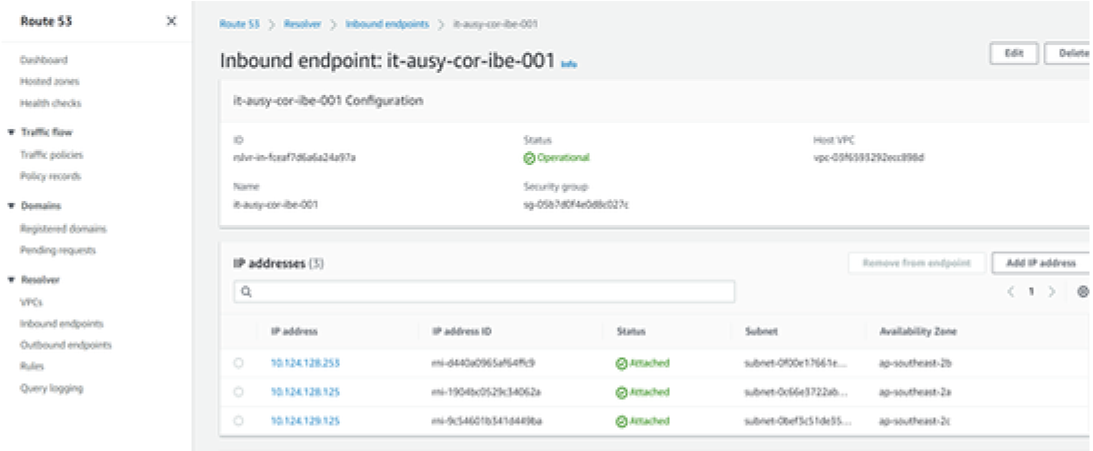
* Required

8. In the event of any New Spoke Account into picture, please use the terraform code to share the inbound and outbound resolvers across the new Spoke account .

SOP for Queries generated from On-premise:

Any DNS query generated from On-premise will be following Direct Connect path to reach out to the inbound endpoint resolvers for the query. The Inbound Endpoints are configured across 3 subnets as shown below:





Route 53 > Resolver > Inbound endpoints > it-ausy-cor-ibe-001

Inbound endpoint: it-ausy-cor-ibe-001 Info

it-ausy-cor-ibe-001 Configuration

ID rslvr-in-fceaf7d6a6a24a97a	Status Operational	Host VPC vpc-05f6593292ecc898d
Name it-ausy-cor-ibe-001	Security group sg-05b7d0f4e0d8c027c	

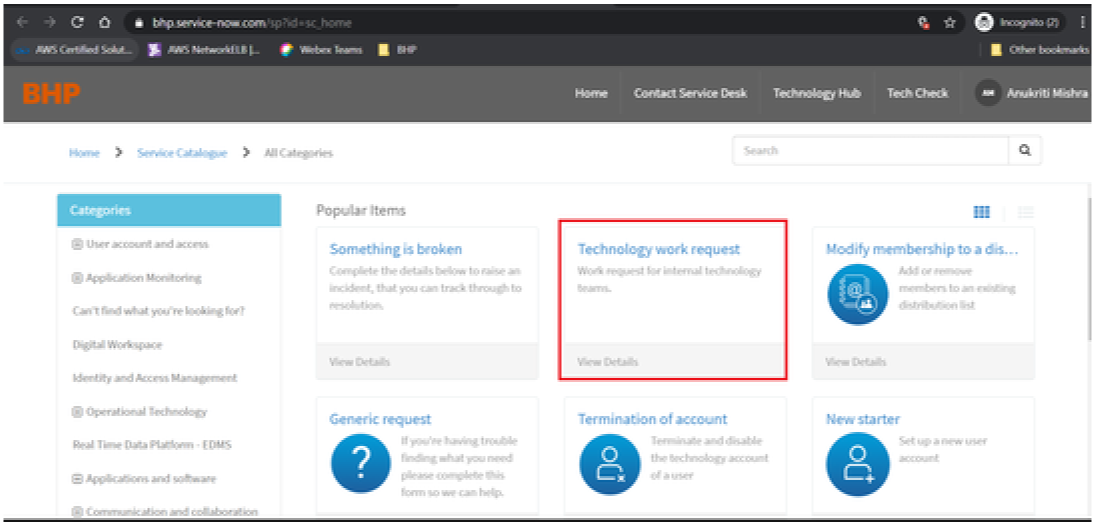
IP addresses (3)

	IP address	IP address ID	Status	Subnet	Availability Zone
○	10.124.128.253	eni-d440a0965af64ffc9	Attached	subnet-0f00e17661e...	ap-southeast-2b
○	10.124.128.125	eni-1904bc0529c34062a	Attached	subnet-0c66e3722ab...	ap-southeast-2a
○	10.124.129.125	eni-9c54601b341d449ba	Attached	subnet-0bef5c51de55...	ap-southeast-2c

To troubleshoot:

1. Verify the IPs are associated with the Inbound Endpoint
2. Verify that the on-premise resolvers are configured to forward the DNS queries to the AWS inbound endpoint resolvers. You can contact the on-premise DNS team on: bhp_dns@infosys.com.
3. Please raise a request using the below path and assign it to on-premise DNS team.

   SNEXT# Service Catalogue>Technical >Technology work request



Something is broken
Complete the details below to raise an incident, that you can track through to resolution.

Technology work request
Work request for internal technology teams.

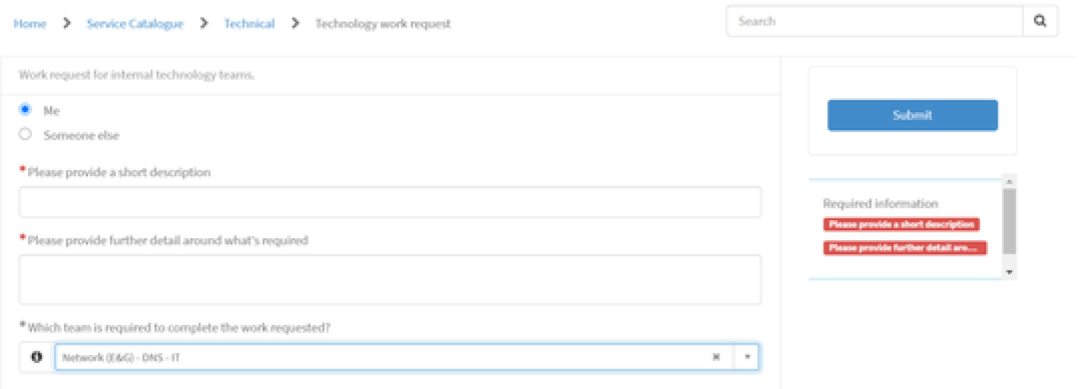
Modify membership to a dis...
Add or remove members to an existing distribution list

Generic request
If you're having trouble finding what you need please complete this form so we can help.

Termination of account
Terminate and disable the technology account of a user

New starter
Set up a new user account

4. Enter the description and details of the request and add “Network (E&G) - DNS - IT” as the team to complete the request.



Work request for internal technology teams.

● Me
○ Someone else

*Please provide a short description

*Please provide further detail around what's required

*Which team is required to complete the work requested?
Network (E&G) - DNS - IT