



Contents

1.	AW	S API Access Overview	4
	1.1.	Key-based Access Overview	4
	1.2.	Role-based Access Overview	5
	1.3.	Combined Access Overview	7
2.	Set	ting Up Key-based Access	8
	2.1.	Creating AWS Access Policy in Amazon Console	8
	2.2.	Enabling Access to Your Amazon Account Using Key-based Access	. 11
	2.3.	Configuring NetBrain to Access AWS Using Key-based Access	. 13
3.	Set	ting Up Role-based Access	. 16
	3.1.	Creating AWS Access Policy and Role for Monitored Accounts	. 16
	3.2.	Configuring EC2 Role for NetBrain Front Server in AWS Gateway Account	. 19
	3.3.	Configuring NetBrain System	. 22
4.	Set	ting Up Combined Access	. 25
4	4.1.	Creating AWS Access Policy and Role for Monitored Accounts	. 26
4	4.2.	Creating Public/Secret Keys for Gateway Accounts	. 28
4	4.3.	Configuring NetBrain System	. 32
5.	Dis	covering AWS Network in NetBrain Domain	. 35
6.	Aut	o-Updating AWS Data in NetBrain through Benchmark	. 39
7.	Wo	rking with Multi-cloud Environment	. 42
8.	Usi	ng REST API to Manage AWS Data	.44
1	8.1.	Integration with AWS Organization	. 46
9.	Арр	pendix	. 51
ļ	9.1.	NetBrain requires AWS IAM permissions?	. 51

1. AWS API Access Overview

NetBrain uses API (more specifically, Boto3 SDK) to retrieve the data from AWS. There are different ways to configure access to AWS, and we will explore each method in detail.

- 1. **Key-based Access**: Set up public and private keys so the NetBrain IE system can use static key(s) to discover AWS resources.
- 2. **Role-based Access**: Set up different roles for the NetBrain IE system to access AWS accounts, and it doesn't require any static key.
- 3. **Combined Access**: Configure the key-based access for one master account and then access the monitored accounts via the role-based access method.

1.1. Key-based Access Overview

NetBrain requires AWS public key and secrete key to be configured to access the data from AWS for key-based access. NetBrain will use the configured credentials to send HTTP requests via Front Server. Therefore Front Server is required to access the Amazon AWS websites from an Internet access perspective: *.amazonaws.com.

The following diagram shows how to configure the NetBrain servers to access your different AWS accounts, named monitored accounts (where the infrastructure data resides). In this deployment model, you will need to create static keys (including public and private keys) for each account and use these keys to access AWS resources.

As the requirement is to access the Amazon AWS website from the Front Server, you may deploy the NetBrain Front Servers in your on-prem data center or AWS. And there is no limitation on how to deploy NetBrain Front Servers. If you have traditional devices, CPE devices, or devices in the colocation to be discovered, make sure that the Front Server has access to these devices.



1.2. Role-based Access Overview

Role-based access requires you to configure the proper roles for NetBrain to assume for data retrieval. The following diagrams demonstrate the high-level concepts of role-based access deployment:



There are two types of accounts:

- 1. **Gateway Account**: Gateway account delegates access to other accounts. It is typically the account for monitoring, security, and auditing purposes in multi-account architecture.
- 2. Monitored Accounts: Accounts that host infrastructure data and need to be discovered.

The solution requires the NetBrain Front Server to run on an EC2 instance in a gateway account. In the account to be monitored, a role needs to be created to delegate and authorize access from the EC2 instance in the gateway account.

Once the proper role and policy have been configured, NetBrain Front Server can read the network configurations and run statistics from the monitored accounts.

The following diagram shows a detailed structure of this deployment.

Note: You only need to install the Front Server within an EC2 instance to assume proper roles. You can still have other NetBrain components in your on-prem Data Centers for communication purposes if you have IPSec or direct connections to the cloud environment.



1.3. Combined Access Overview

You sometimes don't want to permit EC2 instances to assume the role due to security or other considerations. Then, you can leverage the combined access method.

As depicted in the following diagram, we use key-based access to access the gateway account. The created user can assume the role in the monitored accounts. This way, you can install the Front Server anywhere if it has access to the AWS website.



2. Setting Up Key-based Access

This chapter will guide you through the details of how to set up key-based access for your AWS accounts.

2.1. Creating AWS Access Policy in Amazon Console

The AWS access policy defines the minimal scope of permissions that enables NetBrain to retrieve the data to build the data model and use the CloudWatch API to monitor the services running in your AWS account.

Note: You can create and use the policy anytime when enabling NetBrain to access your AWS account.

1. Go to Identity and Access Management (IAM) in your Amazon Console.

aws	Services 🗸 Resource Groups 🗸 🔭				
	AWS Management Console				
	AWS services				
	Find Services You can enter names, keywords or acronyms.				
	IAM Manage access to AWS resources All services				

2. Go to **Policies** and click **Create policy**.



3. Select the **JSON** tab, and paste the predefined policy in JSON as sample follows. To get the latest required AWS IAM permission, refer to <u>Online Help: NetBrain Required AWS IAM Permissions</u>.

Create policy



Import managed policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor JSON

2	"Version": "2012-10-17",	
3 🕶	"Statement": [
4 -	{	
5 -	"Action": [
6	"autoscaling:Describe*",	
7	"autoscaling-plans:Describe*",	
8	"autoscaling-plans:GetScalingPlanResourceForecastData",	
9	"cloudwatch:Describe*",	
10	"cloudwatch:Get*",	
11	"cloudwatch:List*",	
12	"directconnect:Describe*",	
13	"ec2:Describe*",	
14	"ec2:Get*",	
15	"ec2:SearchTransitGatewayRoutes",	
16	"network-firewall:DescribeFirewall",	
17	"network-firewall:DescribeFirewallPolicy",	
18	"network-firewall:DescribeRuleGroup",	
19	"network-firewall:ListFirewallPolicies",	
20	"network-firewall:ListFirewalls",	
21	"network-firewall:ListRuleGroups",	
22	"network-firewall:ListTagsForResource",	
23	"elasticloadbalancing:Describe*"	
24],	
25	"Effect": "Allow",	
26	"Resource": "*"	
27	}	
28	1	
20		_//

4. Click **Review Policy** and enter the policy name in the **Name** field (i.e., NetBrain_access_policy).

Create policy				
Review policy				
Name*				
Description	Use alphanumenc and +=,.@' characters. Maximum 128 characters.			
	Maximum 1000 characters. Use alphanumeric and '+=,.@' characters.			

5. Click **Create policy**.

2.2. Enabling Access to Your Amazon Account Using Key-based Access

NetBrain must identify all virtualized infrastructure components in your AWS environment to get the information required to build the data model. This information is used to understand the context of your applications, services, and hosts. To enable it, you need to authorize NetBrain to access your Amazon metrics.

You can enable NetBrain to access your AWS metrics by either using a private access key (key-based access) or defining a special role for NetBrain (role-based access). In either case, make sure that your Front Server (used for data retrieval) has a connection to AWS by configuring your proxy for Front Server or whitelist ***.amazonaws.com** in your firewall settings.

NetBrain can use access keys to enable secure REST or Query protocol requests to the AWS service API. You will need to generate an Access Key ID and a secret access key so NetBrain can use them to get the metrics from Amazon Web Services.

Note: If you add multiple AWS accounts to NetBrain, you must repeat these steps for each account.

Prerequisites:

- Rights to create a new AWS user
- AWS account ID
- The Amazon Access Key ID and secret access key

Proceed with the following steps:

- 1. In the Amazon IAM Console, click **Users** > **Add user**.
- 2. Enter a name for the key, for example, **NetBrain_access_user** and click **Next**.

ser details					
er name					
WS_test_user					
e user name can have up to 64 characters. Valid c	aracters: A-Z, a-z, 0-9, and + = , . @ (hyphen)				
Provide user access to the AWS Managem If you're providing console access to a person, it	nt Console - optional a best practice 🔀 to manage their access in IAM Identity Cent	ter.			
 If you are creating programmatic acce 	s through access keys or service-specific credentials f	or AWS CodeCommit or Amazon Keyspaces, you ca	n generate them after you create this IAM user.	Learn more 🔀	

3. Click **Attach existing policies directly** and select the monitoring policy you have defined: **NetBrain_access_policy**, then click **Next: Review**.

Add user		1 2
 Set permissions 		
Add user to group	Copy permissions from existing policies directly	

- 4. Review the user details and click **Create user**.
- 5. Click on the User created and locate the **Security credentials** tab and Click on **Create access key** to create at least one active access key for the user account.

Permissions Groups Tags Security credentials Access Advisor					
Console sign-in	Enable console access				
Console sign-in link the https://netbrain-lab.signin.aws.amazon.com/console	Console password Not enabled				
Multi-factor authentication (MFA) (0) Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. Learn more 🔀					
Device type Identifier	Created on				
No MFA devices. Assign an MFA device to improve the security of your AWS environment Assign MFA device					
Access keys (0) Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maxim	mum of two access keys (active or inactive) at a time. Learn more 🔀				
No access keys As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials.&bsp:Learn more 🔀 Create access key					

6. Under the Access key best practices & alternatives, choose the Other option and click on Next

Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Command Line Interface (CLI) You plan to use this access key to enable the AWS CLI to access your AWS account.	
]
You plan to use this access key to enable application code in a local development environment to access your AWS account.	
O Application running on an AWS compute service You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.]
O Third-party service You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.	
Application running outside AWS You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.]
O Other Your use case is not listed here.]
	Cancel Nevt

- 7. On the next page, describe the tag value, if needed, and then click **Create access key**
- 8. Store the Access key ID name (AKID) and secret access key values. You can either download the user credentials or click **Show** to copy the credentials displayed online.

2.3. Configuring NetBrain to Access AWS Using Key-based Access

Once you've granted AWS access to NetBrain, you need to connect NetBrain to your Amazon AWS account.

 On the Domain Management page, select **Operations > Discover Settings > API Server Manager** from the quick access toolbar.

Edit External API Server X			
* Server Name:	AW52		
Description:			
* API Source Type:	Amazon AWS 🗸 🗸		
* Endpoint (Account ID):	AWS925		
* Access Key Id:	AKIA. AT		
* Secret Access Key:			
* Front Server/Front Server Group:	local(127.0.0.1)		
Advanced A			
Кеу	Value		
Region Names	us-east-1,us-east-2, us-west-1,us-west-2		
Managed Devices: 12			
Test	Cancel OK		

- 2. In the **Server Name** field, enter a meaningful name that can uniquely identify your AWS account.
- 3. Create a new external API server and select **Amazon AWS** as the **API Source Type**.
 - 1) In the **Access Key Id** field, paste the identifier of the key you created in AWS for NetBrain access.
 - 2) In the **Secret Access Key** field, paste the value of the key you created in AWS for NetBrain access.
 - 3) In the **Endpoint (Account ID)** field, enter the AWS account identifier.
 - 4) Click **Test** to verify the connection.
 - 5) Click **OK** to save the connection.

Add External API Server		×
	Test External API Server	×
* Server Name:	Start Time: 2020-04-09 14:57:49	٦
L	Connecting to Front Server(fs_local)	
* API Source Type:	Successful Connecting to end points (747895045325) via Front	
* Endpoint (Account ID):	Server(fs_local) Verified programming keys for account 747895045325. Found	
* Access Key Id:	the following regions with allocated resources: ca-central-1,us-	
* Secret Access Key:	east-1,us-east-2,us-west-1,us-west-2 Successful	
* Front Server/Front Server Group:	End Time:2020-04-09 14:58:07	
Advanced V	ОК	
Managed Devices: 0		
Test	Cancel OK	

4. Once the connection is verified and saved, you can proceed to <u>Discovering AWS Network in NetBrain</u> <u>Domain</u> to start the data retrieval process.

Note: By default, NetBrain queries all regions in your AWS accounts for data retrieval. NetBrain will further identify whether there are resources for these regions based on whether the ENI interface exists in these regions. If you only want to retrieve the data for specific regions, you can specify the regions you want NetBrain to access in the **Parameter List** field.

Parameter				×
Key:	Region Names		~	
Value:	us-east-1,us-east-2			
		Cancel	Save	

3. Setting Up Role-based Access

This chapter will guide you through how to set up role-based access for your AWS accounts.

3.1. Creating AWS Access Policy and Role for Monitored Accounts

1. Go to Policies in Identity and Access Management (IAM).

2. Create a new resource access policy to grant read access to the services for monitoring purposes.

Review and create	Policy edi	or	Visual JSON Actions v
	1 ▼ { 2 "Ver 3 ▼ "Sta 4 ▼ 5 ▼ 6 7 8 9 10 11 12 13 4 1 12	<pre>ion": "2012-10-17", ement": [{ "Action": ["autoscaling:Describe*", "autoscaling-plans:Describe*", "autoscaling-plans:GetScalingPlanResourceForecastData", "cloudwatch:Describe*", "cloudwatch:Get*",</pre>	Edit statement Select a statement in th add a new statement. + Add new statement.
	14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 2 6 27 28 3 4 4 4 5 5 26 27 28 3 24	<pre>"ec2:Get", "ec2:Get", "network-firewall:DescribeFirewall", "network-firewall:DescribeFirewallPolicy", "network-firewall:ListFirewallPolicies", "network-firewall:ListFirewallo", "network-firewall:ListFirewalls", "network-firewall:ListTagsForResource", "elastLcloadbalancing:Describe*"], "Effect": "Allow", "Resource": "*" }</pre>	



```
"cloudwatch:Describe*",
         "cloudwatch:Get*",
         "cloudwatch:List*",
         "directconnect:Describe*",
         "ec2:Describe*",
         "ec2:Get*",
         "ec2:SearchTransitGatewayRoutes",
         "network-firewall:DescribeFirewall",
         "network-firewall:DescribeFirewallPolicy",
         "network-firewall:DescribeRuleGroup",
         "network-firewall:ListFirewallPolicies",
         "network-firewall:ListFirewalls",
         "network-firewall:ListRuleGroups",
         "network-firewall:ListTagsForResource",
         "elasticloadbalancing:Describe*"
      ],
       "Effect": "Allow",
       "Resource": "*"
    }
  ]
}
```

Once we created the policy, we need to attach this policy to the Role.

Follow the steps below to configure the role:

- 1. Go to Roles in Identity and Access Management (IAM).
- 2. Create a new role by selecting Trusted entity type as **Custom trust Policy**. Add a Trust policy to allow the EC2 instance's Role from the gateway account to assume this role.



The sample trust relationship JSON statements are as follows. You need to replace the account

ID, role name, and External ID to reflect your specific configuration.

Note: The role name of the EC2 instance, for example, NetbrainAccessRoleForEC2, must match the EC2 instance role name configured in the gateway account.

3.	"Version": "2012-10-17",
4.	"Statement": [
5.	{
6.	"Effect": "Allow",
7.	"Action": "sts:AssumeRole",
8.	"Principal": {
9.	"AWS": [
10.	"arn:aws:iam::<12-digit gateway account number>:role/ <role ec2="" for="" frontserver<="" instance="" netbrain="" run="" td="" your=""></role>
	(i.e. NetbrainAccessRoleForEC2)>"
11.]
12.	},
13.	"Condition": {
14.	"StringEquals": {
15.	"sts:ExternalId": " <external from="" generated="" id="" tenant="">"</external>
16.	}
17.	}
18.	}
19.]
19.1	.}

3.Attach the policy (created previously) to the role.

IAM > Roles > Create role				
Step 1 Select trusted entity	Add permissions Info			
Step 2 Add permissions	Permissions policies (1/965) Info Choose one or more policies to attach to your new role.			C
Step 3		Filter by Type		
Name, review, and create	Q. NetbrainMo	X All types	▼ 1 match < 1	> @
	Policy name 🖸	▲ Туре	▼ Description	
	NetbrainMonitorPolicy	Customer managed		
	 Set permissions boundary - optional 			
			Cancel Previous	Next

3.2. Configuring EC2 Role for NetBrain Front Server in AWS Gateway Account

This section illustrates how to create a role for an EC2 instance in the gateway account using the AWS console. This will allow the EC2 instance that hosts NetBrain system to access the monitored accounts.

- 1. Go to Roles in Identity and Access Management (IAM) and create a new role.
- 2. Select **AWS service** and **EC2** for this role.

p 1 lect trusted entity	Select trusted entity Info			
p 2 d permissions	Trusted entity type			
ep 3 ame, review, and create	 AWS service Allow XWS services like EC2, Lambda, or others to perform actions in this account. 	 AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account. 	Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.	
	SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.	Create a custom trust policy to enable others to perform actions in this account.		
	lin this account.			
	Allow an AWS service like EC2, Lambda, or others to pe	erform actions in this account.		
	Service or use case			
	EC2		•	
	Choose a use case for the specified service.			
	Use case			
	C EC2			

3. Enter the role name (NetbrainAccessRoleForEC2).

Note: The role name shall match the one you previously picked when configuring the trusted relation in the monitored account.

Skip the Permissions (policy) section in the wizards. The policy will be added later.

4. After the role is successfully created, open the role and attach an inline policy to allow the EC2 instance to assume **NetbrainAccessRole** in monitored accounts.

Identity and Access Annual Management (IAM)	IAM > Roles > NetbrainAccessRoleForEC2		
	NetbrainAccessRoleForEC2 Info		
Q Search IAM	Allows EC2 instances to call AWS services on your behalf.		
Dashboard	Summary		
 Access management 	Creation date	ARN	Instance profile ARN
User groups	April 09, 2020, 11:21 (UTC-04:00)	am:aws:iam::747895045325:role/NetbrainAccessRoleForEC2	In arn:aws:lam::747895045325:instance-profile/Net
Users	Last activity	Maximum session duration	
Roles	2 hours ago	1 hour	
Policies Identity providers Account settings	Permissions Trust relationships Tags Last Accessed Revoke sessions	s	
 Access reports 			
Access Analyzer	Permissions policies (2) Info		C Simula
External access	You can attach up to 10 managed policies.		
Unused access		Filter by Type	
Analyzer settings	Q, Search	All types	Ŧ
Credential report Organization activity	Policy name [2]	▲ Туре	▼ Attached entities
Service control policies	EventorianAssumeRolePolicy	Customer inline	0
Related consoles	NetbrainAssumeRolePolicy		
IAM Identity Center	1-[(] version": "2012-10-17", - "Ctatement": [
AWS Organizations 🕻	<pre>3* "Statement: [4* [5* "Statement: [5* [5* [5* [5* [5* [5* [5* [5*</pre>	te" Leforec2"	

A sample policy JSON is as follows.

Note: Use the account ID to monitor your environment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::<12-digit first monitored account number>:role/<role created in previous step
(NetbrainAccessRole)>"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": ""arn:aws:iam::<12-digit second monitored account number>:role/<role created in previous step
(NetbrainAccessRole)>""
    }
  ]
}
```

5. If we want to discover the resources of AWS gateway account in Netbrain, then we need to add new resource access policy to this role to grant read access to the services.

NetbrainAccessRoleForEC2 Info	
Allows EC2 instances to call AWS services on your behalf.	
Summary	
Creation date April 09, 2020, 11:21 (UTC-04:00)	ARN Insta Insta Insta Insta Insta Insta
Last activity S6 minutes ago	Maximum session duration 1 hour
Permissions Trust relationships Tags Last Accessed	Revoke sessions
Permissions policies (2) Info You can attach up to 10 managed policies.	
	Filter by Type
Q Search	All types 🔻
□ Policy name [7] ▲ Type	▼ Attached entities
NetbrainAssumeRolePolicy Customer inline	0
E <u>NetbrainMonitorPolicyDeta</u> Customer managed	3
NetbrainMonitorPolicyDetailed Explicitly list all actions in details. 1 ~ [{] 2 "Version": "2012-10-17", 3 ~ "Statement": [4 ~ { 5 "Sid": "VisualEditor®",	

"Version": "2012-10-17", "Statement": [{ "Action": ["autoscaling:Describe*", "autoscaling-plans:Describe*", "autoscaling-plans:GetScalingPlanResourceForecastData", "cloudwatch:Describe*", "cloudwatch:Get*", "cloudwatch:List*", "directconnect:Describe*", "ec2:Describe*", "ec2:Get*", "ec2:SearchTransitGatewayRoutes", "network-firewall:DescribeFirewall", "network-firewall:DescribeFirewallPolicy", "network-firewall:DescribeRuleGroup", "network-firewall:ListFirewallPolicies",

{



6. Find the EC2 instance where you run NetBrain Front Server, and attach the role to it. You can also specify the role when first launching an EC2 instance.

aws iii Services	Q Searc	[Alt+S]	۵	🗘 🕜 🚷 N. Virginia 🔻	AdministratorAccess/ashhar.mohammed@ne	etbraintech.com 🔻
EC2 Dashboard EC2 Global View Events Console-to- Code <u>Preview</u> V Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservation	X 15	Instances (1/1) Info Q. Find Instance by attribute or tag (case-sensitive) Name # SG2-ypc1-instance2 X Clear filters X Instance ID X SG2-ypc1-instance2 I-030496356ac2052824	Last updated C Less than a minute ago C All states ▼ Instance type ▼ Status check ⊙ Stopped Q Q t2.micro -	Connect Instance state Alarm status Availability : View alarms + us-east-1a Change security groups Get Windows password Modify IAM role	Actions A Launch Instance Connect View details Manage instance state Zo Instance settings Networking Security Image and templates Monitor and troubleshoot	s v S
 Images AMIs 		i-03049636ac2052824 (SG2-vpc1-instance2)	=			® ×

3.3. Configuring NetBrain System

Follow the steps below to add the accounts to monitor:

- On the Domain Management page, navigate to Operations > Discover Settings > API Server Manager.
- 2. In the **API Server Manager** configuration page, click **Add API Server** to add an API Server entry into the table for each account to be monitored.
- 3. Configure the parameters in the Edit External API Server window as follows:
 - 1) API Source Type: Select Amazon AWS.
 - 2) Access Method: Select Role-based Access.

- 3) Endpoints (Account ID): Enter the AWS Monitor account ID
- 4) **External Id**: Enter the External ID previously selected for the trust relationship in the AWS Monitor account.
- 5) **Role Name**: Enter the role name previously selected in the AWS Monitor account.

nain Management				Tenant: Te	enant_fsc_aws	Domain: AWS_RoleBased_1	Operations 💄 y	🛛 🖉 NetBrai
Start Page Discover X	Schedule Task X API Se	rver Manager $~ imes$						
Fotal Items: 1 + Add API Ser	ver			All API	Source Types 🗸	Search	🔍 🕞 Backup 🕞 Re	store 😋 Refresh
API Source Type	Server Name	EndPoints	Description	Username	Front Serve	r / Front Server Group	Device Counts	
Amazon AWS	07 25	07 25	Monitor AWS account 0701135.		fs_aws(17	0)	50	
	Edit External API Server			×				
	* Server Na	me: 070113567925						
	Descript	ion: Monitor AWS account 0 in account 747	77 <mark>1</mark>	legated to role				
	* API Source Ty	/pe: Amazon AWS		~				
	* Access Meth	od: Role-based Access		~				
	* Endpoints(Account	ID): 07						
	* Externa	l ld: netbrain						
	* Role Na	me: NetbrainAccessRole						
	* Front Server/Front Server Gro	sup: fs_aws(12	20)	~				
	Advanced V					R		
	Managed Devices: 50							
	Test		Cance	ок				

Tip: Alternatively, you can call NetBrain northbound APIs to add/update/delete AWS accounts if you have integrated them with your NetOps automation flow. For more information about the APIs, refer to <u>Using REST API to Manage</u> <u>AWS Data</u>.

More information about the configuration parameters is as follows:

	Display Name	Mandatory	Notes
Combined	Authentication Method	Yes	Authentication method to access account resources.
			Use the drop-down menu to select from KeyBase or RoleBase.
	Endpoint (Account ID)	Yes	The AWS account to be monitored.
	Region Names	No	Comma-separated official AWS region names.
			Explicitly specify and limit the regions to monitor. Default to all publicly accessible regions if not specified.
Key-Based	Access Key ld	Yes	Program access key associated with an IAM user, which can be used for programmatic access to AWS account resources.

	Secret Access Key	Yes	The secret key associated with the access key for authentication purposes.
Role-Based	Role Name	Yes	Role configured in AWS account for role-based access.
	External ID	Yes	external ID configured for the role in the monitored account. As recommended by AWS, this is a mandatory field for security purposes.
	Session Name	No	The Session Name will show in the CloudTrail log of the monitored account. It can be used for auditing purposes. Default to "netbrain_monitor" if not configured.

4. Click **Test** to verify that NetBrain system has access to the AWS account resources. If it fails, check if the roles and policies are configured properly.

Edit External API Server			
* Server Name: Description:	07025 Monitor AWS account 07 6************************************		Test External API Server X Start Time: 2020-08-13 14:37:07
* API Source Type:	Amazon AWS		Connecting to Front Server(fs_aws) Successful
* Endpoints(Account ID):	0725		Connecting to end points (075) via Front Server(fs_aws) Verified programming keys for account 075. Found
* External Id: * Role Name:	netbrain NetbrainAccessRole		the following regions with allocated resources: ca-central-1,us- east-1,us-east-2,us-west-1,us-west-2
* Front Server/Front Server Group:	fs_aws(120) v	j	End Time:2020-08-13 14:37:22
Advanced ∨ Managed Devices: 50		L	ок
Test	Cancel OK		

4. Setting Up Combined Access

As shown in the diagram below, monitored accounts on the right-hand side are the accounts you will add to NetBrain for management purposes. You will need to configure the proper roles for these accounts to be accessed by the gateway account.



Compared to pure role-based access, the combined access gains access to the gateway account through keybased access, which gives you the flexibility to set up the Front Servers in any desired location.

Follow the steps below to set up the combined access:

- 1. Creating AWS Access Policy and Role for Monitored Accounts
- 2. <u>Creating Public/Secret Keys for Gateway Accounts</u>
- 3. Configuring NetBrain System
- 4. Auto Updating The Master Keys in Monitor Account

4.1. Creating AWS Access Policy and Role for Monitored Accounts

- 1. Go to Policies in Identity and Access Management (IAM).
- 2. Create a new resource access policy to grant read access to the services for monitoring purposes.





	"network-firewall:DescribeFirewall",
	"network-firewall:DescribeFirewallPolicy",
	"network-firewall:DescribeRuleGroup",
	"network-firewall:ListFirewallPolicies",
	"network-firewall:ListFirewalls",
	"network-firewall:ListRuleGroups",
	"network-firewall:ListTagsForResource",
	"elasticloadbalancing:Describe*"
],	
"E	ffect": "Allow",
"R	esource": "*"
}	
]	
}	

Once we created the policy, we need to attach this policy to the Role.

Follow the steps below to configure the role (**NetbrainAccessRole**):

- 3. Go to Roles in Identity and Access Management (IAM).
- 4. Create a new role by selecting Trusted entity type as **Custom trust Policy**. Add a Trust policy to allow the user from the gateway account to assume this role.

IAM > Roles > Create role	Leo and
Step 1 Select trusted entity	Select trusted entity Info	
Step 2 Add permissions	Trusted entity type	
Step 3 Name, review, and create	AWS service Allow AWS services like EC2. Lambda, or others to perform actions in this account.	Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
	SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account. Create a custom trust policy Create a custom trust Create a custom trust policy	
	Create acutom trust policy Create acutom trust policy to malte others to perform actions in this account.	
	8), 9 *Action: "stsiAssumeRele", 10▼ *Condition: { 11▼ *fringRoule: { 12 *stsiExternald": "netbrain" 13 }	

The sample trust relationship JSON statements are as follows. You need to replace the account ID, role name, and External ID to reflect your specific configuration.

Note: The role name of the EC2 instance, for example, NetbrainAccessRoleForEC2, must match the EC2 instance role name configured in the gateway account.

Ļ	5. "	'Version": "2012-10-17",
6	5. "	'Statement": [
7	7.	{
ξ	3.	"Effect": "Allow",
9	Э.	"Action": "sts:AssumeRole",
-	10.	"Principal": {
-	11.	"AWS": [
-	12.	"arn:aws:iam::<12-digit gateway account number>:user/ <user account="" created="" gateway="" in="" name="">"</user>
-	13.]
-	4.	},
-	15.	"Condition": {
-	16.	"StringEquals": {
-	17.	"sts:ExternalId": " <external from="" generated="" id="" tenant="">"</external>
-	8.	}
-	19.	}
4	20.	}
4	21.]	
		a. }

5. Attach the policy (created previously) to the role.

IAM > Roles > Create role Step 1 Select trusted entity	Add permissions Info		
Step 2 Add permissions	Permissions policies (1/965) Info Choose one or more policies to attach to your new role.		C
Step 3 Name, review, and create	Q. NetbrainMo	Filter by Type X All types	▼ 1 match < 1 > ⊗
	Policy name [2	▲ Туре	ত Description
	Element E	Customer managed	-
	 Set permissions boundary - optional 		
			Cancel Previous Next

4.2. Creating Public/Secret Keys for Gateway Accounts

This section illustrates how to create User Account in the Gateway account with privileges to assume the role in the monitoring accounts using the AWS console.

1. Go to Users in Identity and Access Management (IAM) and create a new user .

aws Services Q Search	[Alt+S]		区 🔶 ⑦ 稔 Global	 AdministratorAccess/ashhar.mohammed@netbraintech.com
Identity and Access X Management (IAM)	IAM > Users			(
	 Ready to streamline human access to AWS and cloud a 	ops?		Dismiss Manage workforce users [2]
C Search IAM	Identity Center is enabled. We recommend managing workforce us	ers' access to AWS accounts and cloud applications i	in Identity Center.	
Dashboard	Learn more C Watch how it works			
 Access management 				
User groups	Users (3) Info			C Delete Create user
Users	An IAM user is an identity with long-term credentials that is used to interact with AWS in	an account.		
Roles	Q Search			< 1 > 🕲
Policies				
Identity providers	□ User name ▲ Path ▼ Grou	p: ▼ Last activity ▼ MFA ▼ Pass	sword age ▼ Console last sign-in ▼	Access key ID Active key age
Account settings		📀 6 minutes ago - 🔥 1	688 days 🛆 September 11, 2020, 07:	Active - AKIARAUYYES 🛕 1689 days
Access reports	villu@netbraintech.com / 1	A 286 days ago Virtual A 5	549 days December 22, 2023, 0	
Access Analyzer			,,	
External access	vitest / 0	<u>▲ 142 days ago</u> - <u>▲</u> 1	42 days May 14, 2024, 03:43 (· · · · ·
Unused access	4			•
Analyzer settings				
Credential report				
Organization activity				

2. Select **Attach policy Directly** and continue to create the user. We will add policy to the user later.

IAM > Users > Create user				(
Step 1 Specify user details	Set permissions Add user to an existing group or create a new one. Using groups is a best-pro	actice way to manage user's permissions by job functions. Learn more [(
Step 2 Set permissions	Permissions options			
Step 3 Review and create	Add user to group. Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.	 Copy permissions Copy all group memberships, attached managed policies, and inline policies from an existing user. 	 Attach policies directly Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group. 	
	Permissions policies (1248) Choose one or more policies to attach to your new user.		C Create policy [2]	
	Q Search	Filter by Type All types	<pre>< 1 2 3 4 5 6 7 63 > (8)</pre>	
	Policy name 🔁	▲ Туре	abla Attached entities $ abla$	

3. Once user has created, create inline policy for the user.

dentity and Access X	IAM > Users > netbrain_user			
lanagement (IAM)	nethrain user a			Dal
Control IAM				De
Search IAM	Summary			
bhoard				
ore management	ARN	Console access Disabled	Access key 1	
r groups	Constant			
s	October 03, 2024, 15:01 (UTC-04:00)	-		
5				
ies ity providers	Permissions Groups Tags Security credentials	Last Accessed		
unt settings				
ss reports	Permissions policies (0)		C Remove	Add permissions
ss Analyzer	Permissions are defined by policies attached to the user directly or through g	oups.		Add permissions
cternal access	O. Sarah	Filter by Type		Create inline policy
nused access nalvzer settings	Search	All types		
ential report	Policy name [7]	▲ Туре	▼ Attached via [2]	
nization activity		No resources to display		
ice control policies				
	Permissions boundary (not set)			
ed consoles	· · · · · · · · · · · · · · · · · · ·			
Permissions policies You can attach up to 10 manag	(2) Into ed policies.			
			Filter by Type	
Q, Search			All types	
Policy name		Type		
NetbrainAs	umeRolePolicy	Customer inline		
NetbrainAssumeRole	Policy			
1-0				
3 "Statement":	12-18-17 ⁻ ,			
2 - Version": "2 3 - "Statement": "4 4 - { 5 "Effe 6 "Acti: 7 "Reso 8 },	sl2-le-l7", (t": "Allow", on": "sts:AssumeRole", unce": "ann:aws:iam:: :role/WetbrainAccess	tole"		
2 "version": "2 3" "Statement": 5 "Effe 6 "Acti 7 "Reso 8), 9" { 10 "Effe 11 "Acti 12 "Reso 13),	<pre>sil-left; "Allow", sh": "sts:AssumeRole", arce": "arn:aws:iam::::role/NetbrainAccess :t": "Allow", sh": "sts:AssumeRole", arce": "arn:aws:iam::role/NetbrainAccess</pre>	tole" ToleForEC2"		
2 "version": "2 3" "Statement": 4" { 5 "Effe 6 "Acti 7 "Reso 8 }, 9" { 10 "Effe 11 "Acti 12 "Reso 13 }, 14" { 15 "Effe 16 "Acti 17 "Reso 13 }, 14" { 16 "Acti 17 "Reso 18 }, 18 "	<pre>siz-la-17", it": "Allow", on": "sts:AssumeRole", on": "Allow", on": "sts:AssumeRole", on": "sts:AssumeRole", on": "Allow", on": "sts:AssumeRole", on": "sts:AssumeRole", on": "sts:AssumeRole", on": "sts:AssumeRole",</pre>	tole" toleForEC2" tole"		
2 "version": "2 3" "Statement": 4" { 5 "Effe 6 "Acti 7 "Neso 8 }, 9" { 10 "Effe 11 "Acti 12 "Reso 13 }, 14" { 16 "Acti 17 "Reso 13 }, 14" { 16 "Acti 17 "Reso 13 }, 14" { 16 "Acti 17 "Reso 18 }, 19" { 18 ST 19 ST 10 "Effe 10 "Effe	<pre>nil-left; it: "Allow", on": "sts:AssumeRole", on": "sts:AssumeRole", on": "sts:AssumeRole", on": "sts:AssumeRole", on": "Allow", on": "sts:AssumeRole", on": "sts:AssumeRole", on: "sts:AssumeRole", on:</pre>	tole" toleForEC2" tole"		

0

Note: Use the account ID to monitor your environment.



4.Create Access Key for the User and Save it safely. We need to input these keys in Netbrain.

Identity and Access × Management (IAM)	ARN Created October 03, 2024, 15:01 (UTC-04:00)	Console access Disabled Last console sign-in -		Access key 1 Create access key
Access management User groups	Permissions Groups Tags Security credentials	Last Accessed		
Users Roles	Console sign-in			Enable console access
Policies Identity providers Account settings	Console sign-in link		Console password Not enabled	
Access reports Access Analyzer External access	Multi-factor authentication (MFA) (0) Use MFA to increase the security of your AWS environment. Signing in with MF/	A requires an authentication code from an MFA device	Each user can have a maximum of 8 MFA devi	Remove Resync Assign MFA device
Unused access	Type	entifier	Certifications	Created on
Analyzer settings Credential report Organization activity Service control policies		No MFA devices. Assign an MFA device to in	nprove the security of your AWS enviror	iment
Related consoles	Access keys (0) Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tor	ols for PowerShell, AWS SDKs, or direct AWS API calls.	You can have a maximum of two access keys (a	Create access key
AWS Organizations [7	No access keys. As a best pract	tice, avoid using long-term credentials like acc	ess keys. Instead, use tools which provid	e short term credentials. Learn more 🕻

6

4.3. Configuring NetBrain System

After you have set up the monitored accounts and gateway accounts, follow these steps to add the accounts to monitor:

- On the Domain Management page, navigate to Operations > Discover Settings > API Server Manager.
- 2. In the **API Server Manager** configuration page, click **Add API Server** to add an API Server entry into the table for each account to be monitored.
- 3. Configure the parameters in the **Edit External API Server** window as follows:
 - 1) API Source Type: Select Amazon AWS.
 - 2) Access Method: Select Role-based Access.
 - 3) Endpoints (Account ID): Enter the AWS account ID to be monitored.
 - 4) **External Id**: Enter the External Id previously selected for the trust relationship in the AWS account to be monitored.
 - 5) **Role Name**: Enter the role name previously selected in the AWS Monitor account.
- 4. In the **Advanced** section, click **+Add** and add the following keys of user account created in the gateway account:
 - **Master Access Key**: This is the public key used to access the gateway account.



Management		١	Tenant: BVT_DB1TEN_8d11	f1 Domain: BVT_DB1	DOM_7ebee3 Operations 💄 ydu 🕜
ge API Server Manager ×	Add External API Server Parameter		×	×	
ms: 0 + Add API Server	* S Key:	Region Names	~	Search	🔍 🕞 Backup 🕞 Restore
urce Type Server Name	Value:	Region Names Federation SSO Url Session Name			Device Counts
	* API : * Access Method:	Master Access Key Master Secret Access Key Kule-Daseu Access	-	~	
	* Endpoint(Account ID): * External ID:	Input your AWS account identifier Input External ID	r		
	* Role Name: * Front Server:	Input Role Name		~	
	Advanced A Parameter List: 0 items + Add				
	Key	Value			
	Managed Devices: 0		Cancel	01	

As part of security best practices, the access key and secret key for the gateway account should be rotated at regular intervals. If you manage multiple monitor accounts, you can use the Master Access Key Rotation plugin to update the new access and secret keys across all monitor accounts with a single click. For more details about the plugin, please visit Auto Updating Master Keys in Monitor Accounts

- 5. Click **Test** in the **Add External API Server** window to verify the connection to the monitored accounts to ensure they are connected successfully.
- 6. Click **Test** in the **Edit External API Server** window to verify that NetBrain IE has access to the AWS account resources. If it fails, check if the roles and policies are configured properly.

Edit External API Server			
* Server Name: Description:	0 25 Monitor AWS account 07 5 which has access delegated to ro in account 74 5.	ble	Test External API Server X Start Time: 2020-08-13 14:37:07
* API Source Type:	Amazon AWS	~	Connecting to Front Server(fs_aws)
* Access Method:	Role-based Access	~	Successful Connecting to end points (075) via Front
* Endpoints(Account ID):	0725		Server(fs_aws) Verified programming keys for account 07(5. Found
* External ld:	netbrain		the following regions with allocated resources: ca-central-1,us- east-1.us-east-2.us-west-1.us-west-2
* Role Name:	NetbrainAccessRole		Successful
* Front Server/Front Server Group:	fs_aws(120)	~	End Time:2020-08-13 14:37:22
Advanced V			ок
Managed Devices: 50			
Test	Cancel OK		

4.4. Auto Updating Master Keys in Monitor Accounts

Please navigate to the plugin "Master_Access_Key_Rotation" in directory "Built-in Plugins\Special_Scenarios\AWS_Support_Information\" in the feature "Domain Management" "Plugin Manger".



Step1: Please update HOST_URL with your Netbrain IE's root URL.

Step2: USER and PWD need to be replaced with your NetBrain's login credentials.

Step3: TENANT and DOMAIN need to be replaced with your tenant ID and domain ID that you want to work with.

	Name: Master_Access_Key_Rotation	angs 🔲 Apply to Device Group: select 💿
Al Flugns Al Flugns Blut Arboyce Blut Arboyce Blut Arboyce Blut Arboyce Blut Arboyce Arboyce Blut Arboyce Arboyce Blut Arboyce Arboyce Arboyce Blut Arboyce Arboyce Arboyce Blut Arboyce Arboyce Arboyce Blut Arboyce Arboyce Arboyce Arboyce Arboyce Arboyce Blut Arboyce Arboyce Arboyce Arboyce Arboyce Arboyce Blut Arboyce Arboyce Arboyce Arboyce Arboyce Arboyce Arboyce Blut Arboyce Ar	Name: Karle (Kors, Goy, Restoon Default mutualized set Descreption mont main.py + 1 from methods, systage import detamating 1 from the start set in the start set in the start 1 from the start set in the start set in the start set in the start 1 from the start set in the start set	Inger Apply to Device Griegerstelets Inger Apply to Device Griegerste

a. Tip: How to find domainID? Go to domain management should be able to see Domain ID

\leftarrow	→ C ▲ Not secure 192.168.48	.178/domainAdmin.html#/domainAdmin <mark></mark> 80d6d125-3de0)-40f3-801e-51c5f7dde200	@ ☆ ⊻
	Domain Management		🌥 Tenant: Initial Tenant 🌐 Domain: Test-aws1	😫 adnkjdsnf@netbrain.com 🖓 🖡
St	art Page			
	Domain: Test-aws1 Desc	ription:		🖉 🕄 Refre
	O Discover	\delta Data Accuracy Resolution	⑤ Site	Schedule Task
	e 43	■ 0	^ 0	<u> </u>

Tip: How to find tenant ID? Go to tenant management should be able to see tenant ID from URL.

$\leftrightarrow \rightarrow 0$		ot secure	192.168.2	29.156/admir	n.html#/tenantA	dmin 2514	6dca-582b-4	40c-a5ab-4f4	a92c27201	ab=userAuthorizatior
🗅 Netbrain	Progra	amming	🗅 News	🗅 House	Containers	🗅 Case	🗅 History	Church	🗀 Bible	CodeCrafters Adva
	Tenar	nt Mai	nageme	ent - Init	ial Tenant					
	Tenar	it Mai	nageme	ent - Init	ial Tenant	t				

Step4: Replace this "Mater Access Key" with the one you used previously and want to replace/rotate now:

rch Q 🖸 Refresh	Name: Master_Access_Key_Rotation Default Installation Settings Apply to Device Group: select	• He
All Degris Image: Control of the second se	Name: Master_Access_Key_Intextion Default installation Settings Apply to Device Group: select Description input main.py from netbreak.syspel import datamodel from netbreak.syspel import from territore from from tertice intervention from terti	
	<pre>22 23 24 25 25 26 26 26 26 27 27 27 27 27 27 27 27 27 27 27 27 27</pre>	

•

Start Page Plugin Manager × API Server Manager × C Refresh Name: Master-Access, Key, Notation Default Installation Settings Apply to Device Group: select Search... ▲ 📶 All Plugins ▲ 🛄 Built-in Plugins Description Input main.py + G. Multisource MB_System_Use
 Platform_Certification 1 from netbrain.sysspi import detamodel 2 from netbrain.sysspi import dericedeta 4 4 import requests 4 import requests 5 import spint 8 import spint 9 import join 9 import join Plugin_Features 5 Samples Special_Scenarios

 Special_Solutions
 i isoring priorit

 WMS_Special_Solutions
 i isoring priorit

 Onces_special_Normation
 i isoring priorit

 Add_Member_Ling_information
 i isoring priorit

 Onces_special_Normation
 i isoring priorit

 Conces_special_Normation
 i isoring priorit

 Conces_special_Normation
 i isoring priorit

 Conces_special_Normation
 i isoring priorit

 Conces_special_Normation
 i isoring priorit

 Concesspecial_Normation
 i isoring priorit

 Socketmack_concessformall_Special_Socketmenul_Special_Concess
 i isoring priorit

 Socketmack_concessformall_Special_Concessformall_Special AWS_Support_Informat Gisco_Support_Informatio
 Add_Member_Link_Info My Plugins

Step5: Update the new "Master Access Key" and "Master Secret Access Key" of Gateway Account.

NOTE: pls delete secrete access key after you manually run the plugin for security purpose



Step6: Click "debug Run" and "Run" and wait to finish.

6. Discovering AWS Network in NetBrain Domain

Follow the steps below to discover the network data model in a NetBrain domain:

- 1. On the **Domain Management** page, select **Operations > Discover** from the quick access toolbar.
- 2. In the **Discover Devices via API** area, click **Select API Servers** to select the API servers you want to discover.

ann Management						т	lenant: Next-Ge	n2021 Don	nain: NextGen I	Demo Operation	· 21	0
art Page Discover × Schedule Task ×												
iscover					Vie	ew Historical Resu	ult: Select					
Discover Devices via SNMP/CLI Network Settings												
Mathod: Dirrovervia Seed Pouterr	an ID Pan	Access N	Ande: SNMP an	d SSH/Teinet	~ 0	Discovery Depth:	30					
Methou: Unscover via seed Routers	an ie nan	ge nuccas n	noue.	o porte realized		biscovery bepair.						
IP/Hostname: e.g. 10.10.10.1; NY_R1	Calast AD	Conserve										
	Pelect API	Servers										
Discover Devices via API + Select API Servers U	Items Fr	ound: 7 out of 24 🕂 A	dd API Server T	Show Selected	Items Only			Amazon AWS	×	Search		0 0
												~ Le :
API Servers: AWS_Lab_Account_747895045325	Ξ	API Source Type	Server Nam	ne	EndPoints	5	Description		Username	Front Server		
API Servers: AWS_Lab_Account_747895045325		API Source Type Amazon AWS	Server Nan	ne It_74789	EndPoints	5	Description The Lab account	unt that has	Username	Front Server	18)	
API Servers: AWS_Lab_Account_747895045325		API Source Type Amazon AWS Amazon AWS	Server Nam	ne it_74789 it_07011	EndPoints 74 07	5	Description The Lab accou	unt that has	Username	Front Server FS1(192 FS1(192	8)	
API Servers: AWS_Lab_Account_747895045325		API Source Type Amazon AWS Amazon AWS Amazon AWS	Server Nam	ne it_74789 it_07011	EndPoints 74 07 04	5 5 5 5	Description The Lab accou	unt that has	Username	Front Server FS1(192 FS1(192 FS1(192	(8) (8) (8)	
API Servers: AWS_Lab_Account_747895045325		API Source Type Amazon AWS Amazon AWS Amazon AWS Amazon AWS	Server Nam AW2 AW2 AW2 aws	it_74789 it_07011	EndPoints 74 07 04 ht	s S S S aws.com	Description The Lab accou	unt that has	Username	Front Server FS1(192 FS1(192 FS1(192	18) 18) 18)	
API Servers: AWS_Lab_Account_747895045325		API Source Type Amazon AWS Amazon AWS Amazon AWS Amazon AWS Amazon AWS	Server Nan AW3 AW3 AW3 aws 070	it_74789 it_07011	EndPoints 74 07 04 ht 07	s 5 5 5 aws.com 5~	Description The Lab accou	unt that has	Username	Front Server FS1(192 FS1(192 FS1(192	18) 18) 18)	
API Servers: AWS_Lab_Account_747895045325		API Source Type Amazon AWS Amazon AWS Amazon AWS Amazon AWS Amazon AWS Amazon AWS	Server Nan AW: AW: AW: aws 070 747	ne It_74789 It_07011	EndPoints 74 07 04 ht 07 74	5 5 5 aws.com 5	Description The Lab accou	unt that has	Username	Front Server FS1(192 FS1(192 FS1(192	8) (8) (8)	

Note: To build the data model correctly, NetBrain requires CLI+SNMP access to all virtual network appliances of each AWS VPC, including the customer gateway devices (CGW), virtual firewall instances, and virtual load-balancer instances.

Note: To discover virtual appliances via SNMP/CLI, you can specify their management IP addresses in the discovery interface.

7. Auto-Updating AWS Data in NetBrain through Benchmark

The discovery only retrieves basic data of your AWS network and builds L3 topology. After the discovery, you need to execute a benchmark task to retrieve all data and build all components, including visual spaces and data views.

Example: Benchmark AWS in a NetBrain Domain.

- 1. On the Start Page, click **Schedule Task**.
- 2. On the Schedule Discovery/Benchmark tab, click +Add Benchmark Task.
- 3. On the **Frequency** tab, define the task frequency.
- 4. On the **Device Scope** tab, check the **Select external API servers to retrieve data of SDN nodes** check box and select controllers.

dit Benchmark Task			
Task Name: Basic System Benchmark Description: Default system be	enchmark task		
Frequency Device Scope Retrieve Live Data	CLI Commands Add	itional Operations after Benchmark Plugi	ins Summary
Site	Select external API servers t	Amazon AWS v	iearch Q
Load Balancer(1)	API Source Type	Server Name EndPoints	Description
	Amazon AWS	AWS_Lab_Account_7478 74	The Lab account t
Router(18)	Amazon AWS	AWS_Lab_Account_0701 070 25	
End System(373)	Amazon AWS	AWS Lab 041 55	
Firewall(13)			
🔿 Cloud(13)			
L3 Switch(17)			
Exclude Device Groups: exclude			

Note: As a best practice, we recommend re-using the "Basic System Benchmark" with a full benchmark task, where all devices are selected. This ensures that all AWS-connected physical or virtual devices are selected within the device scope.

5. On the **Retrieve Live Data** tab, select the **Amazon AWS** check box, and make sure the following tables (under the NCT table) are selected:

- AWS ENI Interface Table
- AWS ELB Listener Table
- AWS NAT Table
- AWS Network ACL Table
- AWS Security Group Table
- AWS ELB Target Group Table
- AWS Transit Gateway Attachments Table
- AWS Transit Gateway Route Table
- AWS VPC Peering Table
- AWS PC Route Table

Edit Benchmark Task			
Task Name: AWS Benchmark Description:			
Frequency Device Scope Retrieve Live Data CLI Commands Additional Operations after Benchmark	Plugins	Sur	nmary
Stop retrieving after Hours 0 Minutes			
 Built-in Live Data NCT Table VMware vCenter Viptela SD-WAN VMware NSX-V Cisco Meraki Cisco ACI Versa SD-WAN Versa SD-WAN Vamzon AWS Basic Data Node Properties Topology Data VMware VeloCloud SD-WAN CheckPoint R80 API 			
		Capital	Submit

6. On the Additional Operation After Benchmark tab, select the following checkboxes:

- Update MPLS Cloud
- Update Public Cloud

Update Build Topology

Benchmark Task		
ask Name: Basic Syste	m Benchmark Description: Default system benchmark task	
Frequency	Vevice Scope Retrieve Live Data CLI Commands Additional Operations after Benchmark Plugins Summary	
∨ Update MPLS Cloud		I.
Enable	Operation Name	
	Recalculate Cloud	
	Recalculate Cloud NCT	
✓ Update Public Cloud Enable	Operation Name Recalculate AWS Virtual Route Table	
 ✓ 	Recalculate Azure Virtual Route Table	
∨ Build Topology		
Enable	Operation Name	
	IPv4 L3 Topology	
	IPv6 L3 Topology	
	L2 Topology	
	L3 VPN Tunnel	
	Logical Topology	
	12 Overlag Topology	-

Cancel Submit

7. Click Submit.

8. Working with Multi-cloud Environment

If your public cloud environment has multiple public cloud providers, you may want to discover the other public cloud providers, such as Azure and Google Cloud. Refer to their quick setup guides for details.

If the AWS and Azure networks are connected to your on-prem network via L3 VPN, you can use NetBrain to discover both of them. As shown in the diagram below, you need to make sure AWS and Azure are in the same benchmark task to get the entire public cloud data updated:



It is recommended to use one single benchmark task to retrieve all public cloud data. The screenshot below shows an example of retrieving the data from both AWS and Azure:

Task Name: Basic System Benchmark Description: Default system be	nchmark task	
Frequency Device Scope Retrieve Live Data	CLI Commands Additional Operations after Benchmar	rk Plugins Summary
Select Device	Select external API servers to retrieve data	
All Devices Device Group Site	Total Items: 9 All API Source	ce Types 🗸 Search Q
Load Balancer(1)	API Source Type - Server Name	EndPoints Description
	VMware vCenter 192 05	https://1 105
Router(18)	VMware NSX-V 192 06	https://1 106
End System(373)	Viptela SD-WAN Der	https://14
France 10420	Microsoft Azure Azure	85914 pf-988
Firewali(13)	Cisco ACI 192 85	https: 135
📄 Cloud(13)	CheckPoint R80 API 192	https: 5
	Amazon AWS AWS_Lab_Account_7478	74789 The Lab account t
L3 Switch(17)	Amazon AWS AWS_Lab_Account_0701	07011
	Amazon AWS AWS Lab	04144
	·	1

In the Update Public Cloud area of Additional Operations after Benchmark tab, make sure both Recalculate AWS Virtual Route Table and Recalculate Azure Virtual Route Table are selected.

Benchmark Task										
Task Name: Basic Sy	stem Benchmark	Description:	Default system	benchmark task						
Frequency	Device Scope	Retrieve Liv	e Data	CLI Commar	ds	Additional Oper	ations after Benchn	ark	Plugins	Summary
∨ Update MPLS Clo	ud									
Enable	Operatio	n Name								
	Recalculat	e Cloud								
	Recalculat	e Cloud NCT								
✓ Update Public Clo	oud									
Enable	Operatio	n Name								
~	Recalcula	ate AWS Virtual R	oute Table							
	Recalcula	ate Azure Virtual	Route Table							

9. Using REST API to Manage AWS Data

If your organization has hundreds or even thousands of accounts, you can use the corresponding REST APIs to add these accounts to the system and manage your AWS accounts. This chapter illustrates the main flow and explains how to use these APIs.

For a complete list of APIs, refer to <u>https://github.com/NetBrainAPI/NetBrain-REST-API-</u><u>R10/tree/master/REST%20APIs%20Documentation/API%20Server%20Management.</u>

Onboarding New Accounts:



If you want to have the scripts integrated into your account onboarding process, you can use the REST APIs to perform the following tasks after adding the new accounts:

- Add AWS Accounts to NetBrain: You will need to define your strategy to choose what types of accounts to add to NetBrain, either by using the tag or OU (organizational unit) as a filter based on your preference.
- Update Schedule Discovery Tasks: After adding the AWS accounts into NetBrain, you will need to add these accounts into the scheduled discovery process.

Note: You only need to discover the new accounts once (when you add these new accounts to NetBrain). After the data of these accounts are discovered and initialized, you don't need to **discover them for a second time**. You can use the Rest API to query the discovery results (succeed or fail). If some accounts are discovered successfully, you could use the API to delete these accounts from the schedule discovery task.

Domain Management Tenant: Initial Tenant: Domain: R10 Training	Operations 👤	, Eddy.Zhao@net	0	NetB
Start Page Discover × Edit Discovery Task		_	×	
Schedule Discovery/Benchn Task Name: Scheduled System Discovery Description: Default scheduled discovery task				Refresh
Enable. Task Name Frequency Network Settings Discovery Seed Plugins Email Alerts		Summary		cope
Basic System Benchm. Discover All Live Network Discover Selected Live Network API Triggered Discovery				es;vCent
Update ESki topology Discover Devices via SNMP/CLI Network Settings				es;vCent
AWS Benchmark Method: Discover via Seed Routers Scan IP Range Access Mode: SNMP and SSH/Telnet Discovery Depth: IP/Hostname: e.g: 10.10.10.1; NY_R1 	Import IP List	~		es;AWS_I
Discover Devices via API + Select API Servers Unselect AII API Servers: AWS_Lab_Account_747895045325 AWS_Lab_Account_070113567925 AWS Lab				
Advanced Options				
				+

Update Schedule Benchmark Task: After the discovery process, the corresponding data for the AWS accounts will be added to the system. The system will then need to run the benchmark to update the AWS data. If you have selected certain AWS accounts for the discovery, you will need to add these newly added accounts to the benchmark scope, as shown in the screenshot below.

Task Name:	Basic System Benchmark	Description:	Default system	i benchmark ta	ask					
Frequency	Device Scope	Retrieve Li	ive Data	CLI Comn	nands Add	itional Operations	after Benchma	rk	F	Plugins
Select D	evice			🗹 Sele	ct external API servers t	o retrieve data				
O All D	evices 🔿 Device Group	⊖ Site		Items F	ound: 3 out of 9		Amazon AW	S	\sim	Search
	2(4)				API Source Type	Server Nam	e	EndPo	oints	Des
W	(4)				Amazon AWS	AWS_Lab_A	count_7478	74	125	The
🛃 Load	d Balancer(1)				Amazon AWS	AWS_Lab_A	count_0701	07	125	
😗 Rout	ter(30)				Amazon AWS	AWS Lab		04	\$55	
🏠 End	System(260)									
💋 Firev	wall(13)									
Clou	ud(16)									

Offboarding Old Accounts:



When you want to remove some AWS accounts that are not in use, you can use the REST APIs to remove these accounts and data from NetBrain.

- **Remove AWS API Instance Data**: You will need to call this API to remove the AWS API instance data so that all the data for the current AWS API Server will be removed from the NetBrain system.
- **Remove AWS API Server**: After successfully removing the AWS API instance data, you can safely remove the AWS API server, so this server will no longer be shown in the API Server Manager.

omain Management				Tenant: Initial T	enant Don	nain: R10 Training	Operations	💄 Ec
Start Page Discover × S	Schedule Task X API Serv	er Manager \times						
Items Found: 4 out of 68 + Add AP	Pl Server			Amazon AW	s v	Search	Q	B
API Source Type	Server Name	EndPoints	Description	Username	Front Server			Devie
Amazon AWS	AWS_Lab_Account_747	74789!	The Lab account that has config		fs28218(192	В)		234
	AWS_Lab_Account_07011	07011:			fs28218(192	В)		56
Amazon AWS	AWS Lab	04144			fs28218(192	В)		34
Amazon AWS a	aws-nt	http						0

9.1. Integration with AWS Organization

<u>Using REST API to Manage AWS Data</u> explains how you can use the REST API to integrate with the NetBrain system and update the AWS data. Sometimes you need to create scripts with these APIs to complete complex tasks and integrate them into your account onboarding/offboarding process. Instead of creating the integration scripts, you can use the NetBrain onboarding/offboarding tool to integrate with your AWS organization. (AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. Reference link: <u>https://aws.amazon.com/organizations/.</u>)

The architecture diagram is shown as follows:



The following requirements must be met to enable the proper function of the AWS onboarding/offboarding tool:

- The tool must have access to the AWS public endpoints to get the AWS organization data, and it can investigate the data to define what accounts can be added to NetBrain System.
- The tool must have access to the NetBrain web servers to use REST APIs defined in <u>Using REST API to</u> <u>Manage AWS Data</u> to update the AWS data.

Note: You can contact NetBrain Support to help you deploy the tool based on your specific requirements.

Configure Access to NetBrain and your AWS Organization

You will need to configure the access to both NetBrain and your AWS organization in **config.YAML**:



- Access to NetBrain: You must specify the NetBrain URL, username, password, tenant, domain, and the front server. Make sure the created user has domain management permission.
- Access to AWS Organization: You will need to specify the access method to the master accounts where the onboarding/offboarding tool can get the AWS organization info:
 - **Key-based Access**: Using the key-based access to configure the access key/secret key to access the AWS master account.
 - Role-based Access: Using the role-based access so the onboarding/offboarding tool can access the AWS master account.

You can use the combination of OU, accounts, and tag as the filter to only onboard specific accounts into the NetBrain system. The following rules should be obeyed:

- 1) **Select_ous**: Define the search scope and the function scope of excelude_ous, exclude_accounts, and exclude_tags. In most cases, select the OUs you want to onboard and do not leave them empty.
- 2) **Exclude_ous**: Define what OUs or subOUs you want to exclude.
- 3) **Exclude_accounts**: Define specific accounts you want to exclude.
- 4) **Exclude_tags**: Define tags so accounts with these tags won't be included. In most cases, you may want to exclude sandbox accounts or other types of accounts that you don't want to add to NetBrain.

The following diagram gives an overview of how the various conditions work together. The green color represents the entire organization tree. From there, you can define the select_ou to specify certain OUs you want to add to NetBrain. Within the selected OU group, you can use different types of excluding flags to exclude certain ous/accounts/tags. The final accounts added to NetBrain are the area shown in blue.



Access to the Master Accounts:

To access the master accounts and list all accounts within the current organization, you must configure the correct access policy. We have attached different policies for you to choose from based on your security considerations.

If your security team permits, you can use the board policy, which allows access to the entire organization:



Or, if you want more specific policies, you can use the following detailed policy:

```
₽{
     "Version": "2012-10-17",
     "Statement": [
Ł
              "Action": [
                  "organizations:DescribeOrganization",
                  "organizations:ListRoots",
                  "organizations:ListTagsForResource",
                  "organizations:ListOrganizationsUnitsForParent",
                 "organizations:ListAccountsForParent"
             ],
             "Effect": "Allow",
              "Resource": "*"
         }
     1
L,
```

There are two ways to access the master accounts: key-based access or role-based access:

Key-based access to the Master Account

If you use the key-based access to access the master account, list organization information, select the access method as key-based access and configure the access key/secret key to the master accounts, NetBrain will access the master account and list the organization information.

```
aws_organizations:
    access_key_id: "key_id" # access key for master account to allow read access to accounts list in the organizations
    secret_key: "secret_key"
    #master_account_id: "635844821045" # master account id, for fs ec2 server to assum master account role
    #master_access_role_name: "ListOrganizationRole2" # access role for master account to allow read access to accounts list in the organizations
    #master_external_id: "netbrain"
    #mixed_mode_master_access_key_id: ""
    #mixed_mode_master_secret_key: ""
    access_role_name: "NetbrainAccessRole" # role name is member accounts to be assumed by Netbrain FrontServer for monitoring.
    external_id: "netbrain" # External ID required to assume the role.
    select_ous: # limit the OUS IDs to onboard. search the entire organizations if not specified.
    #- ou-la2c
```

Role-based Access to the Master Account

If you use role-based access to access the master account, list organization information, select the access method as role-based access and configure the role and other details, NetBrain will access the master account and list the organization information.

10. Appendix

10.1. NetBrain requires AWS IAM permissions?

11	{
	"Version": "2012-10-17"
	"Statement": [
	{
12.	"Action": [
13.	"autoscaling:Describe*",
14.	"autoscaling-plans:Describe*",
15.	"autoscaling-plans:GetScalingPlanResourceForecastData",
16.	"cloudwatch:Describe*",
17.	"cloudwatch:Get*",
18.	"cloudwatch:List*",
19.	"directconnect:Describe*",
20.	"ec2:Describe*",
21.	"ec2:Get*",
22.	"ec2:SearchTransitGatewayRoutes",
23.	"network-firewall:DescribeFirewall",
24.	"network-firewall:DescribeFirewallPolicy",
25.	"network-firewall:DescribeRuleGroup",
26.	"network-firewall:ListFirewallPolicies",
27.	"network-firewall:ListFirewalls",
28.	"network-firewall:ListRuleGroups",
29.	"network-firewall:ListTagsForResource",
30.	"elasticloadbalancing:Describe*"
31.],
32.	"Effect": "Allow",
33.	"Resource": "*"
34.	}
35.]
	}