



Contents

1. Public Clo	oud Support	4
1.1. Disco	over Public Cloud Resources	6
1.1.1.	AWS Supported Networking Objects	7
1.1.2.	Azure Supported Networking Objects	9
1.2. Map	Public Cloud Resources	11
1.2.1.	AWS Network Tree	13
1.2.1.1.	VPC Reachability Context Map	14
1.2.2.	Azure Network Tree	15
1.2.2.1.	Virtual Network Context Map	18
1.2.2.2.	Subnet Context Map	18
1.2.2.3.	Region Context Map	19
1.2.2.4.	Azure to On-premise Network Context Map	20
1.2.2.5.	Virtual Hub Context Map	21
1.3. Appli	cation Path for Hybrid and Multi-cloud	21
1.3.1.	AWS Application Path Deep Dive	22
1.3.1.1.	AWS On-Prem Connection via Direct Connect	25
1.3.1.2.	Transit Gateway Reference Architecture	26
1.3.1.3.	Virtual Appliance	27
1.3.1.4.	VPC Endpoint and Private Link	28
1.3.1.5.	Application View (NLB/ELB)	29
1.3.1.6.	AWS Lambda Support / Serverless Support	30
1.3.2.	Azure Application Path Deep Dive	31
1.3.2.1.	Traffic Cross Azure Cloud and On-Premises Scenario	32
1.3.2.2.	Hub-Spoke Typical Network Scenarios	33
1.3.2.3.	Virtual Network (VNet) Connection Scenarios	34
1.3.2.4.	Azure Firewall Scenarios	36

	1.3.2.5.	Azure Load Balancer Scenarios	38
	1.3.2.6.	Azure Virtual WAN Network Scenarios	40
	1.3.2.7.	Virtual Appliance Scenarios	42
	.3.3.	Path across Accounts (AWS) and across Tenants/Subscriptions (Azure)	43
	.3.4.	Multi-Cloud Support	45
	1.3.4.1.	Public Cloud Exchange via Cloud Exchange Provider Cloud	45
	1.3.4.2.	Public Cloud communicate via IPSec Tunnels provided by cloud Virtual Appliances	46
1.4	. SPOC	G with Cloud Native Management Tools	47
	1.4.1.	SPOG with AWS Cloud Infrastructure Data	49
	1.4.1.1.	Resource Links and Account Info	49
	1.4.1.2.	Infrastructure View for Resources	50
	1.4.1.3.	Cloud Interconnect BGP Design	51
	.4.2.	SPOG with AWS CloudWatch	51
	1.4.2.1.	CloudWatch Basic Statistics	51
1.5	. SPOC	G with 3rd Party Cloud Management Tools	52
	1.5.1.	Datadog - AWS/Azure Monitoring Metrics	52
	1.5.2.	Splunk – VPC Security Group Check Log	53
1.6	. Runb	book Automation for Public Cloud	53
	1.6.1.	AWS - Troubleshoot General VPC Info	54
	.6.2.	AWS - Troubleshoot Transit Gateway Connectivity Issue	. 54

1. Public Cloud Support

As more and more IT workloads are being moved to the public cloud, operating the public cloud environment becomes a very changeling task for IT specialists. Even if the automation and agility during the provisioning process have been greatly improved, it is not the same when it comes to the manageability of the pubic cloud environment. The main challenges of managing public cloud consists of the following aspects:

- Lack of visibility: agile provision of cloud resources makes visibility difficult using the traditional manual method.
- **Huge number of accounts and subscriptions**: to comply with the security requirements, you may have huge number of accounts and subscriptions that used by different teams, managing all resources scattered in all these accounts and subscriptions bring huge management burden to the team when it comes to the troubleshooting cloud issues.
- **Multi-cloud and hybrid-cloud environments**: East-West Traffic supporting key application often traverse physical data center, SDN data center and public cloud. You may also have different public cloud providers to prevent vendor lock-in. As a result, a lot of organizations bring multiple public cloud providers into their production use and you will need to understand different cloud provider's uniqueness.
- **Collaboration within different teams and customers**: as the application that traverses through your network may involves multiple teams: network team, security team, cloud team server team and application team. When problem occurs, you may need to involve all the related teams together to figure out the root cause.

The need to have the visibility into the public cloud becomes very critical. In the R10 version we have built the support for AWS and Azure and the support consists of the following areas:

- **Auto Discovery:** with NetBrain's auto discovery function, NetBrain is able to discover public cloud resources and update the data periodically by leveraging the benchmark function.
- **Review network data and config with dynamic mapping**: like the way we do for traditional network and SDN network, we use API to access the public cloud environment and provide the data model which you can easily build the map based on the data model. The system has the ability to periodically retrieves the data from public cloud providers and update the data model accordingly.
- **Map application dependency across end-to-end network**: with the ability to build the data model for public cloud, SDN, SD-WAN, and also the traditional network, NetBrain is able to provide you the path analysis function across the entire network. NetBrain can check the routing table/security group/network ACL for all the networking objects along the path and display the checking result details.
- SPOG access through cloud-native and 3rd party cloud management tools: NetBrain has the ability to use Data View Template to display the cloud infrastructure data from AWS API, display the cloud monitoring data from AWS Cloud Watch and Azure monitoring, and also we can integrate with any of your cloud monitoring tools, Datadog, Splunk, Dynatrace for example, to overlay the monitoring metrics/logging information on the NetBrain map.
- **Automate Troubleshooting with Runbook**: The support for Runbook Automation is also expanded to Runbook Automation natively, with the support for public cloud, you are able to build different Runbooks according to your public cloud troubleshooting scenarios and can leverage the Automation within NetBrain's entire automation reference workflow.

With all these functions built for public cloud, operating public cloud network which consisting hundreds of even thousands of public cloud account becomes easier. The reference workflow for the hybrid/multi-cloud

network remains the same to give you unified workflow for the entire network. We'll use the following diagram to help you understand the workflow of using NetBrain to troubleshoot the ticket in your hybrid/multi-cloud environment:



- **Tickets Creation**: when a ticket is created in ServiceNow or Remedy, it can send the event to NetBrain system for integration.
- **Triggered Automation**: Upon receiving the event, NetBrain system can take the input (device name, source and destination IP addresses of your traffic flow) to create the map for the problem area, the similar concepts can be applied to hybrid/multi-cloud environment, NetBrain is able to map the entire network work hence it will help you gain the visibility of the entire network. Runbook automation is also supported in cloud environment and the automation can be used to analyze the hypothesis of the root cause in real time.
- Interactive Automation: the map created during the event and also the runbook analysis results can be leveraged by different teams (network team, cloud security team, application team) to collaborate and analyze the problem. NetBrain can help you troubleshoot the problem with the following functions:
 - **Data View Template**: you can leverage DVT to view the cloud monitoring information and also the metrics from other cloud management systems, such as Datadog, Splunk.
 - **Runbook Analysis**: you can leverage different Runbooks to execute different tasks according to your public cloud architecture and different use cases.
 - Data Comparation: since NetBrain captures valuable historical data of your cloud environment, you can compare the data in historical security groups/route tables/Network ACLs etc.
 - **Incident Portal/Function portal**: you can use the portal to share the findings with other teams who don't have access to the NetBrain environment.
- **Problem resolution and Post-mortem/post-change:** After the problem is resolved, you can create the Runbook to share the troubleshooting knowledge so next time when a similar problem happens, the root cause can be identified much quicker.

1.1. Discover Public Cloud Resources

To discover the public cloud resources, you will need to have the related API access to public cloud providers. The general steps for setting public cloud access are as follows:

1. **Setting up API access**: you will need to use either key-based access or role-based access method to discover public cloud resources.

Start Page Discover × API Ser	rver Manager $~ imes$			_
		Edit External API Server		×
Total Items: 37 + Add API Server				
API Source Type 🔺	Server Name	* Server Name:	AWS_Lab_Account_747895045325	
ACI MSO	MSO	Description:	The Lab account that has configured transit VPC	
Amazon AWS	AWS_Lab_Account_74789504			
Amazon AWS	AWS_Lab_Account_07011356	* API Source Type:	Amazon AWS	\sim
Amazon AWS	AWS Lab			
Amazon AWS	070113567925	* Access Method:	Key-based Access	\sim
Amazon AWS	747895045325	* Endpoint(Account ID):	Key-based Access	
Amazon AWS	dev-account-alpha		Role-based Access	
Amazon AWS	dev-account-digit	* Access Key ID:	AKIA24IQEXTGT3VEWB73	
Amazon AWS	dev-account-alpha-wrong	* Secret Access Key:		
Amazon AWS	dev-account-alpha-xxxx	* Front Server:	nethrainfc2024/102 168 20 24)	V
Amazon AWS	dev-account-yyyy	Tonesciven		•
Amazon AWS	Intuit TGW uswast-?	Advanced		

2. **Discover Public Cloud resources:** run the discovery function with the specified accounts to discover the public cloud resources.

Start Page Discover ×										
Discover			View His	storical Result: Select						
Discover Devices via SNMP/CLI Network Settings										
Method: () Discover via Seed Routers 🔿 Scan IP Range	4	Access Mode: SNMP and SS	H/Telnet 🗸 🚯 Disco	very Depth: 30						
IP/Hostname: e.g: 10.10.10.1; NY_R1	Select AP	1 Servers			-	_	_	-	_	
Discover Devices via API + Select API Servers Unselect All	ltems i	Found: 20 out of 36 + Add /	API Server 🗌 Show Selecte	d Items Only		Amazon AWS	v	Search		٩
API Servers: AWS_Lab_Account_747895045325 AWS_Lab_Acc	Ξ	API Source Type	Server Name	EndPoints	Description		Username	From	t Server	
		Amazon AWS	AWS_Lab_Account_74789	747895045325	The Lab acc	ount that has		netb	irainfs2924(192.1	68.29.24
		Amazon AWS	AWS_Lab_Account_07011	070113567925				netb	irainfs2924(192.1	68.29.24
	Z	Amazon AWS	AWS Lab	041444721655				netb	irainfs2924(192.1	68.29.24
		Amazon AWS	070113567925	070113567925				awsi	windowsfs1(172.1	6.102.9
		Amazon AWS	747895045325	747895045325	role based	discovery		8W5\	windowsfs1(172.1	6.102.9
		Amazon AWS	dev-account-alpha	netbrain-ie-nonprod				awsv	windowsfs1(172.1	16.102.9

3. **Setting up benchmark tasks**: you will need to set up benchmark tasks to retrieve the public cloud resources periodically.

Task Name: Basic System Benchmark	Description: Default	system benchmark task			
Frequency Device Scope	Retrieve Live Data	CLI Commands	Additional Operations a	after Benchmark	Plugins Summary
Select Device		Select external AP	l servers to retrieve data of S	DN nodes	
All Devices O Device Group	⊖ Site	Total Items: 4		All API Source Types 🗸	Search Q
Router(10)		API Source 1	Type Server Name	EndPoints	Description
•		Amazon AW	S AWS_Lab_Ac	count_7478 747895045325	The Lab account t
End System(137)		Amazon AW	S AWS_Lab_Ac	count_0701 070113567925	
💋 Firewall(6)		Amazon AW	S AWS Lab	041444721655	
Cloud(9)		Microsoft A:	zure Azure	85914d98-0e74	1-495f-988
L3 Switch(3)					
Exclude Device Groups: 028					

For the complete instruction on how to set up the API access and discover the public cloud resources, please refer to the following document:

- AWS Quick Setup Guide
- Azure Quick Setup Guide

NetBrain's discovery and benchmark functions can periodically capture the public cloud configuration status and update the data model accordingly.

At current stage, the AWS support mainly focuses on the networking objects and the pertaining objects. The following is a complete list of all supported networking objects:

- <u>AWS Supported Networking Objects</u>
- <u>Azure Supported Networking Objects</u>

1.1.1.AWS Supported Networking Objects

ITEMS	SUPPORTED TECHNOLOGY DETAILS	ΜΑΡ	TOPOLOGY	PATH
VPC	 Security Group Network ACL ENI Interface details per VPC VPC Sharing across Multiple Accounts VPC Route Table Ingress Routing 	Yes	Yes	Yes
VPC PEERING	VPC Peering within Same AccountsCross Account VPC Peering	Yes	Yes	Yes
INTERNET GATEWAY	Private to Public IP Mapping Table	Yes	Yes	Yes

VIRTUAL PRIVATE GATEWAY	 Virtual Route Table (based on NetBrain's unique algorithm) Cloudhub function Site-2-Site VPN details 	Yes	Yes	Yes
ELB (ALB/NLB)	 Target Group IP/Instance as targets Listener Table 	Yes	Yes	Yes
NAT GATEWAY	ENI interfaces provisioned for VPCs	Yes	Yes	Yes
AWS DIRECT CONNECT (DX ROUTER SUPPORT)	 Virtual Route Table for DX Router Virtual Interfaces details Private virtual interface Transit virtual interface Traffic engineering (As Path prepend, local preference for BPG community). DX Connection details LAG details 	Yes	Yes	Yes
DIRECT CONNECT GATEWAY	 Virtual Route Table Allowed Prefix for VGW/TGW Cross Account association to VGW/TGW 	Yes	Yes	Yes
TRANSIT GATEWAY	 Transit Gateway attachments Transit Gateway route tables Transit Gateway associations Transit Gateway propagation Transit Gateway peering ENI interfaces provisioned for VPCs Transit Gateway sharing for VPC attachments 	Yes	Yes	Yes
EC2 INSTANCE	EC2 Data DetailsNetwork Interface DetailsSecurity Groups	Yes	Yes	Yes
NETWORK VIRTUAL APPLIANCES	Relationship to EC2 hostsEC2 details	Yes	Yes	Yes
(ASAV, CSR1000V, VEDGE ETC.)				
VPC ENDPOINT (GATEWAY ENDPOINT)		Yes		
VPC ENDPOINT (INTERFACE ENDPOINT) - PRIVATELINK	ENI interfaces provisioned for VPCs	Yes		

1.1.2.Azure Supported Networking Objects

ITEMS	SUPPORTED TECHNOLOGY	MAP	TOPOLOGY	PATH	UNSUPPORTED
	DETAILS				FEATURES
VIRTUAL MACHINE (VM)	 VNIC Interface details VM Device details Network Security Group (Interface Level) 	Yes	Yes	Yes	
VIRTUAL NETWORK (VNET)	 Network Security Group (Subnet Level) Application Security Group Across Multiple Accounts Across Multiple subscription User Defined Route Table (UDR) VNet Peering Table VNIC Effective Route Table Virtual Route Table (based on NetBrain's algorithm) 	Yes	Yes	Yes	
VNET PEERING	 VNet Peering within the same subscription VNet Peering across Multiple subscriptions VNet Peering within the same Account/Tenant VNet Peering across Multiple Account/Tenant 	Yes	Yes	Yes	
VIRTUAL NETWORK GATEWAY (VPN/EXPRESSROUTE GATWAY)	 VPN/ExpressRoute Gateway device details Virtual Route Table (based on NetBrain's algorithm) 	Yes	Yes	Yes	
AZURE LOAD BALANCER (PUBLIC)	 Device details Inbound NAT Rules Table Load Balancing Rule Table Outbound Rules Table Virtual Route Table (based on NetBrain's algorithm) 	Yes	Yes	Yes	

AZURE LOAD BALANCER (INTERNAL)	• • •	Device details Inbound NAT Rules Table Load Balancing Rule Table Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes		
NAT GATEWAY	•	Device details NAT Table Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes		
AZURE FIREWALL	• • •	Device details Network Rule Collection Table DNAT Rule Collection Table Application Rule Collection Table Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes		
APPLICATION GATEWAY	• • • •	Device details Listener Table Rules Talbe Http Setting Table Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	NO	•	OSI Layer 7 Path (URL/Http/Https)
NETWORK VIRTUAL APPLIANCES (ASAV, CSR1000V, VEDGE ETC.)	•	Relationship to Virtual Machine host Virtual Machine details	Yes	Yes	Yes		
INTERNET CLOUD	•	Device details	Yes	Yes	Yes	•	NCT route table Path Originated from Internet
MPLS CLOUD	•	Device details Virtual Route Table (based on NetBrain's algorithm)	Yes	Yes	Yes		
PRIVATE LINK			No	No	No		
PUBLIC SERVICE			No	No	No		

1.2. Map Public Cloud Resources

After your public cloud and on-prem networks are discovered, you will be able to view the related public cloud resources. There are different ways to view the related public cloud resources:

- **Network Pane**: network page gives you the resource view for a specific technology, whether that is your traditional network, SDN network or public cloud environment, we will cover more details in the following chapters.
- **Global Search**: through the global search, you can search for specific public objects with their name/ID, as the name and ID are searchable in the global search, this will help you quickly identify where the resource is located at and create maps based on the search results.
 - Search by IP

Net3	Brain (17	72.16.101.75		× (x	Path
Search i	Results(3)				~ ≡ − ∓ >
🗸 🗌 De	vice (1/1)				
ć	&2*`\n/&(i-	-094cb7 Site:	Unassigned		
1	Interfaces 21	L3 Neighbors 0	L2 Neighbors		
A۱	WS EC2 Instand	ce			
Μ	gmt IP: <mark>172.16</mark> .	.101.75			
In	terface (1 mato (eni-02da172	:hed) edb75815f0) <mark>172.</mark>	16.101.75/28 2 Neight	oors	
- Netw	ork Context (1/	1)			
t-in Cate 5_Lab_A 12.16.10	egory: AWS, Vie .ccount_747895 11.64/28 \EC2: 8 P Table (1/1)	ew: Network Centr 5045325 (7478950 &2*`\n/& 172.16	ric View\View by Account 145325)\Region: us-east- 5.101.75	s I\VPC: Spoke1 172.16.101.(0/24\Subnet: qa-simulation- Launch One-IP Table
	Switch Port	DNS Name	Description	Data Source	Data Retrieved
		0.2+`\p/0/; 00		Device Interface	12/21/2020 6.05.17 DM
		QZ. 11/Q(I-09		Device interface	12/21/2020, 0:03:17 PM

o Search by ID

net3rain (i-094cb7dd8645541	12c		X	🔶 Path	
Search Results(4)					~	≣ — Ŧ ×
 Device (1/1) 						
وی &2*`\n/ 1 Interfaces AWS EC2 Inst	/&(<mark>-094cb7</mark> Site: 2 L3 Neighbors 0 :ance	Unassigned L2 Neighbors				
▼ Site (1/1)						
My Netwo Device Cou 1 Matched	unt: 119 Devices: &2*`\n/&(-094cb7dd8645541	<mark>2c</mark>)			
Built-in Category: Physi Device Category/End Sy	ical Network, View: D ystem\&2*`\n/&(<i>i-09</i>	evice Type 4cb7dd86455412c)				
▼ One-IP Table (1/1)				Launch (One-IP Table
IP Address	LAN Segment	MAC Address	Vendor	Switch Port	DNS Name	Description
172.16.101.75	172.16.101.64/28	027C.A097.BE67			&2*`\n/&(<mark>i-09</mark> .	

• **Map**: another way to find your public cloud resources is through the extend neighbor function, if you have your On-Prem devices connected to the public cloud environment, you can use the extend neighbor function to extend the neighbors.



1.2.1.AWS Network Tree

In the example below, you will have access to all of your accounts discovered in a single view:

Below is one hieratical view for the AWS resources:

Account > Region > VPC > Subnet

You will also find the other networking objects as listed based on their hierarchy.

- Transit gateway is listed under regions as transit gateway is a reginal service that resides within a certain region.
- AWS direct connect gateways are logical components that can interconnect VGW and TGW from different regions, so they are listed under account.
- AWS direct connect router is a physical device that resides in certain direct connect locations, so it's listed under region.



From the details pane you can view the details for each object and the hyperlink will take you to the AWS console directly.

Context Maps	Device Details
Property Interfa	ces
Name:	awsAWS-Support Test(i-00f7ccd3f1bcf96ca)
Instance ID:	i-00f7ccd3f1bcf96ca 🐴
AMI ID:	ami-0d5d9d301c853a04a
Instance Type:	t2.micro
Launch Time:	2020-12-16 12:00:34+00:00
Owner:	747895045325 🐴
Availability Zone:	us-east-2a
Platform:	linux/Unix
Private DNS:	ip-172-26-0-46.us-east-2.compute.internal
Private IP:	172.26.0.46
Public DNS (IPv4):	
Security Groups:	sg-00808211878a9b791 🖞
Source/dest. check	c true
Instance state:	running
Subnet ID:	subnet-01fb350af825a53f5 🖉
VPC ID:	vpc-08248fb7d26b2feca 🖒
Tags:	
Name:	awsAWS-Support Test

You can use the search function to view all matched results.

Network		G	₽
Category	View		
AWS 🗸	Network Centric View\	\vee	≡
spoke		×	
61 Results			
WPC: Spoke1 172.16.101 AWS_Lab_Account_74789	.0/24 5045325 (747895045325)\Region	: us-e	ast-
VPC: Spoke2 172.16.102 AWS_Lab_Account_74789	. 0/24 5045325 (747895045325)\Region	: us-e	ast-
VPC: Spoke3 172.16.105 AWS_Lab_Account_74789	.0/24 5045325 (747895045325)\Region	: us-e	ast-
WPC: Spoke4 172.16.144 AWS_Lab_Account_74789	.0/24 5045325 (747895045325)\Region	: us-e	ast-
VPC: Spoke5 172.16.155 AWS_Lab_Account_74789	i. 0/24 5045325 (747895045325)\Region	: us-e	ast-

1.2.1.1. VPC Reachability Context Map

The following context map is to help you understand the reachability from VPC via the transit gateway.



1.2.2.Azure Network Tree

In the example below, you will have access to all of your tenants discovered in a single view:

Below is an example of hieratical view for the Azure resources:

- Level 0: Tenant
 - Level 1: Subscription
 - Level 2: Region
 - Level 3: VNet
 - Level 4: Virtual Network Distributed Router
 - Level 4: Subnet
 - Level 5: Virtual machines
 - Level 4: VPN Gateway
 - Level 4: Express Route Gateway
 - Level 4: Application Gateway
 - Level 4: Azure Load Balancer(Internal)
 - Level 4: NAT Gateway
 - Level 4: Azure Firewall
 - Level 3: MSEE
 - Level 3: Azure Load Balancer (Public)
 - Level 3: Unassigned NAT Gateway
 - Level 2: Virtual WAN
 - level 3: Virtual WAN Hub
 - level 4: VPN Gateway for vHub
 - level 4: Express Route Gateway for vHub
 - level 4: Azure Firewall

You can find the network objects listed in this hierarchy tree.

- The virtual network as a parent node to include sub node virtual network distributed router and subnet.
 - The virtual network distributed router is a NetBrain conceptual compoent to simulate virtual network as a network object to build relationship with other resources that belong to this virtual network.

- The virtual machine is listed under subnet that belong to this virtual network.
- The VPN gateway, ExpressRoute gateway, application gateway, Azure load balancer (internal), NAT gateway, Azure firewall are listed under virtual network which they belong to.
- The MSEE is simulated as a network object to connect with virtual network and on premise network, so it is listed under region.
- The Azure load balancer (public) might not belong to a certain virtual network, so it is listed under region.
- If the NAT gateway does not belong to any virtual network, it will be listed under region as an unassigned NAT gateway.
- The Virtual WAN is used to connect networks within different region, so it is listed under subscription. The virtual WAN hub is listed under virtual WAN, and the VPN gateway for vhub, ExpressRoute gateway for vhub and Azure firewall are listed under virtual WAN hub

Category		View		
Azure	\sim	Network View	\sim	≡
Find			۹	
🖌 📶 Azure Multi S	ubscription(1)			
🖌 🔶 NetBrain T	echnologies In	nc(2)		
🖌 📍 NetBraii	n Azure subscr	ription(8)		
þ 🌰 Cana	da Central(11)			
þ 🌰 Centr	al US(4)			
þ 🌰 East l	JS(14)			
🖌 🌰 East l	JS 2(3)			
⊿ o VN	et: North-VNE	T(North-RG1)(073e6f	45)(VirtualNetwo	D
<>	VNet Router: N	North-VNET-router(N	orth-RG1)(073e6	5f
<•>	Subnet: Gatev	vaySubnet(North-RG	1)(073e6f45)(Sub)
▲ ^(*)	Subnet: North	-subnet1(North-RG1)(073e6f45)(Subr	٦
	👤 VM: North-	VNET-VM1(North-RG	1)(073e6f45)(Virt	:u
	VPN Gateway:	North-VPN-Gateway	(North-RG1)(073	3e
⊳	et: Spoke-VNE	T-2(Spoke-VNET-2)(0	73e6f45)(Virtual	N
📶 Un	attached NAT	gateways		
þ 🌰 West	US(4)			
þ 🌰 West	US 2(4)			
⊳ 😵 Virtua	al WAN: HC-Vir	tal_WAN(HC)(073e6f	45)(VirtualWAN)((1)
⊳ 😨 Virtua	al WAN: VWAN	-TO-BUR(East-RG1)(0)73e6f45)(Virtual	
⊳ 💁 West ⊳ 😨 Virtua ⊳ 😨 Virtua	US 2(4) al WAN: HC-Vir al WAN: VWAN	tal_WAN(HC)(073e6f -TO-BUR(East-RG1)(0	45)(VirtualWAN)(73e6f45)(Virtual	(1)

From the details pane you can view the details for each object and the hyperlink will take you to the Azure console directly.

ontext Maps D	evice Details	
roperty Interfaces		
Resource Group:	North-RG1 🖆	
Location:	eastus2	
Subscription:	NetBrain Azure subscription 省	
Subscription ID:	073e6f45-d1ae-40fe-93af-88231d2377bd	
SKU:	VpnGw1	
Gateway Type:	Vpn	
Virtual Network:	North-VNET(North-RG1)(073e6f45)(VirtualNet	
Public IP Address:	40.65.218.132. 52.147.167.55(North-VPN-GW	

You can use the search function to view all matched results.

Network		SŦX
Tategory	View	
Azure	∨ Network V	′iew ∨ ≡
east		×
3 Results		
🍊 East US		A
Azure Multi Sub	scription\NetBrain Tech	nologies Inc\NetBrain A
👍 East US 2		
Azure Multi Sub	scription\NetBrain Tech	nologies Inc\NetBrain A
A Minter NAVA NI - X0A		
Azure Multi Sub	vAN-TO-BOR(<mark>Edst</mark> -RGT)(0	nologies Inc\NetBrain A
, Lai e maiti bab	Senption iterbrain reen	
🚸 Azure Load Bala	ancer(Public): TestPublicI	LB(<mark>East</mark> -RG1)(073e6f
Azure Multi Sub	scription\NetBrain Tech	nologies Inc\NetBrain A
💻 MSEE: Bur-Netb	ond(Primary)(<mark>East</mark> -RG1)(073e6f45)(MSEE)
Azure Multi Sub	scription\NetBrain Tech	nologies Inc\NetBrain A
🛤 MSEE: Bur-Netb	ond(Secondary)(<mark>East</mark> -RG	51)(073e6f45)(MSEE)
Azure Multi Sub	scription\NetBrain Tech	nologies Inc\NetBrain A
Whet East PG1	wpet(Fast_RG1)(073e6f4	5)(VirtualNetwork)
Azure Multi Sub	scription/NetBrain Tech	

1.2.2.1. Virtual Network Context Map

The following context map is to help you understand the relationship of resources within the same virtual network. The virtual machine will not be mapped by default due to its massive number.



1.2.2.2. Subnet Context Map

The following context map is to help you understand the virtual machine connecting to the same subnet within the virtual network.



1.2.2.3. Region Context Map

The region context map provides the following information:

• Displaying all virtual network and its resources relationship within the same region.



• Displaying the management view for the selected region.



1.2.2.4. Azure to On-premise Network Context Map

The following context maps demonstrate the relationship between Azure and on-promise network.

• VPN gateway context map demonstrate the IPsec VPN connection between VPN gateway and onpremise edge device.

Network	G Ŧ X	»	📮 🗆 🖌 🔊 Stencils Instant Qapp Dashbo
Category View Azure V Find Network View	✓ Ξ		
Low VNet: AVIControllervnet787(AVI-Controller)(0 Low VNet: DC1-Vnet1(DC1)(073e6f45)(VirtualNetw Low VNet: DC2-Vnet1(DC2)(073e6f45)(VirtualNetw Low VNet: East-RG1-vnet(East-RG1)(073e6f45)(VirtualNetw Low VNet: East-Test-VNET(East-RG1)(073e6f45)(VirtualNetw) Low VNet: East-Test-VNET(East-RG1)(073e6f45)(VirtualNetw) Low VNet: East-Test-VNET(East-RG1)(073e6f45)(VirtualNetw) Low VNet: East-Test-VNET(East-RG1)(073e6f45)(VirtualNetw) Low VNet: East-VNET(Fast-RG1)(073e6f45)(VirtualNetw) Low VNet: East-VNET(Fast-RG1)(073e6f45)(VirtualNetw)	73e6f45)(ork)(3) ork)(2) ualNetwo tualNetw INetwork)	VRF:_for /subscript	172.17.11.128/26 East-VNETI(East-RG1)(073e6f45)(Virt ions/073e6f45-d1ae-40fe-93af-88231
 When EuserWhen (East-NET1-router(East-RG1)) When Router: East-VNET1-router(East-RG1)) Subnet: ASAV-Subnet1(East-RG1)(073e6f43) Subnet: ASAV-Subnet3(East-RG1)(073e6f43) Subnet: ASAV-Subnet4(East-RG1)(073e6f43) Subnet: Azav-BastionSubnet(East-RG1)(073e6f43) Subnet: CastewaySubnet(East-RG1)(073e6f43) Subnet: CastewaySubnet(East-RG1)(073e6f43) Subnet: Subnet1 (East-RG1)(073e6f43) Subnet: Subnet1 (East-RG1)(073e6f43) Subnet: Subnet1 (East-RG1)(073e6f43) Ven Gateway: East-VPN-GWEast-RG1)(073e6f43) 	(073e6f45)(Subnet)()(Subnet)()(Subnet)()(Subnet)(3e6f45)(S 45)(Subne net)(172.1		East-VNET1-router(East-RG
 VFN GateWay: EdstVPN-GV(EdstRd 1/0/) Express Route: East-Express-GW(East-Rd1 Azure Load Balancer(Private): EdstPstLB Azure Load Balancer(Private): TestLBStance NAT Gateway: TestNATGW(East-RG1)(073e 	(073e6f4 East-RG1) ard(East 6f45)(Nat	BUR12-LAB-FW1/act 192.168.0.25 Cisco ASA Firewall	

• ExpressRoute gateway context map demonstrate the connection between ExpressRoute gateway and on-promise network via MSEE.



1.2.2.5. Virtual Hub Context Map

In this context map will demonstrate the resources used to connect to on-promise network, the connected virtual network within different region(s), and other connected virtual hub(s) via MS backbone.



1.3. Application Path for Hybrid and Multi-cloud

NetBrain's path function has been extended to the public cloud in v10. The system supports end-to-end path calculation in hybrid/multi-cloud environment, and you can analyze the traffic flow between two endpoints. To start a path calculation:

1. Click **Path** on the search bar.



- 2. Enter the IP address of endpoint A in the **Source** field and the IP address of endpoint B in the **Destination** field.
- 3. By default, the system calculates two-way paths. To change the path direction, select the \subseteq icon or the icon.
- 4. The related gateways will be auto identified. If a device has multiple gateways, you can select the desired one from the **Gateway** list.

Click **Path** to view the diagrammed path on the map with a detailed summary log (in the left pane).



Create Application Path

Your application may consist of web tier/application tier/database tier, so you probably want to create a application to include multiple paths for different paths. In this case, you can use NetBrain's path browser function to create applications and include the corresponding paths.

For more information about how to use the application manager to create and manage paths, please refer to the online help: <u>Organizing and Verifying Paths in Application Manager</u>

~	Application Mar	nager													
									+ N	lew Applicati	on +New F	Path 🔒 Impoi	rt 🔒 Export 🗸	Ġ Refre	esh
Total	Entries: 2 Applications, 2	2 Paths			Filtere	d by: Resu	lt 🛨 Con	npare with Go	lden 👻 (Compare wi	th Last 🛛 👻	Search	(Res	set
	Application	Path	Source	0	Source Po	Source De	Destina 🚯	Destinatio	Destinatio	Group (Protocol	Result	Result Cat	History	≡
	Email Service														
		U Client	172.24.1	0		172.24.10	172.25.16.6		172.25.16.6		IPv4	N/A		0	
		U POP T	10.10.1.5	2		10.10.1.52	10.10.13.1		10.10.13.1		IPv4	N/A		0	
	Untitled Application														
		No Path													
	4														÷
0 Suc	ceeded 0 Failed	0 Not Change	ed From G	older	0 Changed	From Golden	0 Not Cl	hanged From L	.ast 0 Chang	ed From Las	i i				

1.3.1.AWS Application Path Deep Dive

A VPC consists IP range, subnets, and it may also contain cloud-native networking services as NAT gateway, IGW, VGW etc., NetBrain will create a AWS VPC router for each VPC to simulate the routing/security check function for this VPC. Subnet is visualized in NetBrain's dynamic map via the concept called LAN media. From the dynamic map, you can view different networking objects and how they are connected. VPC peering is also supported- the corresponding peering ID will be visualized in the dynamic map.



Path calculation will render the path log containing the related routing and security check details.



The link of each object will direct you to the AWS console, where you can view more information about the object or make desired changes.

Next hop is Spoke3(vpc-0cc7817f50c71a1ee)	aws
Check Output Security Group (Path Failed)	
 Retrieving Security Group Table (sg-0875d0ffa87925745) from Spoke3(vpc- 0cc7817f50c71a1ee) 	Sign in
View Sec <mark>urity Group Table(<u>ac-007540/ft87925745</u>) in AWS Console [2] Owner Account Login:747985045325 [2] No matching entries were found in Security GroupTable sg-0875d0ffa87925745 [2] </mark>	Root user Account owner that performs tasks requiring unrestricted access. Learn more
Failed to match security group rules Check Output Source and Destination (Has Source IP) Source and Destination Check is enabled	IAM user User within an account that performs daily tasks. Learn more
Check Source and Destination successfully, has source IP	Account ID (12 digits) or account alias
	Next
	New to AWS?
	Create a new AWS account

Path Example 1 - EC2 to Internet

The following path diagram demonstrates how a EC2 instance in a public subnet accesses the internet directly.



Path Example 2 - NAT Gateway

The following path diagram demonstrates how NetBrain can help you identify the traffic flow when a EC2 instance tries to access the internet via NAT gateway. From the path log, you will be able to better understand how the NAT works.



1.3.1.1. AWS On-Prem Connection via Direct Connect

There are a lot of different architectures for connections between your on-prem network to the public cloud resources. NetBrain supports all of these popular deployment types as previously illustrated.

The key of supporting end-to-end path for public cloud environment is really to understand all the routing & security checks across the entire network. You may know AWS natively doesn't provide the routing tables for the following networking objects:

- Virtual private gateway
- Direct connect gateway
- Direct connect router

NetBrain has invented a unique algorithm to build the virtual routing table based on the topology info and route advertisement it captures for the surrounding devices. These information are also very useful for you to understand the potential routing problems:

- Neighbor relationship table: this table includes neighbors device information which are recognized as directly connected neighbors.
- Route dependency table: this table includes devices with routes advertised to the current device.
- AWS virtual routing table: this is the virtual route table NetBrain calculate to be used in path calculation. We also strictly follow AWS's route selection priority rules to choose the best path available if there's multiple paths to the destination.

AWS Vi	irtual Route Ta	able of BGP-Transit	-NB-VGW(vgw-01fc8	88164f72433e2)						×
Data	Source: Cur	rrent Baseline	✓ Execution 1	lime: 12/22/2020, 2	2:56:00 PM			ø	Φ	4
NCT:	AWS Virtua	l Route 🗸	Subname:for	transit-vpc(vpc-0824	48fb ∨	S	earch			Q
Des	tination	Туре	ALG	Local Preferenc	AS Path	DX Location	Out Interface	Originato	or	
172	.16.101.0/	Direct Connect	В				_to_To-ATT-Net	Spoke1(vpc-03	
172	2.16.8.0/22	Direct Connect	В		64665 64665 6		_to_To-ATT-Net	ustb0013	306/ac	:
172	2.16.8.0/22	Direct Connect	В		64666 64665		_to_To-ATT-Net	ustb0013	307/act	:

Below is an example demonstrating path from an EC2 instance to an end system in the on-prem network. This is a transit VPC architecture where we build the IPSEC tunnel between the customer gateway with the CSR1000v sitting in the transit VPC. The underlay communication is achieved via the direct connections via ATT Netbound.

You will be able to understand the overlay path for the IPSec tunnels as well as the underlay path going through the direct connect router and direct connect gateway to the virtual private gateway of the transit VPC.



1.3.1.2. Transit Gateway Reference Architecture

Transit Gateway is used to enable VPC-to-VPC communication or/and on-prem to cloud communication. The above scenarios are fully supported by NetBrain.



1.3.1.3. Virtual Appliance

Virtual appliance can be used in the public cloud environment (CSR1000v, ASAv, vedge etc.). The relevant deployment scenarios (including the application path across these virtual appliances) are fully supported by NetBrain.

In order to successfully establish a path going through the virtual appliances, CLI access to the virtual appliances is required in addition to accessing the AWS API (to retrieve the EC2 instance information).

The example below demonstrates how the ingress routing works with the ASAv configured within VPC to inspect the incoming traffic.



1.3.1.4. VPC Endpoint and Private Link

AWS Public Services are fully supported in current release, including the gateway endpoints and the interface endpoints.

😰 Amazon Dynamo DB	AWS	Amazon Dyna
🚑 Amazon EC2	AWS	Amazon EC2
🕞 Amazon S3	AWS	Amazon S3
🚳 Amazon SageMaker Notebook	AWS	Amazon SageM

The following path shows how an EC2 instance communicates with the Amazon S3 service via the gateway endpoints. You can verify the traffic flow from NetBrain by entering the source IP, destination URL and NetBrain can confirm that the traffic goes through the Gateway endpoints instead of using the internet gateway.



The following diagram demonstrates the private-link support. From the right hand side, the application owner shares the application with others via the private link service. NetBrain can map the private link services accordingly. When you calculate the path from the EC2 instance to the private link service, NetBrain can further visualize the entire path as well as the EC2 instances sitting behind the NLB.



1.3.1.5. Application View (NLB/ELB)

Path Example- Application Load Balancer

Note: At the current stage we don't support layer 7 inspection details. Only layer 4 inspection is performed.



Path Example- Network Load Balancer

The following one shows the path goes through a network load balancer. You will find the EC2 instances behind the load balancer has been mapped out as expected.



1.3.1.6. AWS Lambda Support / Serverless Support

The current release only provides limited support for serverless application dues to NetBrain's current focus on Networking Objects. When launching a serverless application, AWS will automatically generate ENI interfaces to communicate with other VPC resources. You will need to configure the correct security group and ensure it can work properly. You can leverage NetBrain's path function to check the application flow from ENI interfaces to destinations.

The following path demonstrates the path from an ENI interface provisioned by AWS for serverless application to the AWS S3.



1.3.2.Azure Application Path Deep Dive

For a detailed list of Azure Networking Supported Functions, please refer to:

Azure Networking Supported Function List

NetBrain has invented the concept of Virtual Network Distributed Router (VNet Router) with various resources and features to simplify the Azure Cloud network connections inside and outside the Virtual Network. The resources/features include:

- Routing information such as User Defined Route and Virtual Route Table for Virtual Network.
- Security rule information such as Network/Application Security Group rule in subnet/interface level.
- Peering information for various VNet peering details.
- Network Interface (NIC) Effective Route Table information



NetBrain has invented the unique algorithm to build the virtual routing table based on the topology info and route advertisement it captures for the surrounding devices. This information is very useful in the context of reviewing the potential routing problems:

- Neighbor Relationship Table: This table includes the neighbor device information which are recognized as directly connected neighbors.
- Route Dependency Table: This table includes the devices with routes advertised to the current device.
- Virtual Routing Table: This is the virtual route table to be used in path calculation. We strictly follow Azure's route selection priority rules to choose the best path available if there's multiple paths to the destination.

ure Virtual Route Table	of Spoke-VNET3-Router(U	S-West-RG)(073e6f45)(Virtu	ualNetworkDistributedRoute	er)						
ata Source: Current	Baseline V Exe	cution Time: 1/29/2021, 2:2	29:44 PM					8	÷	[
CT: Azure Virtual Ro	out V Subname:	_for_GW_172.17.16.1	\sim				Search			(
Destination	Type *	ALG	Local Preference	AS Path	Out Interface	Next Hop IP Address	Next Hop Device	Originator		
10.0.0/8	Default							Spoke-VNET3-R	outer(U	J
100.64.0.0/10	Default							Spoke-VNET3-R	outer(U	J
192.168.0.0/16	Default							Spoke-VNET3-R	outer(U	J
0.0.0.0/0	Default				_to_Internet_Cloud		_for_Azure_Internet_Cl	Spoke-VNET3-R	outer(U	J
172.16.101.0/24	ExpressRoute	в		8030	_to_East-VNET1(East-R		East-VNET1-Router(Eas	Bur-Netbond(Pri	mary)((
172.17.18.0/24	ExpressRoute	в		65515 65520 65520 e	_to_East-VNET1(East-R		East-VNET1-Router(Eas	Canada-Central-	VNET1	
172.17.19.0/24	ExpressRoute	в		65515	_to_East-VNET1(East-R		East-VNET1-Router(Eas	East-Test-VNET-I	Router((
172.17.251.0/30	ExpressRoute	в		65515	_to_East-VNET1(East-R		East-VNET1-Router(Eas	Bur-Netbond(Pri	mary)((
172.17.253.0/24	ExpressRoute	в		65515	_to_East-VNET1(East-R		East-VNET1-Router(Eas	East-VHUB(East-	RG1)((0.
172.18.1.0/24	ExpressRoute	в		65515	_to_East-VNET1(East-R		East-VNET1-Router(Eas	2nd-Sub-Vnet-R	outer(2	2
172.16.101.0/24	ExpressRoute	в		8030	_to_East-VNET1(East-R		East-VNET1-Router(Eas	Bur-Netbond(Se	condar.	r
172.17.251.0/30	ExpressRoute	в		65515	_to_East-VNET1(East-R		East-VNET1-Router(Eas	Bur-Netbond(Se	condar.	r
3.8.8.8/32	UDR	U				172.17.16.68		/subscriptions/0	73e6f4	ŧ
72.17.14.0/30	UDR	U				172.17.16.68		/subscriptions/0	73e6f4	ŧ
172.16.101.0/24	UDR	U				172.17.16.68		/subscriptions/0	73e6f4	ŧ
172.17.17.0/24	UDR	U			_to_East-VNET1(East-R	172.17.15.20		/subscriptions/0	73e6f4	ŧ
172.17.13.0/24	UDR	U			_to_East-VNET1(East-R	172.17.15.20		/subscriptions/0	73e6f4	ŧ
172.17.11.0/24	VNet Global Peering	в			_to_East-VNET1(East-R		East-VNET1-Router(Eas	East-VNET1-Rou	ter(Eas	s
172.17.15.0/24	VNet Global Peering	в			_to_East-VNET1(East-R		East-VNET1-Router(Eas	East-VNET1-Rou	ter(Eas	s
172.17.11.190/32	VPN	в			_to_East-VNET1(East-R		East-VNET1-Router(Eas	East-VPN-GW(Ea	ast-RG1	1
72.17.14.0/24	VPN	в			_to_East-VNET1(East-R		East-VNET1-Router(Eas	West-Hub-VNET-	Router	r
172.17.22.132/32	VPN	в			_to_East-VNET1(East-R		East-VNET1-Router(Eas	North-VPN-Gate	way(No	o
172.17.22.133/32	VPN	в			_to_East-VNET1(East-R		East-VNET1-Router(Eas	North-VPN-Gate	way(No	o
172.17.22.0/24	VPN	в			_to_East-VNET1(East-R		East-VNET1-Router(Eas	North-VNET-Rou	ter(Nor	r

1.3.2.1. Traffic Cross Azure Cloud and On-Premises Scenario

There are several ways to connect an on-premises network to an Azure Virtual Network (VNet).

• VPN connection

A VPN gateway is a type of virtual network gateway that sends encrypted traffic between an Azure virtual network and an on-premises location. The encrypted traffic goes over the public Internet.

NetBrain VPN connection path sample:



• ExpressRoute connection

ExpressRoute connections use a private, dedicated connection through a third-party connectivity provider. The private connection extends your on-premises network into Azure.

The figure below shows the traffic path between Azure Cloud and On-Premise via two ExpressRoute Circuits connections provisioned by ATT Netbound. Microsoft Enterprise edge (MSEE) devices are sitting at the edge of Azure Cloud.





1.3.2.2. Hub-Spoke Typical Network Scenarios

A hub-spoke network topology is a way to isolate workloads while sharing services such as identity and security. The hub is a virtual network (VNet) in Azure that acts as a central point of connectivity to your onpremises network. The spokes are VNets that peer with the hub. Shared services are deployed in the hub, while individual workloads are deployed as spokes.

NetBrain can visualize the abstract cloud traffic path between different Azure nodes and enhance your efficiency of troubleshooting cloud network issues. The figure below shows the Hub provides a secure network boundary using Network Virtual Appliance (NVA) such as Cisco ASA by checking all inbound and outbound network traffic and passing only the traffic that meets network security rules.

NetBrain Hub-Spoke Network path sample:



1.3.2.3. Virtual Network (VNet) Connection Scenarios

There are several options to connect Virtual Networks (VNet). You can connect virtual networks to each other with virtual network peering or using the VNet-to-VNet connection type.

• VNet Peering

These virtual networks can be in the same region or different regions (also known as Global VNet peering). Once virtual networks are peered, resources in both virtual networks are able to communicate with each other, with the same latency and bandwidth as if the resources were in the same virtual network.

NetBrain provides various Virtual Network information on the MAP such as VNet Peering Table, from which you can view the peering details for current Virtual Network.

Virtual Network Available data table:



			1.8						
Azure VNet Peering Table of East-V	NET1-Router(East-RG1)(073	e6f45)(VirtualNetworkDistributedRouter)							×
Data Source: Current Baseline	✓ Execution Time	n 1/29/2021, 2:18:31 PM					8	Ф Ъ	D.
NCT: Azure VNet Peerin V	V Subname: 'Global'	\vee				Search			Q
Peering Name	Peering Status	Neighbor VNET ID	Allow Gateway Transit	Use Remote Gateways	Allow Forw	arded Traffic	Allow Virtual	Network A	cc
Hub-VNET-To-Spoke-VNET3	Connected	/subscriptions/073e6f45-d1ae-40fe-93af-8	Enabled	Disabled	Enabled		Enabled		
Hub-VNET-To-Spoke-VNET4	Connected	/subscriptions/073e6f45-d1ae-40fe-93af-8	Enabled	Disabled	Enabled		Enabled		
Hub-VNET-To-Spoke-VNET2	Connected	/subscriptions/073e6f45-d1ae-40fe-93af-8	Enabled	Disabled	Enabled		Enabled		
Hub-VNET-To-Spoke-VNET1	Connected	/subscriptions/073e6f45-d1ae-40fe-93af-8	Enabled	Disabled	Enabled		Enabled		
EastVNetHub-to-Spoke5-sam	Connected	/subscriptions/073e6f45-d1ae-40fe-93af-8	Enabled	Disabled	Disabled		Enabled		
TenantA-To-B	Connected	/subscriptions/f34a04c1-fe04-453e-83d1-9	Disabled	Disabled	Disabled		Enabled		
Global_Peer_Test	Connected	/subscriptions/eb48417e-0d31-46b0-acd4	Disabled	Disabled	Enabled		Enabled		

The VNet peering path sample:



• VNet-to-VNet Connection

You can connect virtual networks by using the VNet-to-VNet connection type. The virtual networks can be in the same or different regions, and from the same or different subscriptions. When connecting VNets from different subscriptions, the subscriptions do not need to be associated with the same Active Directory tenant.

NetBrain has invented the proprieties Virtual Route Table based on Azure routing policies and rules, which can provide you an easy way to understand cloud routing details instead of struggling with abstract cloud routing strategies.

Azure Virtual Route Tab	le of East-VPN-GW(East	-RG1)(073e6f45)(Virtu	alNetworkGateway)							
Data Source: Curre	nt Baseline V	Execution Time: 1/29,	/2021, 2:29:44 PM					Ø	Φ	
Destination		ALG	Local Preference	AS Path	Out Interface	Next Hop IP Addres.	Next Hop Device	Originator		4
172.17.14.0/24	VPN	в			_to_West-VPN-GW(C		West-VPN-GW(Cen	- West-Hub-V	NET-Ro.	
172.17.22.132/32	VPN	в			_to_West-VPN-GW(C		West-VPN-GW(Cen	North-VPN-	Gatewa.	
172.17.22.133/32	VPN	в			_to_West-VPN-GW(C		West-VPN-GW(Cen	North-VPN-	Gatewa.	
172.17.22.0/24	VPN	в			_to_West-VPN-GW(C		West-VPN-GW(Cen	North-VNET	-Router.	
172.17.14.190/32	VPN	в			_to_West-VPN-GW(C		West-VPN-GW(Cen	West-VPN-0	W(Cent	
172.16.8.0/22	VPN	в			_Tunnel_outside_52	104.207.208.66	BUR12-LAB-FW1	BUR12-LAB	FW1	
172.17.254.0/30	VPN	В			_Tunnel_outside_52	104.207.208.66	BUR12-LAB-FW1	BUR12-LAB	-FW1	

The VNet-to-VNet connection path sample is shown as below:



1.3.2.4. Azure Firewall Scenarios

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

NetBrain uses various tables to visualize different Azure Firewall Rule information, and performs lookup across all rules to calculate the path following Azure rule check policy.



Azure Firewall Networ	k Rule Collection T	able of Spoke-3-Fi	ewall(US-West-RG)(073e6f45)(Azurel	Firewall)									×
Data Source: Curr	ent Baseline	V Execution	Time: 1/29/2021, 2	18:40 PM								đ٥.	•	D.
NCT: Azure Firewa	all Net V	Subname: Glob	al'	\sim						Searc	h			Q
Rule Collection	Rule Collection	Group Priority	Collection Priori	Action	Inherited From	Rule Name	Source Type	Source	Protocol	Destination Po	r Destination Typ.	Destinat	ion	
Deny8081	DefaultNetwor	200	220	Deny		Deny8081_16	IP address	172.17.16.39	TCP	8081	IP address	8.8.8.8		
Deny8081	DefaultNetwor	200	220	Deny		Deny8081_16.6	IP address	172.17.16.6	TCP	8081	IP address	8.8.8.8		
Deny8082	DefaultNetwor	200	190	Deny		Deny8082	IP address	172.17.16.6	ТСР	8082	IP address	0.0.0.0		
AzurePathTest	DefaultNetwor	200	200	Allow		Allow-DNS	IP address	172.17.16.39	UDP	53	IP address	209.244.0).3,20	
AzurePathTest	DefaultNetwor	200	200	Allow		AllowSSH	IP address	*	TCP	22	IP address	8.8.8.8		
AzurePathTest	DefaultNetwor	200	200	Allow		AllowICMP	IP address	*	ICMP	*	IP address	*		
AzurePathTest	DefaultNetwor	200	200	Allow		SPK3toCanCent	IP address	172.17.16.32/28	Any	*	IP address	172.17.18	3.0/24	
AzurePathTest	DefaultNetwor	200	200	Allow		Allow8080	IP address	172.17.16.39	Any	8080	IP address	8.8.8.8		
AzurePathTest	DefaultNetwor	200	200	Allow		Allow8080-to1	IP address	172.17.16.39	TCP	8080	IP address	172.17.14	1.0/24	
AzurePathTest	DefaultNetwor	200	200	Allow		Allow8080-to8	IP address	172.17.16.6	TCP	8080	IP address	8.8.8.8		
AzurePathTest	DefaultNetwor	200	200	Allow		Allow16.6_ori	IP address	172.17.16.6/32	TCP	8081-8082	IP address	0.0.0.0		
AzurePathTest	DefaultNetwor	200	200	Allow		Allow16.6_des	IP address	0.0.0.0	TCP	8081	IP address	172.17.16	6/32	
AzurePathTest	DefaultNetwor	200	200	Allow		IP_Group_Test	IP Group	172.17.21.0/2	TCP	8888	IP address	8.8.8.8		
AzurePathTest	DefaultNetwor	200	200	Allow		Allow8080-to1	IP address	172.17.16.39,	TCP	8083	IP address	172.17.14	1.0/24	
AzurePathTest	DefaultNetwor	200	200	Allow		Allow8080-to1	IP address	172.17.16.6	TCP	8084	IP address	172.17.14	1.0/24	
AzurePathTest	DefaultNetwor	200	200	Allow		AllowAWSto-17	IP address	172.17.16.6	Any	*	IP address	172.16.10)1.0/24	

The Azure Firewall path sample:



1.3.2.5. Azure Load Balancer Scenarios

Azure Load Balancer operates at layer four of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load balancing rules. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

NetBrain supports both Public/Internal Load Balancer path and various Load Balancer features, including:

- Azure LoadBalancer Backend Pools Table
- Azure LoadBalancer Inbound NAT Rules Table
- Azure LoadBalancer Load Balancing Rules Table
- Azure LoadBalancer Outbound Rules Table
- Azure LoadBalancer Virtual Route Table

Azure Load Balancer available data table:



Azure Load Balancer Load Balancing Rules Table:

Azure LoadBalan	cer Load Balancing Rules Tal	ble of VNET-1-Pri	vate-Load-Balance	er(Spoke-VNET-1)	(073e6f45)(Load	Balancer)									×
Data Source:	Current Baseline V	Execution Tin	ne: 1/29/2021, 2:	18:48 PM								8	÷	.	ß
NCT: Azure L	.oadBalance v Subr	name: 'Global'		\sim							Search				Q
Name	Load Balancing Rule	IP Version	Frontend IP A	HA Ports	Protocol	Port	Backend Port	Backend Pool	Health Probe	Session Persi	Idle Timeout	TCP Reset	Floatin	ig IP	
TestHAPorts	TestHAPorts (ALL/0)	IPv4	LoadBalancer	Yes	All	0	0	VNET-1-Priva	HTTP (HTTP:	None	4	Disabled	Disabled		
AzurePathTe	AzurePathTest-NoHA (T	IPv4	AzurePathTes	No	Тср	8080	8081	AzurePathTest	HTTP (HTTP:	None	4	Enabled	Disabled		

Azure Load Balancer Backend Pools Table:

1	zure LoadBalancer Backend Pools Table of VNET-1-Private-Loa	d-Balancer(Spoke-VNET-1)(073e6f45)(LoadBalancer)							
	Data Source: Current Baseline V Execution Time	: 1/29/2021, 2:18;48 PM				5	Φ	•	D.
	NCT: Azure LoadBalance V Subname: AzurePath	Test v			Search				Q
	Virtual Machine	Virtual Machine Status	Network Interface	Private IP Addr	ess				
	VNET-1-Private-Endpoint-3	VM deallocated	vnet-1-private-endpo455	172.17.12.39					
	VNET-1-Public-Endpoint-4	VM deallocated	vnet-1-public-endpoi401	172.17.12.10					

The Azure Load Balancer path sample:





NetBrain supports the following global transit connectivity paths of Azure Virtual WAN. The letters in parentheses corresponds to the letters in the diagram above.

- Branch-to-VNet (a)
- Branch-to-branch (b)
 - ExpressRoute Global Reach and Virtual WAN
- Remote User-to-VNet (c)
- Remote User-to-branch (d)
- VNet-to-VNet (e)
- Branch-to-hub-hub-to-Branch (f)
- Branch-to-hub-hub-to-VNet (g)
- VNet-to-hub-hub-to-VNet (h)

NetBrain can provide key information including Virtual Hub Effective Route Table and Virtual Route Table.



Virtual Hub Available Data Table:

Virtual Hub Virtual Route Table:

	Azure Virtual Route Tal	ble of East-VHUB(East	-RG1)(073e6f45)(VirtualHub)									
	Data Source: Curre	ent Baseline 🗸 🗸	Execution Time: 1/29/202	1, 2:29:42 PM						6	Ф	D.
£1	NCT: Azure Virtual	Rout V Sub	name:for_2nd-Sub-Vnet(:	2nd-Sub 🗸					Search			Q
L	Destination	Туре	ALG	Local Preference	AS Path	Out Interface	Next Hop IP Address	Next Ho	p Device	Originator		
	172.16.8.0/22	ExpressRoute	в		12076 8030 65101 64665	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	BUR12-LAB-FW1		
١.	10.4.0.0/16	ExpressRoute	в		12076 12076	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	testVNET-Router	(Spoke	
	172.17.11.0/24	ExpressRoute	в		12076 12076	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	East-VNET1-Rout	er(East-	
L	172.17.12.0/24	ExpressRoute	в		12076 12076	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	Spoke-VNET-1-R	outer(Sp	p
L	172.17.13.0/24	ExpressRoute	в		12076 12076	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	Spoke-VNET-2-R	outer(Sp	p
	172.17.15.0/24	ExpressRoute	в		12076 12076	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	East-VNET1-Rout	er(East-	·
Ŀ.	172.17.16.0/24	ExpressRoute	в		12076 12076	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	Spoke-VNET3-Ro	uter(US	i
5	172.16.101.0/24	ExpressRoute	в		12076 8030	_GW_172.17.253.1	172.17.253.6/24	Bur-Netb	ond(Primary)(E	East-VHUB(East-	RG1)(07	7
it	172.17.18.0/24	VHub	в			_to_MS_Backbone		Canada-0	Central-Hub(Eas	Canada-Central-	/NET1-R	Ł
·21												

Virtual Hub Effective Route Table:

A	ure VHub Effective Route Table of East-	VHUB(East-RG1)(073e6f45)(VirtualHub)								
	Data Source: Current Baseline	V Execution Time: 1/29/2021, 2:18:42 PM					8	ф	•	D,
1	NCT: Azure VHub Effecti V S	Subname: 'Global' V				Search				٩
	Prefix	Next Hop Type	Next Hop	Origin	AS path					
	172.16.8.0/22	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-803	0-65101-64665				
	10.4.0.0/16	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-120	76				
	172.17.11.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-120	76				
	172.17.12.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-120	76				
	172.17.13.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-120	76				
	172.17.15.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-120	76				
	172.17.16.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-120	76				
	172.16.101.0/24	ExpressRoute	10.3.129.58	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b	12076-803	0				
	172.17.251.0/30	VPN	172.17.253.13	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b						
	172.17.18.0/24	Remote Hub	On-link	/subscriptions/073e6f45-d1ae-40fe-93af-88231d2377b						
	172.18.1.0/24	Virtual Network Connection	On-link							
	172.17.19.0/24	Virtual Network Connection	On-link							

The Azure Virtual WAN path sample is shown as below:



1.3.2.7. Virtual Appliance Scenarios

A Network Virtual Appliance (NVA) is typically used to control the flow of network traffic from a perimeter network, also known as a DMZ, to other networks or subnets.

The diagram below shows the NVA provides a secure network boundary by checking all inbound and outbound network traffic and passing only the traffic that meets network security rules.



1.3.3.Path across Accounts (AWS) and across Tenants/Subscriptions (Azure)

Enterprise customers may have a lot of AWS accounts and Azure subscriptions for data isolation. The application path may traverse multiple accounts/subscriptions. By setting API access to multiple accounts and subscriptions, NetBrain will be able to visualize the traffic path across multiple accounts as well as multiple subscriptions.

NetBrain can visualize the peering details if the crossing subscription/tenant is using VNet Peering.

_					1 / 3ª			
1	Azure VNet Peering Table of East-VNE	T1-Router(East-RG1)(073e6f45)(Virtu	ualNetworkDistributedRouter)					
-	Data Source: Current Baseline	V Execution Time: 1/29/2023	1, 2:18:31 PM				S 🕆 🍡	D.
(NCT: Azure VNet Peerin V	Subname: 'Global'	V			s	iearch	Q
	Peering Name	Peering Status	Neighbor VNET ID	Allow Gateway Transit	Use Remote Gateways	Allow Forwarded Traffic	Allow Virtual Network Access	
	Hub-VNET-To-Spoke-VNET3	Connected	/subscriptions/073e6f45-d1ae-40	Enabled	Disabled	Enabled	Enabled	
4	Hub-VNET-To-Spoke-VNET4	Connected	/subscriptions/073e6f45-d1ae-40	Enabled	Disabled	Enabled	Enabled	
e	Hub-VNET-To-Spoke-VNET2	Connected	/subscriptions/073e6f45-d1ae-40	Enabled	Disabled	Enabled	Enabled	
<i>a</i>	Hub-VNET-To-Spoke-VNET1	Connected	/subscriptions/073e6f45-d1ae-40	Enabled	Disabled	Enabled	Enabled	
2	EastVNetHub-to-Spoke5-samere	Connected	/subscriptions/073e6f45-d1ae-40	Enabled	Disabled	Disabled	Enabled	
	TenantA-To-B	Connected	/subscriptions/f34a04c1-fe04-45	Disabled	Disabled	Disabled	Enabled	
İ.	Global_Peer_Test	Connected	/subscriptions/eb48417e-0d31-4	Disabled	Disabled	Enabled	Enabled	
Ŀ								
Ł								
F								4

Azure crossing subscription path sample:



Azure crossing Tenant sample:



1.3.4.Multi-Cloud Support

You may have one or more public cloud providers, with NetBrain's support for multiple cloud providers, you will be able to get a complete view of your public cloud infrastructure as well as the traffic flow going through multiple public cloud providers.

Following is the typical multi-cloud application design patterns:

- Public Cloud Exchange via Cloud Exchange Provider Cloud
- Public Cloud communicate via IPSec Tunnels provided by cloud Virtual Appliances

1.3.4.1. Public Cloud Exchange via Cloud Exchange Provider Cloud

The following diagram depicts the typical dedicated cloud interconnect solution provided by different cloud providers. NetBrain is able to map the entire topology as well as the path going through multiple cloud providers.



After setting up the benchmark to retrieve the data successfully, NetBrain will be able to calculate the path across public clouds. The following diagram shows how an EC2 instance can communicate with the virtual machines sitting on Azure via AT&T Netbound.



1.3.4.2. Public Cloud communicate via IPSec Tunnels provided by cloud Virtual Appliances

You can also use the transit VPC architecture to build the IPSec VPN tunnel between different cloud providers so the traffic flow can go through transit VPCs.



1.4. SPOG with Cloud Native Management Tools

NetBrain's data view function gives you the ability to monitor various public data in NetBrain environment. This chapter will focus on explaining how NetBrain system manages to visualize the data from public cloud providers in its dynamic map. There are basically two kinds of data that can visualized by NetBrain:

- **Public Cloud Infrastructure Data**: this involves the basic information of cloud operational status, routing/security, tag information etc.
- **Cloud Monitoring Metrics**: this involves the monitoring metrics from the cloud native monitoring tools, such as AWS CloudWatch and Azure Monitoring. These metrics are usually data plane status that can be visualized in NetBrain maps.

In order to visualize the relevant data using DVT, you can leverage the following two types of data:

- **GDR Data:** GDR data is already available for use since this type of data is retrieved during the discovery/benchmark process.
- **API Parser Data:** By using the API parser, you can retrieve any data from public cloud provider.

Building Data View Template with Public Cloud GDR Data

Since NetBrain uses API to retrieve the data from AWS for the related networking objects, the system makes some of these data available for you to select when using the data view template. You can re-organize and select the data you want to use in data view template based on your specific needs.

In order to select these data, you need to select the branch type first and then click the **Select Built-in Data** option.

ENI Interface	5 🖪 Status	🧿 🖪 Subnet ID
	🌗 🖪 Availability Zone	Pescription
1	🗿 🖪 Mac Address	4 🖪 Source/dest. check
	?	3
▲ 1 Interface Highlights	▷ Define More	Select Built-in Data Select Parser Variable
		Add Text

The following screenshot demonstrates the data you can select for the elastic load balancer. The selectable data will vary according to the type of network object.

Name: AWS Load Balancer		Drill Down Actions: 0 Actions	Default Data Source: Current baseline	
Description:	S	upporting Variables: 0 Variables	Sample Picture: + Add Picture	
ch: ELB V (2 Branch Defined)	Branch Type: AWS Load Balancer (1 Inter	face types) () Bran	ch Filter Criteria: None	
			Select Built-in Data	×
+ Add Device N	lote ENI Interface	5 🖪 Status		e
\square		1 D Availability Zone	Select an interface property	
1 Device Highlights		Availability zone	Interface Property V Search	۹ .
		3 🖪 Mac Address	Attachment	
Hostname			Availability Zone	
		V	Description	
Availability Zones			Mac Address	
📀 🗉 Hosted zone	 1 Interface Highlights 	Define More	Source/dest. check	
			Status	
Via Creation time			Subnet ID	
😔 🗊 DNS name				
Define More				

Note: Since the selected data is retrieved from the GDR stored in MongoDB, when you apply the Data View including the AWS GDR data, these data is cached from the system and will be retrieved during the latest discover/benchmark process. The data presented is infrastructure data and rarely changes.

Building Data View Template with API Parser Data

To retrieve more types of data from AWS (e.g., live CloudWatch data), you will need to use the API parser to retrieve the data from AWS and then select respective Parser Variables. As the API parser data can be retrieved from live network with desired frequency, you can use this method to build your Data View Template if you need to pull the data from live.



Sample Data View Templates provided by NetBrain

NetBrain has built a lot of useful data view templates based on different use cases. We will go through some of these data view templates with the design intent. Please be aware that these data view templates are for reference purpose only. Thanks to the scalability of NetBrain platform, the function can be extended to any interested data.

1.4.1.SPOG with AWS Cloud Infrastructure Data

The following Data View Templates make it possible to visualize different types of AWS cloud infrastructure data in NetBrain dynamic map:

- <u>Resource Links and Account Info</u>
- Infrastructure View for Resources
- <u>Cloud Interconnect BGP Design</u>

1.4.1.1. Resource Links and Account Info

This data view template can visualize the account information for different networking objects and it provides the link to AWS management console.

Links are also available for resources such as ENI interfaces, security groups and network ACLs.

routerable	name: modified-TGW-Burlington(t accountid: 747855045325 (Sector) name: modified-TGW-Burlington(two-Col91f03edf14349) (Sector) 0 vWr.96th etrol	47a44aea79a) accountid: 747895045325 🕓 attachm routeTable: tgw-rtb-0fd3feead375641ee	en:: tgw-attach-0310:433b0998acad in networkAck: N/A in accountid: 747895045325 in to move Table N/A in accountid: 747895045325 in to move Table in modified-TGW-Burlin Variable: in route Table in aws route table in Transit Gateway Route Table	Iffied-TGW-Burlington(tgw-0cf09 Spol name: GM-1716-01110 GM-1716-01110 GM-1716-01110 GM-1716-01110 GM-1716-01110 GM-1716-01110 GM-1716-0110 GM-1716-00 GM-1716-00 GM-1716-00 GM-1716-00 GM-1716-00 GM-1716-00 GM-1716-00 GM-1716-00 GM-1706-00 GM-17
_	2.16.101.12			C.Sokerin
łyperlink -	Result 1			· · · · · · · · · · · · · · · · · · ·
\sim	s routeTable			
e Data	Golden Baseline Analysis: N/A Golden Baseline: Define			
	1 items			Compare
	routeTable	Time		
	tgw-rtb-0fd3feead375641ee	01/15/2021 10:53:33 AM (Map Data Time)		
a44aea79;				

1.4.1.2. Infrastructure View for Resources

This data view template can visualize the infrastructure information for different networking objects.



1.4.1.3. Cloud Interconnect BGP Design

This data view template can demonstrate the detailed information about your Cloud Interconnect design. It visualizes all AS number from AWS and the advertised route details of the customer's gateway devices.



1.4.2.SPOG with AWS CloudWatch

1.4.2.1. CloudWatch Basic Statistics

This data view template demonstrates the metrics retrieved from AWS CloudWatch. It currently includes the following information:

- EC2 status
- VGW Tunnel status
- Direct Connect Status per Physical Connection
- Direct Connect Status per Virtual Interface
- TGW entire status
- TGW status per Attachment
- ELB Status



1.5. SPOG with 3rd Party Cloud Management Tools

The ability to visualize data from 3rd Party cloud management tools enables NetBrain dynamic map to render a complete view of your cloud infrastructures. The integration with 3rd Party cloud management tools is highly customizable meaning NetBrain can be integrated with any cloud management tools to suit your specific needs. The following integrations are the SPOG solutions currently supported by NetBrain:

- Datadog AWS/Azure Monitoring Metrics
- <u>Splunk VPC Security Group Check Log</u>

1.5.1.Datadog - AWS/Azure Monitoring Metrics

The following data view demonstrates the integration with Datadog- the metrics are retrieved from the Datadog agents installed on EC2 instances. NetBrain can retrieve and demonstrate the following types of metrics through the data view template:

- system.cpu.user (5 min aveg double)
- system.mem.pct_usable (5 min aveg double)
- system.uptime (The last non-empty value of the 5 min int)
- system.net.packets_out.error (5 min aveg int)
- system.disk.free (5 min aveg int)
- system.io.r_s (5 min aveg int)
- system.net.packets_in.error (5 min aveg int)

NetBrain also provides a link to Datadog so you can easily switch to Datadog to explore more details.

DataDog-Agen CPU of User Space Physical RAM Uptime: Packet Tran	t-Haoran(i-00 Processe: 0.15% Fraction: 0.88 4452055 smitterror: 0	DataDog-Agent-Haoran(i-00 CPU of User Space Processes 0.15% (3 Physical RAM Proction: 0.83	Recommended Action (1)	×
0	Overflow Data Unit Free Disk Space: 8481989017bytes	Packet Transmit Errors: 0	Device: DataDog-Agent-Haor Variable: vsystem_cpu_user	
	IO Read Requests per Second: 0 Packet Receive Errors: 0			

1.5.2.Splunk – VPC Security Group Check Log

AWS CloudTrail is a service that allows you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. The integration with Spunk allows you to view change log of security groups/network ACL and much for VPCs during a specific period of time.



1.6. Runbook Automation for Public Cloud

Runbook Template can be used to help you understand the network design and also troubleshoot network problems based on certain scenarios. A lot of useful functions such as DVT, Qapp, Gapp and Compare can be wrapped into Runbook to accomplish your tasks.

The following are some of the sample Runbooks we have provided based on some Troubleshooting scenarios:

- <u>AWS Troubleshoot General VPC Info</u>
- <u>AWS Troubleshoot Transit Gateway Connectivity Issue</u>

1.6.1.AWS - Troubleshoot General VPC Info

This runbook can help you quickly identify important resource information for the devices on map, which includes:

- Path Application Path
- DVT [AWS] Resource Links and Account Info
- DVT [AWS] Infrastructure View for Resources
- DVT [AWS CloudWatch] Basic Stats
- Qapp Security Group
- Qapp Network ACL



1.6.2.AWS - Troubleshoot Transit Gateway Connectivity Issue

This runbook can help customers troubleshoot the transit gateway routing issue and understand the current deployment. This Runbook includes:

- Path Application Path
- DVT AWS basic stats DVT
- Qapp Map reachability from specific VPC
- Qapp Map reachability from specific TGW Route Table
- Compare Compare TGW NCT Tables (Attachment table/Route Table)

