Amazon Virtual Private Cloud

VPC Reachability Analyzer

Amazon Virtual Private Cloud: VPC Reachability Analyzer

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is VPC Reachability Analyzer?

VPC Reachability Analyzer is a configuration analysis tool that enables you to perform connectivity testing between a source resource and a destination resource in your virtual private clouds (VPCs). When the destination is reachable, Reachability Analyzer produces hop-by-hop details of the virtual network path between the source and the destination. When the destination is not reachable, Reachability Analyzer identifies the blocking component. For example, paths can be blocked by configuration issues in a security group, network ACL, route table, or load balancer.

For more information, see How Reachability Analyzer works (p. 2).

Use cases

You can use Reachability Analyzer to do the following:

- Troubleshoot connectivity issues caused by network misconfiguration.
- Verify that your network configuration matches your intended connectivity.
- Automate the verification of your connectivity intent as your network configuration changes.

Working with Reachability Analyzer

You can use any of the following interfaces to work with Reachability Analyzer:

- **AWS Management Console** — A web interface for AWS services, including Reachability Analyzer.
- **AWS Command Line Interface (AWS CLI)** — Provides commands for AWS services, including Reachability Analyzer. The AWS CLI is supported on Windows, macOS, and Linux. For more information, see the AWS Command Line Interface User Guide.
- **AWS CloudFormation** — Enables you to create templates that describe your AWS resources. You use a template to provision and manage AWS resources as a single unit. For more information, see the following resources: AWS::EC2::NetworkInsightsAnalysis and AWS::EC2::NetworkInsightsPath.
- **AWS SDKs** — Provides language-specific APIs and takes care of many of the connection details, such as calculating signatures, handling request retries, and handling errors. For more information, see AWS SDKs.
- **Query API** — Provides low-level API actions that you call using HTTPS requests. Using the Query API is the most direct way to access Reachability Analyzer. However, the Query API requires that your application handle low-level details such as generating the hash to sign the request, and handling errors. For more information, see the Amazon EC2 API Reference.

Pricing

You are charged per analysis run between a source and destination. For more information, see Pricing.

How VPC Reachability Analyzer works

VPC Reachability Analyzer analyzes the path between a source and destination by building a model of the network configuration, and then checking for reachability based on the configuration. It does not send packets or analyze the data plane.

To use Reachability Analyzer, you specify the path for the traffic from a source to a destination. For example, you could specify an internet gateway as the source, an EC2 instance as the destination, 22 as the destination port, and TCP as the protocol. This would allow you to verify that you can connect to the EC2 instance through the internet gateway using SSH.

If there are multiple reachable paths between a source and a destination, Reachability Analyzer identifies and displays the shortest path. You can analyze the path again, specifying an intermediate component, to find an alternative reachable path that traverses the intermediate component.

If the path is not reachable, Reachability Analyzer displays information about the component or combination of components that is blocking the path. There might be additional components blocking the path.

Contents

Source and destination resources

The source and destination resources must be owned by the same AWS account and must be in the same Region. The source and destination resources must be in the same VPC or in VPCs that are connected through a VPC peering connection. In the case of a shared VPC the resources must be owned by the same AWS account.

Reachability Analyzer supports the following resource types as sources and destinations:

- Instances
- Internet gateways
- Network interfaces
- Transit gateways
- Transit gateway attachments
- VPC endpoints
- VPC peering connections
- VPN gateways

Intermediate components

Reachability Analyzer supports the following resource types as intermediate components:

- Load balancers (except for Gateway Load Balancers)
- NAT gateways
- Transit gateways
- Transit gateway attachments
- VPC peering connections

Path components

The following resource types can appear in reachable paths and in explanations when a path is not reachable:

- EC2 instances
- Internet gateways
- Load balancers (except for Gateway Load Balancers)
- NAT gateways
- Network ACLs
- Network interfaces
- Prefix lists
- Route tables
- Security groups
- Subnets
- Target groups
- Transit gateways
- Transit gateway attachments
- Transit gateway route tables
- Virtual private gateways
- VPC endpoints
- VPC gateway endpoints
- VPC peering connections
- VPCs
- VPN connections

Limitations

- Transit gateway Connect attachments are not supported. Reachability Analyzer analyzes connectivity only up to these attachments.
- With the TCP protocol, when a network path traverses a transit gateway route table, only forward traffic is analyzed.
- Reachability Analyzer can find paths through at most two transit gateway route tables. To analyze paths through additional transit gateway route tables, use Route Analyzer. For more information, see Route Analyzer in the *Amazon VPC Transit Gateways* guide.

IP addresses

Reachability Analyzer supports only resources with an IPv4 address. If a resource has both IPv4 and IPv6 addresses, Reachability Analyzer includes only the IPv4 addresses in its analysis.

Shared resources

Reachability Analyzer supports shared resources only if they can be fully described by the calling principal. For example, if a route references a prefix list owned by another account, the owner must share the prefix list with the calling principal for the analysis to succeed.

Resource configuration

Use the following documentation to help you update the configuration of your network resources:

- Elastic network interfaces
- Internet gateways
- Load balancers and target groups
  - Application Load Balancers
  - Classic Load Balancers
  - Network Load Balancers
- Network ACLs
- Route tables
- Security groups for Linux instances
- Security groups for Windows instances
- Transit gateways
- VPC peering configurations
- VPN connections

Getting started with VPC Reachability Analyzer

You can use VPC Reachability Analyzer to determine whether a destination resource in your virtual private cloud (VPC) is reachable from a source resource. To get started, you specify a source and a destination. For example, you can run a reachability analysis between two network interfaces or between a network interface and a gateway. If there is a reachable path between the source and destination, Reachability Analyzer displays the details. Otherwise, Reachability Analyzer identifies the blocking component.

Tasks

Before you begin

Verify that your source and destination resources meet the following requirements.

- The following resources types are supported as sources and destinations:
  - Instances
  - Internet gateways
  - Network interfaces
  - Transit gateways
  - Transit gateway attachments
  - VPC endpoints
  - VPC peering connections
  - VPN gateways
- The source and destination resources must be owned by the same AWS account.
- The source and destination resources must be in the same Region.
- The source and destination resources must be in the same VPC or in VPCs that are connected through a VPC peering connection. In the case of a shared VPC, the resources must be owned by the same AWS account.

Step 1: Create and analyze a path

Specify the path for the traffic from a source to a destination. After you create the path, Reachability Analyzer analyzes the path once. You can analyze a path at any time to determine whether your intended connectivity is supported, even as your network configuration changes.

To create a path

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Reachability Analyzer**.
3. Choose **Create and analyze path**.
4. (Optional) For **Name tag**, enter a descriptive name for the analysis.
5. To specify the source resource, choose the resource type from **Source type**, and then choose the specific resource from **Source**.

   For components that support multiple IP addresses, such as instances, you can optionally enter a private IP address for **Source IP address**. By default, Reachability Analyzer considers all IP addresses.
6. To specify the destination resource, choose the resource type from **Destination type**, and then choose the specific resource from **Destination**.

   For components that support multiple IP addresses, such as instances, you can optionally enter a private IP address for **Destination IP address**. By default, Reachability Analyzer considers all IP addresses.
7. (Optional) Enter the port number for **Destination port**. By default, Reachability Analyzer considers all ports.
8. For **Protocol**, choose **TCP** or **UDP**.
9. (Optional) To add a tag, choose **Add new tag** and then enter the tag key and tag value.
10. Choose **Create and analyze path**.

Step 2: View the results of the path analysis

After the path analysis completes, you can view the results.

To view the results of a path analysis

1. Choose the ID of the path in the **Path ID** column to view the path details page.
2. In the **Analysis explorer** panel, find **Reachability status** and check whether it is **Reachable** or **Not reachable**. If the path is reachable, the console displays the shortest route found between the source and destination. Otherwise, expand **Explanations**, **Details** for information about the blocking component.
3. If the reachability status matches your intent, there is no further action required. Consider running the analysis again if you change your network configuration so that you can ensure that the reachability status still matches your intent. Otherwise, proceed to Step 3 (p. 6).

Step 3: Change the network configuration and analyze the path

If the reachability status does not match your intent, you can change your network configuration. Then you can analyze the path again to confirm that the reachability status matches your intent.

To restore connectivity for a path that is not reachable

1. The **Analysis explorer** panel includes an explanation code (p. 15) and detailed information about the component or combination of components that is blocking the path (under **Explanations**, **Details**). For example, in the following explanation, the security group shown does not have an inbound rule that allows the traffic to reach the destination EC2 instance:

Explanations

None of the ingress rules in the following security groups apply: sg-0a9cd30aba504dc16.

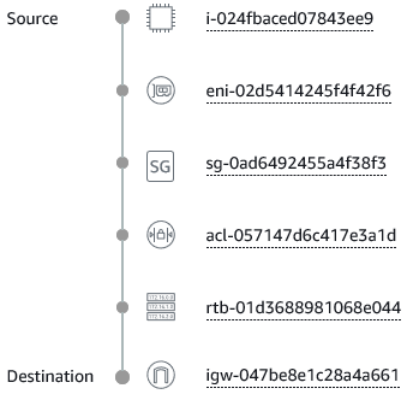
▼ Details


```
{
  "direction": "ingress",
  "explanationCode": "ENI_SG_RULES_MISMATCH",
  "networkInterface": {
    "arn": "arn:aws:ec2:us-east-1:123456789012:network-interface/eni-0628508ba821c1009",
    "id": "eni-0628508ba821c1009"
  },
  "securityGroups": [
    {
      "arn": "arn:aws:ec2:us-east-1:123456789012:security-group/sg-0a9cd30aba504dc16",
      "id": "sg-0a9cd30aba504dc16"
    }
  ],
  "subnet": {
    "arn": "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-0a7bd12d516760099",
    "id": "subnet-0a7bd12d516760099"
  },
  "vpc": {
    "arn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-0244168bae214ad2d",
    "id": "vpc-0244168bae214ad2d"
  }
}
```


2. Update the configuration of the component so that the desired traffic can traverse the component.
3. Choose **Analyze path** to confirm that the path is now reachable. You can optionally specify the Amazon Resource Name (ARN) of a resource that the path must traverse. The following are supported as intermediate components: load balancers, NAT gateways, and VPC peering connections.

To remove connectivity for a reachable path

1. The **Analysis explorer** panel includes a visual representation of the shortest route found between the source and destination. It includes all components between the source and destination. For example, the following diagram shows the components that traffic traverses from the source EC2 instance to the destination internet gateway:



2. Identify the component that is overly permissive and update its configuration.
3. Choose **Analyze path** to confirm that the path is no longer reachable.

Getting started with VPC Reachability Analyzer using the AWS CLI

You can use VPC Reachability Analyzer to determine whether a destination resource in your virtual private cloud (VPC) is reachable from a source resource. To get started, you specify a source and a destination. For example, you can run a reachability analysis between two network interfaces or between a network interface and a gateway. If there is a reachable path between the source and destination, Reachability Analyzer displays the details. Otherwise, Reachability Analyzer identifies the blocking component.

Tasks

Before you begin

Verify that your source and destination resources meet the following requirements.

- The following resources types are supported as sources and destinations:
  - Instances
  - Internet gateways
  - Network interfaces
  - Transit gateways
  - Transit gateway attachments
  - VPC endpoints
  - VPC peering connections
  - VPN gateways
- The source and destination resources must be owned by the same AWS account.
- The source and destination resources must be in the same Region.
- The source and destination resources must be in the same VPC or in VPCs that are connected through a VPC peering connection. In the case of a shared VPC, the resources must be owned by the same AWS account.

Step 1: Create a path

Use the following create-network-insights-path command to create a path. In this example, the source is an internet gateway and the destination is an EC2 instance.

```
aws ec2 create-network-insights-path --source igw-0797cccdc9d73b0e5 --
destination i-0495d385ad28331c7 --destination-port 22 --protocol TCP
```

The following is example output.

```
{
    "NetworkInsightsPaths": {
        "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
        "NetworkInsightsPathArn": "arn:aws:ec2:us-east-1:123456789012:network-insights-
path/nip-0b26f224f1d131fa8",
        "CreatedDate": "2021-01-20T22:43:46.933Z",
        "Source": "igw-0797cccdc9d73b0e5",
        "Destination": "i-0495d385ad28331c7",
        "Protocol": "tcp"
    }
}
```

Step 2: Analyze the path

Use the following start-network-insights-analysis command to determine whether the destination is reachable using the protocol and port that you specified for the path. The analysis can take a few minutes to complete.

```
aws ec2 start-network-insights-analysis --network-insights-path-id nip-0b26f224f1d131fa8
```

The following is example output.

```
{
    "NetworkInsightsAnalysis": {
        "NetworkInsightsAnalysisId": "nia-02207aa13eb480c7a",
        "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-east-1:123456789012:network-insights-
analysis/nia-02207aa13eb480c7a",
        "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
        "StartDate": "2021-01-20T22:58:37.495Z",
        "Status": "running"
    }
}
```

Step 3: Get the results of the path analysis

After the path analysis completes, you can view the results using the describe-network-insights-analyses command.

```
aws ec2 describe-network-insights-analyses --network-insights-analysis-
ids nia-02207aa13eb480c7a
```

Example 1: Not reachable

The following is example output where the path is not reachable. When a path is not reachable, `NetworkPathFound` is `false` and `ExplanationCode` contains an explanation code. For descriptions of the explanation codes, see VPC Reachability Analyzer explanation codes (p. 15). In this example, `ENI_SG_RULES_MISMATCH` indicates that the security group does not allow the traffic. After you add

a rule to the security group to allow the traffic, you can reanalyze the same path and confirm that it is reachable.


```
{
    "NetworkInsightsAnalyses": [
        {
            "NetworkInsightsAnalysisId": "nia-02207aa13eb480c7a",
            "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-east-1:123456789012:network-
insights-analysis/nia-02207aa13eb480c7a",
            "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
            "StartDate": "2021-01-20T22:58:37.495Z",
            "Status": "succeeded",
            "NetworkPathFound": false,
            "Explanations": [
                {
                    "Direction": "ingress",
                    "ExplanationCode": "ENI_SG_RULES_MISMATCH",
                    "NetworkInterface": {
                        "Id": "eni-0a25edef15a6cc08c",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a25edef15a6cc08c"
                    },
                    "SecurityGroups": [
                        {
                            "Id": "sg-02f0d35a850ba727f",
                            "Arn": "arn:aws:ec2:us-east-1:123456789012:security-group/
sg-02f0d35a850ba727f"
                        }
                    ],
                    "Subnet": {
                        "Id": "subnet-004ff41eccb4d1194",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-004ff41eccb4d1194"
                    },
                    "Vpc": {
                        "Id": "vpc-f1663d98ad28331c7",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-
f1663d98ad28331c7"
                    }
                }
            ],
            "Tags": []
        }
    ]
}
```


Example 2: Reachable

The following is example output where the path is reachable. When a path is reachable, `NetworkPathFound` is `true`, `ForwardPathComponents` contains component-by-component details about the shortest reachable path from source to destination, and `ReturnPathComponents` contains component-by-component details about the shortest reachable path from destination to source.


```
{
    "NetworkInsightsAnalyses": [
        {
            "NetworkInsightsAnalysisId": "nia-076744f74a04c3c7f",
            "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-west-2:123456789012:network-
insights-analysis/nia-076744f74a04c3c7f",
            "NetworkInsightsPathId": "nip-0614b9507b4e3e989",
            "StartDate": "2021-01-20T23:47:08.080Z",
            "Status": "succeeded",
            "NetworkPathFound": true,
```

```
            "ForwardPathComponents": [
                {
                    "SequenceNumber": 1,
                    "Component": {
                        "Id": "igw-0797cccdc9d73b0e5",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:internet-gateway/
igw-0797cccdc9d73b0e5"
                    },
                    "OutboundHeader": {
                        "DestinationAddresses": [
                            "10.0.2.87/32"
                        ]
                    },
                    "InboundHeader": {
                        "DestinationAddresses": [
                            "35.161.108.53/32"
                        ],
                        "DestinationPortRanges": [
                            {
                                "From": 443,
                                "To": 443
                            }
                        ],
                        "Protocol": "6",
                        "SourceAddresses": [
                            "0.0.0.0/5",
                            "11.0.0.0/8",
                            "12.0.0.0/6",
                            ...
                        ],
                        "SourcePortRanges": [
                            {
                                "From": 0,
                                "To": 65535
                            }
                        ]
                    }
                },
                {
                    "SequenceNumber": 2,
                    "AclRule": {
                        "Cidr": "0.0.0.0/0",
                        "Egress": false,
                        "Protocol": "all",
                        "RuleAction": "allow",
                        "RuleNumber": 100
                    },
                    "Component": {
                        "Id": "acl-f3663d9a",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-acl/acl-
f3663d9a"
                    }
                },
                {
                    "SequenceNumber": 3,
                    "Component": {
                        "Id": "sg-02f0d35a850ba727f",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:security-group/
sg-02f0d35a850ba727f"
                    },
                    "SecurityGroupRule": {
                        "Cidr": "0.0.0.0/0",
                        "Direction": "ingress",
                        "PortRange": {
                            "From": 443,
                            "To": 443
```

```
                        },
                        "Protocol": "tcp"
                    }
                },
                {
                    "SequenceNumber": 4,
                    "Component": {
                        "Id": "eni-0a25edef15a6cc08c",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-interface/
eni-0a25edef15a6cc08c"
                    },
                    "Subnet": {
                        "Id": "subnet-004ff41eccb4d1194",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-004ff41eccb4d1194"
                    },
                    "Vpc": {
                        "Id": "vpc-f1663d98ad28331c7",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:vpc/vpc-
f1663d98ad28331c7"
                    }
                },
                {
                    "SequenceNumber": 5,
                    "Component": {
                        "Id": "i-0626d4edd54f1286d",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-0626d4edd54f1286d"
                    }
                }
            ],
            "ReturnPathComponents": [
                {
                    "SequenceNumber": 1,
                    "Component": {
                        "Id": "i-0626d4edd54f1286d",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-0626d4edd54f1286d"
                    },
                    "OutboundHeader": {
                        "DestinationAddresses": [
                            "0.0.0.0/5",
                            "11.0.0.0/8",
                            "12.0.0.0/6",
                            ...
                        ],
                        "DestinationPortRanges": [
                            {
                                "From": 0,
                                "To": 65535
                            }
                        ],
                        "Protocol": "6",
                        "SourceAddresses": [
                            "10.0.2.87/32"
                        ],
                        "SourcePortRanges": [
                            {
                                "From": 443,
                                "To": 443
                            }
                        ]
                    }
                },
                {
                    "SequenceNumber": 2,
```

```
                    "Component": {
                        "Id": "eni-0a25edef15a6cc08c",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-interface/
eni-0a25edef15a6cc08c"
                    },
                    "Subnet": {
                        "Id": "subnet-004ff41eccb4d1194",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-004ff41eccb4d1194"
                    },
                    "Vpc": {
                        "Id": "vpc-f1663d98ad28331c7",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:vpc/vpc-
f1663d98ad28331c7"
                    }
                },
                {
                    "SequenceNumber": 3,
                    "Component": {
                        "Id": "sg-02f0d35a850ba727f",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:security-group/
sg-02f0d35a850ba727f"
                    }
                },
                {
                    "SequenceNumber": 4,
                    "AclRule": {
                        "Cidr": "0.0.0.0/0",
                        "Egress": true,
                        "Protocol": "all",
                        "RuleAction": "allow",
                        "RuleNumber": 100
                    },
                    "Component": {
                        "Id": "acl-0a8e20a0a9f144d36",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-acl/
acl-0a8e20a0a9f144d36"
                    }
                },
                {
                    "SequenceNumber": 5,
                    "Component": {
                        "Id": "rtb-0d49a54c0a8c0bd9b",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:route-table/
rtb-0d49a54c0a8c0bd9b"
                    },
                    "RouteTableRoute": {
                        "DestinationCidr": "0.0.0.0/0",
                        "GatewayId": "igw-0797cccdc9d73b0e5",
                        "Origin": "createroute"
                    }
                },
                {
                    "SequenceNumber": 6,
                    "Component": {
                        "Id": "igw-0797cccdc9d73b0e5",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:internet-gateway/
igw-0797cccdc9d73b0e5"
                    },
                    "OutboundHeader": {
                        "SourceAddresses": [
                            "35.161.108.53/32"
                        ]
                    }
                }
            ],
```

```
            "Tags": []
        }
    ]
}
```

VPC Reachability Analyzer explanation codes

If a destination is not reachable, Reachability Analyzer provides one or more explanation codes to help you diagnose and address network misconfiguration.

Contents

Path is not reachable

If you receive one of these explanation codes, the path analysis determined that the path is not reachable.

BAD_STATE

This component is not in a functional state.

BAD_STATE_ATTACHMENT

The attachment between these components is not in a functional state.

BAD_STATE_ROUTE

This route is not in a functional state.

BAD_STATE_VPN

This VPN connection is not in a functional state.

CANNOT_ROUTE

This route can't transmit traffic because its destination CIDR or prefix list does not match the destination address of the packet.

COMPONENT_FILTER_RESTRICTION

The source, destination, or intermediate components specified for the path prevent some components from being used.

ELB_ACL_RESTRICTION

Classic Load Balancers apply network ACLs to outbound traffic, even if it's destined for a target in the same subnet as the load balancer.

ELB_INSTALLED_AZ_RESTRICTION

This load balancer can send traffic only to targets in Availability Zones that are enabled for the load balancer.

ELB_LISTENER_PORT_RESTRICTION

This Classic Load Balancer listener allows only inbound traffic destined for the specified port, and outbound traffic with the specified destination port.

ELB_LISTENERS_MISMATCH

This Classic Load Balancer does not have a listener that accepts the traffic.

ELB_NOT_CROSSZONE

This load balancer can't send traffic to some targets because cross-zone load balancing is disabled.

ELBV2_LISTENER_HAS_NO_TG

This listener is associated with target groups that have no targets.

ELBV2_LISTENER_PORT_RESTRICTION

This listener does not accept traffic unless it has the specified destination port.

ELBV2_LISTENER_REQUIRES_TG_ACCEPT

This listener does not have a target group that accepts the traffic.

ELBV2_LISTENERS_MISMATCH

This load balancer does not have a listener that accepts the traffic.

ELBV2_SOURCE_ADDRESS_PRESERVATION

If source address preservation is enabled, the outgoing source address is unaltered while traversing the Network Load Balancer.

ENI_ADDRESS_RESTRICTION

This network interface does not allow inbound or outbound traffic unless the source or destination address matches its private IP address.

ENI_SG_RULES_MISMATCH

This security group has no inbound or outbound rules that apply.

ENI_SOURCE_DEST_CHECK_RESTRICTION

Network interfaces with source/destination check enabled reject inbound traffic if the destination address does not match one of its private IP addresses, and reject outbound traffic if the source address does not match one of their private IP addresses.

GATEWAY_REJECTS_SPOOFED_TRAFFIC

Gateways reject traffic from network interfaces if the source IP address is not a public IP address associated with the network interface.

HIGHER_PRIORITY_ROUTE

This route table contains a route to the destination that can't be used because there is a higher priority route with the same destination CIDR.

IGW_DESTINATION_ADDRESS_IN_VPC_CIDRS

Internet gateways accept traffic only if the destination address is within the VPC CIDR block.

IGW_DESTINATION_ADDRESS_NOT_IN_RFC1918_EGRESS

Internet gateways reject outbound traffic with destination addresses in the private IP address range (see RFC1918).

IGW_NAT_REFLECTION

Internet gateways do not model NAT reflection. Without NAT reflection, traffic originating in a VPC and destined for the public IP address of an instance in the same VPC can't be redirected back to the VPC.

IGW_PRIVATE_IP_ASSOCIATION_FOR_INGRESS

Internet gateways reject inbound traffic with a destination address that is not the public IP address of a network interface in the VPC with an available attachment.

IGW_PUBLIC_IP_ASSOCIATION_FOR_EGRESS

Traffic can't reach the internet through the internet gateway if the source address is not paired with a public IP address or if the source address does not belong to a network interface in the VPC with an available attachment.

IGW_SOURCE_ADDRESS_NOT_IN_RFC1918_INGRESS

Internet gateways reject inbound traffic with source addresses in the private IP address range (see RFC1918).

INGRESS_RTB_NO_PUBLIC_IP

A middlebox appliance can't receive traffic from the internet through an ingress route table if it does not have a public IP address.

INGRESS_RTB_TRAFFIC_REDIRECTION

Subnets whose traffic is redirected to a middlebox appliance can't use a direct route to the internet gateway even when the subnet route table provides one.

MORE_SPECIFIC_ROUTE

The specified route can't be used to transmit traffic because there is a more specific route that matches.

NGW_DEST_ADDRESS_PRESERVATION

NAT gateways do not alter destination addresses.

NGW_REQUIRES_SOURCE_IN_VPC

NAT gateways can only transmit traffic that originates from network interfaces within the same VPC. NAT gateways can't transmit traffic that originates from peering connections, VPN connections, or AWS Direct Connect.

NGW_SOURCE_ADDRESS_REASSIGN

NAT gateways transform the source's addresses in outbound traffic to match its private IP address.

NO_POSSIBLE_DESTINATION

The network component can't deliver the packet to any possible destination.

NO_ROUTE_TO_DESTINATION

The route table does not have an applicable route to the destination resource.

PCX_REQUIRES_ADDRESS_IN_VPC_CIDR

Traffic can traverse this peering connection only if the destination or source address is within the CIDR block of the destination VPC.

PROTOCOL_RESTRICTION

This component only accepts traffic with specific protocols.

REMAP_EPHEMERAL_PORT

Outbound traffic from a NAT gateway or load balancer has the source port remapped to an ephemeral port in the range [1024–65535].

SG_HAS_NO_RULES

This security group has no inbound or outbound rules.

SUBNET_ACL_RESTRICTION

Inbound or outbound traffic for a subnet must be admitted by the network ACL for the subnet.

TARGET_ADDRESS_RESTRICTION

This target group can only emit packets that are destined for the target address.

TARGET_PORT_RESTRICTION

This target group can only route traffic that's destined for the target port.

TGW_ATTACH_MISSING_TGW_RTB_ASSOCIATION

This transit gateway attachment doesn't have a valid transit gateway route table association.

TGW_ATTACH_VPC_AZ_RESTRICTION

Traffic from a VPC attachment in the default mode can't be forwarded to the network interface in this Availability Zone because it comes from an Availability Zone where the attachment has a different network interface. Traffic from a VPC attachment in appliance mode can't be forwarded to the network interface in this Availability Zone because on the forward path it used a different Availability Zone.

TGW_BAD_STATE_VPN

This VPN connections is in a non-functional state.

TGW_ROUTE_AZ_RESTRICTION

This transit gateway is not registered in the Availability Zone where the traffic originates.

TGW_RTB_BAD_STATE_ROUTE

This transit gateway route table has a route to the destination that is in a bad state.

TGW_RTB_CANNOT_ROUTE

This transit gateway route table has a route to the intended destination, but the route does not match the package destination address.

TGW_RTB_HIGHER_PRIORITY_ROUTE

This transit gateway route table contains a route to the intended destination that can't be used because there is a higher-priority route with the same destination CIDR.

TGW_RTB_MORE_SPECIFIC_ROUTE

This transit gateway route table has a route to the destination, but there is a more specific route.

TGW_RTB_NO_ROUTE_TO_TGW_ATTACHMENT

This transit gateway route table has no route to this transit gateway attachment.

TGW_RTB_ROUTES_ARE_UNKNOWN

The routes of this transit gateway route table are not known. This might be due to an internal error or because the transit gateway route table does not belong to the account running the analysis.

UNKNOWN_DESTINATION

The path can't be extended because the information about the destination is insufficient.

UNKNOWN_PEERED_SGS

One of the VPCs in the VPC peering connection is unknown. This is typically because the VPC is in a different account. Access controls referencing security groups are treated as inaccessible and deny traffic crossing this peering connection.

VGW_PRIVATE_IP_ASSOCIATION_FOR_EGRESS

Virtual private gateways can't accept outbound traffic if the source address does not belong to a network interface in the VPC with an available attachment.

VGW_PRIVATE_IP_ASSOCIATION_FOR_INGRESS

Virtual private gateways can't accept inbound traffic if the destination address is not the private IP address of a network interface in the VPC with an available attachment.

VPC_LOCAL_ROUTE_CIDR_RESTRICTION

Local routes apply only to packets with a destination address within the VPC CIDR block.

VPCE_GATEWAY_EGRESS_SOURCE_ADDRESS_RESTRICTION

VPC gateway endpoints emit only traffic with source addresses within the CIDRs of their corresponding prefix lists.

VPCE_GATEWAY_PROTOCOL_RESTRICTION

VPC gateway endpoints accept only TCP or ICMP ECHO traffic, and emit only TCP or ICMP ECHO reply traffic.

Request not valid

If you receive one of these explanation codes, the specified request is not valid and no path is possible.

DISCONNECTED_VPCS

The source and destination are in separate VPCs that are not connected by a supported resource.

NO_PATH

There is no path from the source to the destination.

NO_SOURCE_OR_DESTINATION

The source or destination resource does not exist.

UNASSOCIATED_COMPONENT

The component is not associated with a VPC in your account (for example, a recently terminated instance), or none of its network interfaces has an IPv4 address.

UNSUPPORTED_COMPONENT

The component is not supported by Reachability Analyzer.

Identity and access management for VPC Reachability Analyzer

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Reachability Analyzer resources. IAM is an AWS service that you can use with no additional charge.

To use VPC Reachability Analyzer, you need an AWS account and AWS credentials. To increase the security of your AWS account, we recommend that you use an *IAM user* to provide access credentials instead of using your AWS account credentials. For more information, see AWS account root user credentials vs. IAM user credentials in the *Amazon Web Services General Reference* and IAM best practices in the *IAM User Guide*.

For an overview of IAM users and why they are important for the security of your account, see AWS security credentials in the *Amazon Web Services General Reference*. For more information about working with IAM, see the *IAM User Guide*.

The following sections provide details on how an IAM administrator can use IAM to help secure your AWS resources, by controlling who can perform Reachability Analyzer actions.

Contents

How VPC Reachability Analyzer works with IAM

Before you use IAM to manage access to VPC Reachability Analyzer, you should understand what IAM features are available to use with Reachability Analyzer. To get a high-level view of how Reachability Analyzer and other AWS services work with IAM, see AWS services that work with IAM in the *IAM User Guide*.

Contents

VPC Reachability Analyzer identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. VPC Reachability Analyzer supports specific actions and resources. There are no Reachability Analyzer service-specific condition keys that can be used in the `Condition` element of policy statements. To learn about all of the elements that you use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Reachability Analyzer shares its API namespace with Amazon EC2. Policy actions in Reachability Analyzer use the following prefix before the action: `ec2:`. For example, to grant someone permission to create a path with the `CreateNetworkInsightsPath` API operation, you include the `ec2:CreateNetworkInsightsPath` action in their policy. Policy statements must include either an `Action` or `NotAction` element.

To specify multiple actions in a single statement, separate them with commas as shown in the following example.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action.

```
"Action": "ec2:Describe*"
```

The following actions are supported by Reachability Analyzer:

- `CreateNetworkInsightsPath`
- `DeleteNetworkInsightsAnalysis`
- `DeleteNetworkInsightsPath`
- `DescribeNetworkInsightsAnalyses`
- `DescribeNetworkInsightsPaths`
- `StartNetworkInsightsAnalysis`

Resources

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

The following Reachability Analyzer API actions do not support resource-level permissions.

- `DescribeNetworkInsightsAnalyses`
- `DescribeNetworkInsightsPaths`

Condition keys

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. For example, you might want a policy to be applied only after a specific date. To express conditions, use predefined condition keys.

Reachability Analyzer does not provide any service-specific condition keys, but it does support using some global condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

All Amazon EC2 actions support the `aws:RequestedRegion` and `ec2:Region` condition keys. For more information, see Example: Restricting Access to a Specific Region.

The `Condition` element is optional.

Authorization based on Reachability Analyzer tags

You can attach tags to Reachability Analyzer resources or pass tags in a request. To control access based on tags, you provide tag information in the condition element of a policy using the `ec2:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, or `aws:TagKeys` condition keys. For more information, see Granting permission to tag resources during creation, Controlling access to specific tags, and Controlling access to EC2 resources using resource tags in the *Amazon EC2 User Guide*.

Reachability Analyzer IAM roles

An IAM role is an entity within your AWS account that has specific permissions.

Using temporary credentials with Reachability Analyzer

You can use temporary credentials to sign in with federation, to assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Reachability Analyzer supports using temporary credentials.

Service-linked roles

Reachability Analyzer has no service-linked roles.

Service roles

Reachability Analyzer has no service roles.

Allow IAM users or groups to access VPC Reachability Analyzer

Any IAM user that signs in to the AWS Management Console or AWS Command Line Interface (AWS CLI) must have permissions to access specific resources. You provide those permissions by using AWS Identity and Access Management (IAM), through policies.

The following procedure shows you how to attach an IAM policy to your IAM user or group that allows full access to Reachability Analyzer.

Note
We recommend creating a new IAM policy that grants only the permissions necessary to use Reachability Analyzer.

Create an IAM policy

Create an IAM policy that provides IAM users full access to Reachability Analyzer. Then attach the policy to your IAM user or group.

To create and attach an IAM policy (console)

1. Sign in to the IAM console at https://console.aws.amazon.com/iam/ with administrator credentials.
2. In the navigation pane, choose **Policies**.
3. In the content pane, choose **Create policy**.
4. Choose the **JSON** tab.
5. Paste the following JSON policy document in the text field.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetTransitGatewayRouteTablePropagations",
                "ec2:DescribeTransitGatewayPeeringAttachments",
                "ec2:SearchTransitGatewayRoutes",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGatewayAttachments",
                "ec2:DescribeTransitGateways",
                "ec2:GetManagedPrefixListEntries",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRegions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeTags",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "tiros:CreateQuery",
```

```
                "tiros:GetQueryAnswer",
                "tiros:GetQueryExplanation",
                "ec2:CreateNetworkInsightsPath",
                "ec2:DescribeNetworkInsightsPaths",
                "ec2:DeleteNetworkInsightsPath",
                "ec2:StartNetworkInsightsAnalysis",
                "ec2:DescribeNetworkInsightsAnalyses",
                "ec2:DeleteNetworkInsightsAnalysis",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        }
    ]
}
```

6. When you are finished, choose **Review policy**.
7. On the **Review** page, enter a name for the policy, for example, `ReachabilityAnalyzerAccessPolicy`. Optionally, enter a description for **Description**.
8. In **Summary**, review the policy to see the permissions that it grants, and then choose **Create policy**.
9. Attach the new policy to your IAM user or group.

   For information on attaching a policy to a user, see Changing permissions for an IAM user in the *IAM User Guide*. For information on attaching a policy to a group, see Attaching a policy to an IAM Group in the *IAM User Guide*.

Required API permissions for VPC Reachability Analyzer

VPC Reachability Analyzer relies on data from other AWS services. The following permissions are used by Reachability Analyzer for various operations:

- `ec2:GetTransitGatewayRouteTablePropagations`
- `ec2:DescribeTransitGatewayPeeringAttachments`
- `ec2:SearchTransitGatewayRoutes`
- `ec2:DescribeTransitGatewayRouteTables`
- `ec2:DescribeTransitGatewayVpcAttachments`
- `ec2:DescribeTransitGatewayAttachments`
- `ec2:DescribeTransitGateways`
- `ec2:GetManagedPrefixListEntries`
- `ec2:DescribeManagedPrefixLists`
- `ec2:DescribeAvailabilityZones`
- `ec2:DescribeCustomerGateways`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeNatGateways`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribePrefixLists`
- `ec2:DescribeRegions`
- `ec2:DescribeRouteTables`

- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcPeeringConnections
- ec2:DescribeVpcs
- ec2:DescribeVpnConnections
- ec2:DescribeVpnGateways
- ec2:DescribeVpcEndpointServiceConfigurations
- elasticloadbalancing:DescribeListeners
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeLoadBalancerAttributes
- elasticloadbalancing:DescribeRules
- elasticloadbalancing:DescribeTags
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:DescribeTargetHealth
- tiros:CreateQuery
- tiros:GetQueryAnswer
- tiros:GetQueryExplanation
- ec2:CreateNetworkInsightsPath
- ec2:DescribeNetworkInsightsPaths
- ec2:DeleteNetworkInsightsPath
- ec2:StartNetworkInsightsAnalysis
- ec2:DescribeNetworkInsightsAnalyses
- ec2:DeleteNetworkInsightsAnalysis
- ec2:CreateTags
- ec2:DeleteTags

Networking-related describe calls

Reachability Analyzer uses various describe calls to resources in Amazon VPC, Amazon EC2, and Elastic Load Balancing to analyze and return information about a network configuration (such as a CIDR block, subnet, network interface, or security group). To access Reachability Analyzer, IAM users must also have the same API permissions.

Tiros API calls

If you monitor API calls, you might see calls to Tiros APIs. Tiros is a service that is only accessible by AWS services and that surfaces network reachability findings to Reachability Analyzer. Calls to the Tiros endpoint are required for Reachability Analyzer to function. To access Reachability Analyzer, IAM users must also have the same API permissions.

Reachability Analyzer API calls

The following permissions are required to call the Reachability Analyzer APIs. Users need these permissions to create and start analyzing a specified path for reachability, or to view and delete existing paths and analyses in your account. You must grant IAM users permission to call the Reachability Analyzer API actions they need.

- ec2:CreateNetworkInsightsPath
- ec2:DescribeNetworkInsightsPaths
- ec2:DeleteNetworkInsightsPath

- `ec2:StartNetworkInsightsAnalysis`
- `ec2:DescribeNetworkInsightsAnalyses`
- `ec2:DeleteNetworkInsightsAnalysis`

Tagging-related API calls

To tag or untag Reachability Analyzer resources, users need the following Amazon EC2 API permissions. To allow IAM users to work with tags, you must grant them permission to use the specific tagging actions they need.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Quotas for VPC Reachability Analyzer

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. You can request increases for some quotas, but not for all quotas.

To view the quotas for Reachability Analyzer, open the Service Quotas console. In the navigation pane, choose **AWS services**, and then select **Network Insights**. To request a quota increase, see Requesting a quota increase in the *Service Quotas User Guide*.

Your AWS account has the following quotas related to VPC Reachability Analyzer.

Name	Default	Adjustable
Paths	100	Yes
Analyses	1,000	Yes
Concurrent analyses	6	Yes

Document history for VPC Reachability Analyzer

The following table describes the releases for VPC Reachability Analyzer.

update-history-change	update-history-description	update-history-date
New feature (p. 28)	You can specify transit gateways and transit gateway route tables as sources, destinations, and intermediate path components.	March 25, 2022
Initial release (p. 28)	This release introduces Reachability Analyzer.	December 10, 2020