aws

Reachability Analyzer

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: Reachability Analyzer

This documentation is a draft for private preview for regions in the AWS European Sovereign Cloud. Documentation content will continue to evolve. Published: January 2, 2026.

Table of Contents

What is Reachability Analyzer?

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.

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.

Get started

To learn more about Reachability Analyzer, see *How Reachability Analyzer works*. For step-by-step directions using the AWS Management Console, see *Getting started*. For example commands using the AWS Command Line Interface (AWS CLI), see *Getting started using the CLI*.

Access Reachability Analyzer

You can use any of the following options to create and manage Reachability Analyzer resources:

- **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.
- **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** — Provide language-specific APIs and take 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 pricing details, open the Amazon VPC Pricing page, choose the **Network Analysis** tab, and find **Reachability Analyzer Pricing**.

How Reachability Analyzer works

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 or excluding 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 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 or a transit gateway. The source and destination resources can belong to different AWS accounts in the same organization from AWS Organizations.

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

- EC2 instances

- Internet gateways
- Network interfaces
- Transit gateways
- Transit gateway attachments
- Virtual private gateways
- VPC endpoint services
- VPC endpoints
- VPC peering connections

In addition, Reachability Analyzer supports IP addresses as destinations.

Intermediate components

Reachability Analyzer supports the following resource types as intermediate components. Specific intermediate components can be included or excluded from analysis when you're creating a path to analyse. See *Getting started* for more information.

- Load balancers
- NAT gateways
- AWS Network Firewall
- 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
- NAT gateways

- Network ACLs
- Network Firewall firewall
- Network interfaces
- Prefix lists
- Route tables
- Security groups
- Subnets
- Target groups
- Transit gateways
- Transit gateway attachments
- Transit gateway route tables
- Virtual private gateways
- VPC endpoint services
- VPC endpoints
- VPC gateway endpoints
- VPC peering connections
- VPCs
- VPN connections

Considerations

Consider the following when working with Reachability Analyzer:

- 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.
- If you enable trusted access, the delegated administrator account can create and delete paths that traverse owner and participant subnets within your organization from AWS Organizations. This account can also start and delete path analyses. For more information, see *Cross-account analyses*.
- Paths are not a shareable resource.
- 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.
- Paths through a Gateway Load Balancer endpoint do not include the Gateway Load Balancer or its targets. You should verify connectivity between the Gateway Load Balancer and its targets using a separate analysis.
- Reachability Analyzer does not consider the health of registered targets.
- Reachability Analyzer does not support Network Firewall rule groups that reference a resource group. In this case, the analysis fails.
- For a cross-account path through a Network Firewall firewall, the rule group must be created in the same delegated administrator account as the user running the analysis.
- Reachability Analyzer supports all stateful and stateless 5-tuple rules in Network Firewall. It doesn't support domain lists, Suricata rules, rule options, and tag-based resource groups. When Reachability Analyzer encounters an unsupported rule in Network Firewall, it provides an informational message in the path details.
- The packet header leaving the source and the packet header arriving at the destination can differ, due to intermediate components transforming the packets. For example, internet gateways and NAT gateways provide network address translation (NAT).
- Reachability Analyzer does not consider the advertised state of BYOIP address ranges. If a BYOIP address range is not advertised, resources that use these addresses might not be reachable from the internet.
- Reachability Analyzer does not report connectivity due to traffic mirroring.
- Reachability Analyzer automatically deletes an analysis 120 days after its creation date.
- Your account has quotas related to Reachability Analyzer. For more information, see *Quotas*.

Resource configuration

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

- Elastic network interfaces
- Firewalls (AWS Network Firewall)
- Internet gateways
- Load balancers and target groups (ELB)
  - Application Load Balancers

  - Classic Load Balancers
  - Gateway Load Balancers
  - Network Load Balancers
- Network ACLs
- Route tables
- Security groups for EC2 instances
- Transit gateways
- VPC endpoint services (AWS PrivateLink)
- VPC peering configurations
- VPN connections

Getting started with Reachability Analyzer

You can use 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

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 Network Manager console at https://eusc-de-east-1.console.amazonaws-eusc.eu/networkmanager/home.
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**.

   (Optional) You can filter the scope of the result based on the packet header leaving the source resource. For example, use the source and destination IP addresses and ports of interest. By default, the analysis considers all combinations of IP addresses and ports.

6. To specify the destination resource, choose the resource type from **Destination type**, and then choose the specific resource from **Destination**.

   (Optional) You can filter the scope of the result based on the packet header arriving at the destination resource. For example, use the source and destination IP addresses and ports of interest. By default, the analysis considers all combinations of IP addresses and ports.

7. For **Protocol**, choose **TCP** or **UDP**.
8. (Optional) To add a tag, choose **Add new tag** and then enter the tag key and tag value.
9. Choose **Create and analyze path**.

Step 2: Include or exclude intermediate resources

Reachability Analyzer supports the ability to include or exclude intermediate resources from analysis.

- Including a specified intermediate component makes it particularly valuable for security audits, policy enforcement, and compliance verification in cloud environments and enterprise networks. While this provides granular control over path analysis, note that it will only show paths that *include* the specified intermediate component, requiring good knowledge of the network topology for effective use.
- Excluding an intermediate component removes that component from analysis. This makes it particularly valuable when you don't want your analysis to include a particular component. For example, you might have a path that runs through AWS Network Firewall, but you only want to analyze paths that bypass it. In this case, you would add the Network Firewall ARN to the exclude field. Reachability Analyzer will then ignore this resource and analyze only those paths that don't go through it.

To include or exclude intermediate resources

1. Choose the checkbox for the path that you want to include or exclude Amazon Resource Numbers (ARNs) for.
2. On the **Analysis path** panel, enter an optional ARN for either of the following:

   - **Include an intermediate component feature**

     The analyzer only considers paths that include the specified intermediate component.

- **Exclude an intermediate component feature**

  The analyzer ignores a specific intermediate component during analysis and only analyzes alternate paths.

> **Note**
>
> You can only include a single ARN to include or exclude from analysis. Each ARN must be unique in order to prevent a conflict.

3. Choose **Confirm**.

Step 3: View the results of the path analysis

After the path analysis completes, you can view the result of the analysis.

To view the results of the 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.

Step 4: 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 and detailed information about the component or combination of components that is blocking the path (under **Explanations**,

Details). For example, in the following explanation, a security group is missing a required inbound rule.

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.

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 internet gateway to the destination EC2 instance.
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.

Step 5: Delete the path

If you no longer need the path, you can delete it. When you delete a path, you also delete all its analyses. If you keep the path, note that Reachability Analyzer will automatically delete the analysis 120 days after its creation date.

To delete the path

1. Open the Network Manager console at https://eusc-de-east-1.console.amazonaws-eusc.eu/networkmanager/home.
2. In the navigation pane, choose **Reachability Analyzer**.
3. Select the path.
4. Choose **Actions**, **Delete path**.
5. When prompted for confirmation, choose **Delete path**.

Getting started with Reachability Analyzer using the AWS CLI

You can use 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

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
    --protocol TCP
    --filter-at-source file://source-filter.json
```

The following is an example `source-filter.json`.

```
{
    "DestinationPortRange": {
        "FromPort": 22,
        "ToPort": 22
    }
}
```

The following is example output.

```
{
    "NetworkInsightsPaths": {
        "NetworkInsightsPathId": "nip-0b26f224f1d131fa8",
        "NetworkInsightsPathArn": "arn:aws:ec2:us-east-1:123456789012:network-insights-
path/nip-0b26f224f1d131fa8",
        "CreatedDate": "2023-03-20T22:43:46.933Z",
        "Source": "igw-0797cccdc9d73b0e5",
        "Destination": "i-0495d385ad28331c7",
        "SourceArn": "arn:aws:ec2:us-east-1:123456789012:internet-
gateway/0797cccdc9d73b0e5",
        "DestinationArn": "arn:aws:ec2:us-
east-1:123456789012:instance/0495d385ad28331c7",
        "Protocol": "tcp"
    }
}
```

To specify an IP address as the destination resource, omit the `--destination` parameter and filter on the destination address as follows.

```
aws ec2 create-network-insights-path
    --source igw-0797cccdc9d73b0e5
    --protocol TCP
    --filter-at-source file://source-filter.json
```

The following is an example of `source-filter.json`.

```
{
    "DestinationAddress": "34.230.71.227",
    "DestinationPortRange": {
        "FromPort": 22,
        "ToPort": 22
    }
}
```

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-0abc123def456789
```

The following is example output.

```
{
    "NetworkInsightsAnalysis": {
        "NetworkInsightsAnalysisId": "nia-0abc123def456789",
        "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-east-1:123456789012:network-
insights-analysis/nia-02207aa13eb480c7a",
        "NetworkInsightsPathId": "nip-0abc123def456789",
        "StartDate": "2023-03-20T22:58:37.495Z",
        "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-0abc123def456789
```

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 Reachability Analyzer explanation codes. 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-0abc123def456789",
            "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-west-2:123456789012:network-
insights-analysis/nia-0abc123def456789",
            "NetworkInsightsPathId": "nip-0abc123def456789",
            "FilterInArns": [
```

```
                "arn:aws:ec2:us-west-2:123456789012:vpc/vpc-0abc123def456789"
            ],
            "FilterOutArns": [
                "arn:aws:ec2:us-west-2:123456789012:internet-gateway/
igw-0abc123def456789"
            ],
            "StartDate": "2025-03-15T14:30:00.000Z",
            "Status": "succeeded",
            "StatusMessage": "Analysis completed successfully",
            "NetworkPathFound": false,
            "ForwardPathComponents": [
                {
                    "SequenceNumber": 1,
                    "Component": {
                        "Id": "i-0abc123def456789",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-0abc123def456789",
                        "Name": "Source Instance"
                    }
                },
                {
                    "SequenceNumber": 2,
                    "Component": {
                        "Id": "eni-0abc123def456789",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-interface/
eni-0abc123def456789",
                        "Name": "Source ENI"
                    }
                },
                {
                    "SequenceNumber": 3,
                    "Component": {
                        "Id": "subnet-0abc123def456789",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:subnet/
subnet-0abc123def456789",
                        "Name": "Private Subnet"
                    }
                }
            ],
            "Explanations": [
                {
                    "Direction": "ingress",
                    "ExplanationCode": "ENI_SG_RULES_MISMATCH",
                    "NetworkInterface": {
```

```
                        "Id": "eni-0def456789abc0123",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-interface/
eni-0def456789abc0123",
                        "Name": "Destination ENI"
                    },
                    "SecurityGroups": [
                        {
                            "Id": "sg-0abc123def456789",
                            "Arn": "arn:aws:ec2:us-west-2:123456789012:security-group/
sg-0abc123def456789",
                            "Name": "Source Security Group"
                        },
                        {
                            "Id": "sg-0def456789abc0123",
                            "Arn": "arn:aws:ec2:us-west-2:123456789012:security-group/
sg-0def456789abc0123",
                            "Name": "Destination Security Group"
                        }
                    ],
                    "Vpc": {
                        "Id": "vpc-0abc123def456789",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:vpc/
vpc-0abc123def456789",
                        "Name": "Main VPC"
                    },
                    "PacketField": "destination-port",
                    "Port": 443,
                    "Protocol": "tcp"
                }
            ],
            "AlternatePathHints": [
                {
                    "ComponentId": "sg-0fff111222333444",
                    "ComponentArn": "arn:aws:ec2:us-west-2:123456789012:security-group/
sg-0fff111222333444"
                }
            ],
            "Tags": [
                {
                    "Key": "Project",
                    "Value": "NetworkTroubleshooting"
                },
                {
                    "Key": "Environment",
```

```
                    "Value": "Production"
                }
            ]
        },
        {
            "NetworkInsightsAnalysisId": "nia-0def456789abc0123",
            "NetworkInsightsAnalysisArn": "arn:aws:ec2:us-west-2:123456789012:network-
insights-analysis/nia-0def456789abc0123",
            "NetworkInsightsPathId": "nip-0abc123def456789",
            "FilterInArns": [
                "arn:aws:ec2:us-west-2:123456789012:vpc/vpc-0abc123def456789"
            ],
            "FilterOutArns": [
                "arn:aws:ec2:us-west-2:123456789012:internet-gateway/
igw-0abc123def456789"
            ],
            "StartDate": "2025-04-10T09:45:00.000Z",
            "Status": "succeeded",
            "StatusMessage": "Analysis completed successfully",
            "NetworkPathFound": false,
            "ForwardPathComponents": [
                {
                    "SequenceNumber": 1,
                    "Component": {
                        "Id": "i-0def456789abc0123",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:instance/
i-0def456789abc0123",
                        "Name": "Source Instance"
                    }
                },
                {
                    "SequenceNumber": 2,
                    "Component": {
                        "Id": "eni-0def456789abc0123",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-interface/
eni-0def456789abc0123",
                        "Name": "Source ENI"
                    }
                }
            ],
            "Explanations": [
                {
                    "Direction": "ingress",
                    "ExplanationCode": "ENI_SG_RULES_MISMATCH",
```

```
                    "NetworkInterface": {
                        "Id": "eni-0fff111222333444",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:network-interface/
eni-0fff111222333444",
                        "Name": "Target Load Balancer ENI"
                    },
                    "SecurityGroupRule": {
                        "SecurityGroupId": "sg-0def456789abc0123",
                        "Direction": "ingress",
                        "PortRange": {
                            "From": 80,
                            "To": 80
                        },
                        "Protocol": "tcp",
                        "Cidr": "10.0.0.0/16"
                    },
                    "PacketField": "source-address",
                    "Vpc": {
                        "Id": "vpc-0abc123def456789",
                        "Arn": "arn:aws:ec2:us-west-2:123456789012:vpc/
vpc-0abc123def456789",
                        "Name": "Main VPC"
                    }
                }
            ],
            "Tags": [
                {
                    "Key": "Purpose",
                    "Value": "SecurityAudit"
                }
            ]
        }
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiJwYWdlLTIifQ=="
}
```


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-east-1:123456789012:network-
insights-analysis/nia-076744f74a04c3c7f",
            "NetworkInsightsPathId": "nip-0614b9507b4e3e989",
            "StartDate": "2023-03-20T23:47:08.080Z",
            "Status": "succeeded",
            "NetworkPathFound": true,
            "ForwardPathComponents": [
                {
                    "SequenceNumber": 1,
                    "Component": {
                        "Id": "igw-0797cccdc9d73b0e5",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:internet-gateway/
igw-0797cccdc9d73b0e5",
                    },
                    "OutboundHeader": {
                        "DestinationAddresses": ["10.0.2.87/32"]
                    },
                    "InboundHeader": {
                        "DestinationAddresses": ["34.230.71.227/32"],
                        "DestinationPortRanges": [{
                            "From": 22,
                            "To": 22
                        }],
                        "Protocol": "6",
                        "SourceAddresses": ["0.0.0.0/5", "11.0.0.0/8",
 "12.0.0.0/6", ...],
                        "SourcePortRanges": [{
                            "From": 0,
                            "To": 65535
                        }]
                    },
                    "Vpc": {
                        "Id": "vpc-f1663d98ad28331c7",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-
f1663d98ad28331c7"
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
```

```
                {
                    "SequenceNumber": 2,
                    "AclRule": {
                        "Cidr": "0.0.0.0/0",
                        "Egress": false,
                        "Protocol": "all",
                        "RuleAction": "allow",
                        "RuleNumber": 100
                    },
                    "Component": {
                        "Id": "acl-04fbcfb79260f6c5b",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:network-acl/
acl-04fbcfb79260f6c5b"
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "SequenceNumber": 3,
                    "Component": {
                        "Id": "sg-02f0d35a850ba727f",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:security-group/
sg-02f0d35a850ba727f"
                    },
                    "SecurityGroupRule": {
                        "Cidr": "0.0.0.0/0",
                        "Direction": "ingress",
                        "PortRange": {
                            "From": 22,
                            "To": 22
                        },
                        "Protocol": "tcp"
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "SequenceNumber": 4,
                    "AttachedTo": {
                        "Id": "i-0495d385ad28331c7",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:instance/
i-0495d385ad28331c7"
                    },
                    "Component": {
```

```
                        "Id": "eni-0a25edef15a6cc08c",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a25edef15a6cc08c"
                    },
                    "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"
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "SequenceNumber": 5,
                    "Component": {
                        "Id": "i-0626d4edd54f1286d",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:instance/
i-0626d4edd54f1286d"
                    },
                    "InboundHeader": {
                        "DestinationAddresses": ["10.0.4.120/32"],
                        "DestinationPortRanges": [{
                            "From": 22,
                            "To": 22
                        }],
                        "Protocol": "6",
                        "SourceAddresses": ["0.0.0.0/5", "11.0.0.0/8",
 "12.0.0.0/6", ...],
                        "SourcePortRanges": [{
                            "From": 0,
                            "To": 65535
                        }]
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                }
            ],
            "ReturnPathComponents": [
                {
```

```
                    "SequenceNumber": 1,
                    "Component": {
                        "Id": "i-0626d4edd54f1286d",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012: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": 22,
                            "To": 22
                        }]
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "SequenceNumber": 2,
                    "AttachedTo": {
                        "Id": "i-0495d385ad28331c7",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:instance/
i-0495d385ad28331c7"
                    },
                    "Component": {
                        "Id": "eni-0a25edef15a6cc08c",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a25edef15a6cc08c"
                    },
                    "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"
```

```
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "SequenceNumber": 3,
                    "Component": {
                        "Id": "sg-02f0d35a850ba727f",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:security-group/
sg-02f0d35a850ba727f"
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "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-east-1:123456789012:network-acl/
acl-0a8e20a0a9f144d36"
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "SequenceNumber": 5,
                    "Component": {
                        "Id": "rtb-0d49a54c0a8c0bd9b",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:route-table/
rtb-0d49a54c0a8c0bd9b"
                    },
                    "RouteTableRoute": {
                        "DestinationCidr": "0.0.0.0/0",
                        "GatewayId": "igw-0797cccdc9d73b0e5",
                        "Origin": "createroute",
                        "State": "active"
                    },
```

```
                    "AdditionalDetails": [],
                    "Explanations": []
                },
                {
                    "SequenceNumber": 6,
                    "Component": {
                        "Id": "igw-0797cccdc9d73b0e5",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:internet-gateway/
igw-0797cccdc9d73b0e5"
                    },
                    "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": ["34.230.71.227/32"],
                        "SourcePortRanges": [{
                            "From": 22,
                            "To": 22
                        }]
                    },
                    "Vpc": {
                        "Id": "vpc-f1663d98ad28331c7",
                        "Arn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-
f1663d98ad28331c7"
                    },
                    "AdditionalDetails": [],
                    "Explanations": []
                }
            ],
            "Tags": []
        }
    ]
}
```


Step 4: Delete the path

If you no longer need the path, you can delete it. Before you can delete the path, you must delete its analyses.

To delete the path

1. Use the following delete-network-insights-analysis command to delete the path analysis.

```
aws ec2 delete-network-insights-analysis --network-insights-analysis-
id nia-02207aa13eb480c7a
```

2. Use the following delete-network-insights-path to delete the path.

```
aws ec2 delete-network-insights-path --network-insights-path-
id nip-0b26f224f1d131fa8
```

If you keep the path, note that Reachability Analyzer will automatically delete the analysis 120 days after its creation date.

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

The following explanation codes indicate that 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.

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_NO_TARGETS_IN_AZ

The load balancer does not have targets in the specified Availability Zones.

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.

FIREWALL_RULES_RESTRICTION

The traffic is blocked by a matching Network Firewall firewall rule.

GATEWAY_REJECTS_SPOOFED_TRAFFIC

Gateways reject traffic with spoofed addresses from the VPC.

GWLB_DESTINATION_PORT_RESTRICTION

Traffic between a Gateway Load Balancer and its targets must use port 6081 as the destination port. To analyze connectivity through a Gateway Load Balancer, specify port 6081 in the path definition.

GWLB_PROTOCOL_RESTRICTION

Traffic between a Gateway Load Balancer and its targets must use the GENEVE protocol, which is UDP-based. To analyze connectivity through a Gateway Load Balancer, specify the UDP protocol in the path definition.

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_DESTINATION_ADDRESS_NOT_IN_RFC6598_EGRESS

Internet gateways reject outbound traffic with destination addresses in the shared IP address range (see RFC6598).

IGW_NAT_REFLECTION

The path has an internet gateway as an intermediate component, which Reachability Analyzer does not support. Instead, analyze the path from the source to the internet gateway and then analyze the path from the internet gateway to the destination.

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).

IGW_SOURCE_ADDRESS_NOT_IN_RFC6598_INGRESS

Internet gateways reject inbound traffic with source addresses in the shared IP address range (see RFC6598).

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. You can use filters to require that a path include a specific intermediate component.

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 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, or the network component sent traffic to a destination in another account or Region. If the destination is in another account, enable cross-account analyses.

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.

REGIONAL_NGW_ROUTE_AZ_RESTRICTION

The regional NAT gateway is not registered in the Availability Zone where the traffic originates.

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.

SG_REFERENCES_NOT_PRESERVED

The network component discards security group information about forwarded traffic. This prevents traffic from being accepted by security group rules that accept traffic only from a source or destination that belongs to a security group.

SG_REFERENCING_SUPPORT

The transit gateway VPC attachment does not have security group referencing support enabled. Therefore, we discard security group information about forwarded traffic.

SUBNET_ACL_RESTRICTION

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

TARGET_ADDRESS_RESTRICTION

A load balancer can only route traffic that is destined for the address of one of its targets.

TARGET_PORT_RESTRICTION

A load balancer can only route traffic to a target using its registered 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 connection is in a non-functional state.

TGW_ROUTE_AZ_RESTRICTION

This transit gateway is not registered in the Availability Zone where the traffic originates. The VPC attachment must have a subnet association in the Availability Zone.

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 packet 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.

UNKNOWN_RESOURCE

Reachability Analyzer can't analyze this resource because it can't describe the resource.

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_BLOCK_PUBLIC_ACCESS_ENABLED

Internet traffic is blocked because VPC Block Public Access (BPA) is enabled.

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.

VPCE_INTRA_VPC_TRAFFIC

A VPC endpoint can't initiate connections to resources in the same VPC where it is deployed. Instead, analyze the path in the reverse direction.

VPCE_SERVICE_NOT_INSTALLED_IN_AZ

The VPC endpoint service is not installed in the specified Availability Zone.

Configuration

The following explanation codes indicate that the path analysis determined that no path is possible.

DISCONNECTED_VPCS

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

NO_PATH

Reachability Analyzer was unable to find a path from the source to the destination. The following are the most common causes:

- The path does not meet the optional configuration details, such as an IP address, port, or filter.
- The source or destination components are temporarily isolated from the network (for example, a newly started instance that does not yet have a network interface).

- The source can't initiate traffic to the destination (for example, an interface VPC endpoint or gateway VPC endpoint can't initiate connections with components in the same VPC as the VPC endpoint).
- The path requires the ability to analyze an unsupported feature (for example, IPv6) or an unsupported network component.

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.

Search filter codes

The following explanation codes indicate that the path analysis couldn't find a path from the source to the destination that matched the specified filters. However, there might be a path that matches some of the specified filters. Verify that the filters are as intended. Otherwise, remove the filters that didn't match.

COMPONENT_FILTER_RESTRICTION

There is no path that traverses the specified component.

COMPONENT_FILTER_RESTRICTION_REMOVED_COMPONENT

There is no path that traverses the specified component because of an intermediate component filter.

FILTER_AT_DESTINATION_DESTINATION_ADDRESS

There is no path that matches the specified destination IP address at the destination.

FILTER_AT_DESTINATION_DESTINATION_PORT_RANGE

There is no path that matches the specified destination port range at the destination.

FILTER_AT_DESTINATION_PROTOCOL

There is no path that matches the specified destination protocol.

FILTER_AT_DESTINATION_SOURCE_ADDRESS

There is no path that matches the specified source address at the destination.

FILTER_AT_DESTINATION_SOURCE_PORT_RANGE

There is no path that matches the specified source port range at the destination.

FILTER_AT_SOURCE_DESTINATION_ADDRESS

There is no path that matches the specified destination IP address at the source.

FILTER_AT_SOURCE_DESTINATION_PORT_RANGE

There is no path that matches the specified destination port range at the source.

FILTER_AT_SOURCE_PROTOCOL

There is no path that matches the specified protocol.

FILTER_AT_SOURCE_SOURCE_ADDRESS

There is no path that matches the specified source IP address at the source.

FILTER_AT_SOURCE_SOURCE_PORT_RANGE

There is no path that matches the specified source port range at the source.

IGW_EXPECTS_PUBLIC_ADDRESS

IP addresses must be public IP addresses when the resource is an internet gateway.

Reachability Analyzer additional detail codes

Reachability Analyzer uses additional detail codes to provide information about the result of a path analysis.

The following additional detail codes are supported.

ASSUMPTION_PRESERVE_CLIENT_IP_IS_DISABLED

The analysis could not describe target group attributes for the target group, so the network path is based on the assumption that client IP preservation is disabled on the target group. You should verify this assumption.

ASSUMPTION_PRESERVE_CLIENT_IP_IS_ENABLED

The analysis could not describe target group attributes for the target group, so the network path is based on the assumption that client IP preservation is enabled on the target group. You should verify this assumption.

AVAILABILITY_ZONE_CROSSED

The network path crosses Availability Zones.

FIREWALL_UNSUPPORTED_HIGHER_PRIORITY_RULE_GROUP_TYPE

There is at least one higher priority rule that could match the traffic in this path, but we ignored because it contains an unsupported rule type. Verify that the result of the analysis matches the behavior of AWS Network Firewall in your network.

FIREWALL_UNSUPPORTED_HIGHER_PRIORITY_RULES

There is at least one higher priority rule that could match the traffic in this path, but we ignored because it contains an unsupported rule option. Verify that the result of the analysis matches the behavior of AWS Network Firewall in your network.

FIREWALL_UNSUPPORTED_RULE_OPTIONS

The matching firewall rule contains an unsupported rule option. Verify that the result of the analysis matches the behavior of AWS Network Firewall in your network.

MISSING_TARGET_GROUP_ATTRIBUTES

The target group attributes for the target were missing, so the analysis could not consider them.

PATH_THROUGH_GWLB_NOT_CHECKED

The analysis does not consider that traffic entering the VPC endpoint is forwarded to a Gateway Load Balancer for inspection before exiting the VPC endpoint.

RESPONSE_RTB_HAS_NO_ROUTE_TO_TRANSIT_GATEWAY

Traffic is routed from the transit gateway to the VPC endpoint. However, there is no route from the VPC endpoint to the transit gateway, so the network might drop the response traffic.

TRANSIT_GATEWAY_APPLIANCE_MODE_RECOMMENDED

The transit gateway VPC attachment has appliance mode disabled, but traffic is inspected through a Network Firewall. We recommend that you enable appliance mode for the VPC attachment.

UNIDIRECTIONAL_PATH_ANALYSIS_ONLY

The results include forward path analysis from the source to the destination. There might be a blocking configuration in the reverse path, which could not be analyzed.

Cross-account analyses for Reachability Analyzer

Reachability Analyzer analyzes the path between a source and destination. To analyze paths across multiple AWS accounts, enable trusted access for Reachability Analyzer with your organization from AWS Organizations. You can also register member accounts as delegated administrator accounts. A user in the management account can define paths and run analyses using sources and destinations from any account in the organization. A user in a delegated administrator account can define paths and run analyses using sources and destinations from any account in the organization other than the management account, plus any resources in the management account that were explicitly shared with the delegated administrator account.

For more information, see Visualize and diagnose network reachability across AWS accounts.

Pricing

There is no additional charge to run cross-account analyses.

Considerations

- Before accounts in the organization can use this feature in an opt-in Region, the management account must enable the opt-in Region. For more information, see Enable a Region in your organization in the *AWS Account Management Guide*.
- The accounts in the organization must be able to make calls to the AWS CloudFormation API in US East (N. Virginia) (`us-east-1`).
- AWS CloudTrail logs are always written to US East (N. Virginia) (`us-east-1`).

Tasks

- Enable trusted access in Reachability Analyzer
- IAM role deployments in Reachability Analyzer
- Manage delegated administrator accounts in Reachability Analyzer
- Disable trusted access in Reachability Analyzer
- Troubleshoot cross-account analyses in Reachability Analyzer

Enable trusted access in Reachability Analyzer

When you enable trusted access, Reachability Analyzer deploys the AWSServiceRoleForReachabilityAnalyzer service-linked role and the required cross-account access roles to all accounts in your organization.

To enable trusted access using the console

1. Sign in to the management account.
2. Open the Network Manager console at https://eusc-de-east-1.console.amazonaws-eusc.eu/networkmanager/home.
3. From the navigation pane, choose **Reachability Analyzer**, **Settings**.
4. For **Trusted Access**, choose **Turn on trusted access**.
5. Do not close or navigate away from this page until you see a success notification indicating that trusted access is turned on. This can take several minutes.

To enable trusted access using the AWS CLI

From the management account, use the enable-reachability-analyzer-organization-sharing command.

IAM role deployments in Reachability Analyzer

When you enable trusted access, the following roles are deployed in your organization:

- AWSServiceRoleForReachabilityAnalyzer – The service-linked role for Reachability Analyzer.
- IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess – The role for cross-account resource access for Reachability Analyzer.
- AWSServiceRoleForCloudFormationStackSetsOrgAdmin – The service-linked role for AWS CloudFormation StackSets for the management account.
- AWSServiceRoleForCloudFormationStackSetsOrgMember – The service-linked role for AWS CloudFormation StackSets for the member accounts.

The deployments can take several minutes to complete, depending on the number of member accounts in your organization. You can view the status of the role deployments as follows.

To view IAM role deployments

1. Sign in to the management account.
2. Open the Network Manager console at https://eusc-de-east-1.console.amazonaws-eusc.eu/networkmanager/home.
3. From the navigation pane, choose **Reachability Analyzer**, **Settings**.
4. Check **IAM role deployments status**.

Manage delegated administrator accounts in Reachability Analyzer

You can register up to 5 delegated administrator accounts in Reachability Analyzer. If you deregister a delegated administrator account, the users in the account can't run a new cross-account analysis, but they can still see the previously run analyses.

To manage delegated administrators

1. Sign in to the management account.
2. Open the Network Manager console at https://eusc-de-east-1.console.amazonaws-eusc.eu/networkmanager/home.
3. From the navigation pane, choose **Reachability Analyzer**, **Settings**.
4. To register a member account as a delegated administrator account, choose **Register delegated administrator**. Select the check box for the account, and then choose **Register delegated administrator**.
5. To deregister a delegated administrator account, select the check box for the account, and then choose **Deregister**.

Disable trusted access in Reachability Analyzer

After you disable trusted access, the users in the management account and delegated administrator accounts can't run a new cross-account analysis in Reachability Analyzer. However, they can still see the previously run analyses. Before you can disable trusted access, you must deregister the delegated administrator accounts.

You can enable trusted access again after disabling it. However, you must first re-register the delegated administrator accounts.

To disable trusted access using the console

1. Sign in to the management account.
2. Open the Network Manager console at https://eusc-de-east-1.console.amazonaws-eusc.eu/networkmanager/home.
3. From the navigation pane, choose **Reachability Analyzer**, **Settings**.
4. For **Trusted Access**, choose **Turn off trusted access**.
5. Do not close or navigate away from this page until you see a success notification indicating that trusted access is turned off. This can take several minutes.

To disable trusted access using the AWS CLI

From the management account, use the disable-aws-service-access command.

Troubleshoot cross-account analyses in Reachability Analyzer

The following information can help you troubleshoot common issues with running cross-account analyses in Reachability Analyzer.

Issues

- "StackSet is not empty" or "StackSet already exists"
- "Error fetching resources"
- "Organizational unit not found in StackSet"

"StackSet is not empty" or "StackSet already exists"

If you receive one of these errors while enabling trusted access, do the following to resolve the issue.

To resolve the issue

1. Choose **Turn off trusted access**.
2. Wait until you see a banner at the top of the screen indicating that the operation was successful.

3. Choose **Turn on trusted access**.

"Error fetching resources"

If you receive this error while attempting to access resources from another account in the organization, it usually indicates that your account doesn't have all permissions required.

- Verify that you have permission to call the `AssumeRole` and `SetSourceIdentity` API actions. For example, the following policy grants permission to call these actions.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole",
                "sts:SetSourceIdentity"
            ],
            "Resource": "*"
        }
    ]
}
```

- Verify that you have permission to call CloudFormation API actions. For example, the AWSCloudFormationFullAccess and AWSCloudFormationReadOnlyAccess policies grant permissions to call these actions.
- Verify that you have permission to call AWS Organizations API actions. For example, the AWSOrganizationsFullAccess and AWSOrganizationsReadOnlyAccess policies grant permissions to call these actions.

"Organizational unit not found in StackSet"

If you receive this error while disabling trusted access, do the following to resolve the issue.

To resolve the issue

1. Open the CloudFormation console at https://eusc-de-east-1.console.amazonaws-eusc.eu/cloudformation.
2. In the navigation pane, choose **StackSets**.
3. Select `ReachabilityAnalyzerCrossAccountResourceAccessStackSet` and then choose **Actions**, **Delete StackSet**.
4. Return to the Reachability Analyzer settings page and refresh the page.
5. Choose **Turn off trusted access**.

Identity and access management for 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.

Contents

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Reachability Analyzer.

Service user – If you use the Reachability Analyzer service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Reachability Analyzer features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator.

Service administrator – If you're in charge of Reachability Analyzer resources at your company, you probably have full access to Reachability Analyzer. It's your job to determine which Reachability Analyzer features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM.

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Reachability Analyzer.

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be authenticated as the AWS account root user, an IAM user, or by assuming an IAM role.

You can sign in as a federated identity using credentials from an identity source like AWS IAM Identity Center (IAM Identity Center), single sign-on authentication, or Google/Facebook credentials. For more information about signing in, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

For programmatic access, AWS provides an SDK and CLI to cryptographically sign requests. For more information, see AWS Signature Version 4 for API requests in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity called the AWS account *root user* that has complete access to all AWS services and resources. We strongly recommend that you don't use the root user for everyday tasks. For tasks that require root user credentials, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users to use federation with an identity provider to access AWS services using temporary credentials.

A *federated identity* is a user from your enterprise directory, web identity provider, or Directory Service that accesses AWS services using credentials from an identity source. Federated identities assume roles that provide temporary credentials.

For centralized access management, we recommend AWS IAM Identity Center. For more information, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity with specific permissions for a single person or application. We recommend using temporary credentials instead of IAM users with long-term credentials. For more

information, see Require human users to use federation with an identity provider to access AWS using temporary credentials in the *IAM User Guide*.

An *IAM group* specifies a collection of IAM users and makes permissions easier to manage for large sets of users. For more information, see Use cases for IAM users in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity with specific permissions that provides temporary credentials. You can assume a role by switching from a user to an IAM role (console) or by calling an AWS CLI or AWS API operation. For more information, see Methods to assume a role in the *IAM User Guide*.

IAM roles are useful for federated user access, temporary IAM user permissions, cross-account access, cross-service access, and applications running on Amazon EC2. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy defines permissions when associated with an identity or resource. AWS evaluates these policies when a principal makes a request. Most policies are stored in AWS as JSON documents. For more information about JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Using policies, administrators specify who has access to what by defining which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. An IAM administrator creates IAM policies and adds them to roles, which users can then assume. IAM policies define permissions regardless of the method used to perform the operation.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you attach to an identity (user, group, or role). These policies control what actions identities can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

Identity-based policies can be *inline policies* (embedded directly into a single identity) or *managed policies* (standalone policies attached to multiple identities). To learn how to choose between

managed and inline policies, see Choose between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples include IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. You must specify a principal in a resource-based policy.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional policy types that can set the maximum permissions granted by more common policy types:

- **Permissions boundaries** – Set the maximum permissions that an identity-based policy can grant to an IAM entity. For more information, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – Specify the maximum permissions for an organization or organizational unit in AWS Organizations. For more information, see Service control policies in the *AWS Organizations User Guide*.
- **Resource control policies (RCPs)** – Set the maximum available permissions for resources in your accounts. For more information, see Resource control policies (RCPs) in the *AWS Organizations User Guide*.
- **Session policies** – Advanced policies passed as a parameter when creating a temporary session for a role or federated user. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How Reachability Analyzer works with IAM

Before you use IAM to manage access to Reachability Analyzer, learn what IAM features are available to use with Reachability Analyzer.

IAM feature	Reachability Analyzer support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys (service-specific)	No
ACLs	No
ABAC (tags in policies)	Yes
Temporary credentials	Yes
Principal permissions	Yes
Service roles	No
Service-linked roles	Yes

To get a high-level view of how AWS FIS and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for Reachability Analyzer

Supports identity-based policies: Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Define custom IAM permissions with customer managed policies in the *IAM User Guide*.

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. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Resource-based policies within Reachability Analyzer

Supports resource-based policies: No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Reachability Analyzer

Supports policy actions: Yes

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. 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
```

To specify multiple actions in a single statement, separate them with commas.

```
"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`
- `EnableReachabilityAnalyzerOrganizationSharing`
- `StartNetworkInsightsAnalysis`

For more information, see Actions Defined by Amazon EC2 in the *Service Authorization Reference*.

Policy resources for Reachability Analyzer

Supports policy resources: Yes

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. As a best practice, specify a resource using its Amazon Resource Name (ARN). For actions that don't support resource-level permissions, 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`

Policy condition keys for Reachability Analyzer

Supports service-specific policy condition keys: No

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 `Condition` element specifies when statements execute based on defined criteria. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

ACLs in Reachability Analyzer

Supports ACLs: No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Reachability Analyzer

Supports ABAC (tags in policies): Yes

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes called tags. You can attach tags to IAM entities and AWS resources, then design ABAC policies to allow operations when the principal's tag matches the tag on the resource.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see Define permissions with ABAC authorization in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

Using temporary credentials with Reachability Analyzer

Supports temporary credentials: Yes

Temporary credentials provide short-term access to AWS resources and are automatically created when you use federation or switch roles. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM and AWS services that work with IAM in the *IAM User Guide*.

Cross-service principal permissions for Reachability Analyzer

Supports forward access sessions (FAS): Yes

Forward access sessions (FAS) use the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. For policy details when making FAS requests, see Forward access sessions.

Service roles for Reachability Analyzer

Supports service roles: No

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Create a role to delegate permissions to an AWS service in the *IAM User Guide*.

Service-linked roles for Reachability Analyzer

Supports service-linked roles: Yes

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing Reachability Analyzer service-linked roles, see Use service-linked roles for Reachability Analyzer.

Required API permissions for Reachability Analyzer

Reachability Analyzer relies on data from other AWS services. It uses permissions from the following services:

- Amazon EC2
- ELB
- AWS Network Firewall
- AWS Tiros

To view the permissions for this policy, see AmazonVPCReachabilityAnalyzerFullAccessPolicy in the *AWS Managed Policy Reference*.

Additional information

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 users permission to call the Reachability Analyzer API actions they need.

- `ec2:CreateNetworkInsightsPath`
- `ec2:DeleteNetworkInsightsAnalysis`
- `ec2:DeleteNetworkInsightsPath`
- `ec2:DescribeNetworkInsightsAnalyses`
- `ec2:DescribeNetworkInsightsPaths`
- `ec2:EnableReachabilityAnalyzerOrganizationSharing`
- `ec2:StartNetworkInsightsAnalysis`

Describe API calls for networking-related resources

Reachability Analyzer uses describe API calls while gathering information about your resources from Amazon VPC, Amazon EC2, and ELB (for example, subnets, network interfaces, and security groups). To access Reachability Analyzer, users must also have these API permissions.

Cross-account analysis

The following permissions are required to establish a trust relationship between Reachability Analyzer and AWS Organizations.

- cloudformation:ActivateOrganizationsAccess
- iam:CreateServiceLinkedRole
- iam:GetRole
- organizations:EnableAWSServiceAccess
- organizations:DescribeOrganization
- organizations:DisableAWSServiceAccess
- organizations:ListRoots

After you establish a trust relationship, a user in the management account or a delegated administrator account can run cross-account analyses using resources from the member accounts. The user must have the following permissions to do so.

- organizations:DescribeOrganization
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListDelegatedServicesForAccount
- organizations:ListDelegatedAdministrators
- organizations:ListAccounts

Tagging-related API calls

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

- ec2:CreateTags
- ec2:DeleteTags

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, users must also have the same API permissions.

Use service-linked roles for Reachability Analyzer

Reachability Analyzer uses AWS Identity and Access Management (IAM) service-linked roles for multi-account analysis. A service-linked role is a unique type of IAM role that is linked directly to Reachability Analyzer. Service-linked roles are predefined by Reachability Analyzer and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Reachability Analyzer easier because you don't have to add the necessary permissions yourself. Reachability Analyzer defines the permissions of its service-linked roles, and unless defined otherwise, only Reachability Analyzer can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

Service-linked role permissions for Reachability Analyzer

Reachability Analyzer uses the service-linked role named **AWSServiceRoleForReachabilityAnalyzer** to access AWS resources and integrate with AWS Organizations on your behalf.

The **AWSServiceRoleForReachabilityAnalyzer** role trusts the following services to assume the role:

- `reachabilityanalyzer.networkinsights.amazonaws.com`

The **AWSServiceRoleForReachabilityAnalyzer** service-linked role uses the managed policy AWSReachabilityAnalyzerServiceRolePolicy.

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-linked role permissions in the *IAM User Guide*.

Create a service-linked role for Reachability Analyzer

You don't need to create this service-linked role yourself. When you enable integration with AWS Organizations, Reachability Analyzer creates the **AWSServiceRoleForReachabilityAnalyzer** role for you. For more information, see the section called “Enable trusted access”.

If you delete this service-linked role and then enable integration with AWS Organizations, Reachability Analyzer creates the **AWSServiceRoleForReachabilityAnalyzer** role for you again.

Edit a service-linked role for Reachability Analyzer

Reachability Analyzer does not allow you to edit the **AWSServiceRoleForReachabilityAnalyzer** role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role description in the *IAM User Guide*.

Delete a service-linked role for Reachability Analyzer

If you are finished performing multi-account analysis, we recommend that you delete the **AWSServiceRoleForReachabilityAnalyzer** role. You can delete this service-linked role only after you disable the integration of Reachability Analyzer with AWS Organizations.

If the Reachability Analyzer service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To disable integration with AWS Organizations

Make sure that you are not running a path analysis. To disable integration using the Reachability Analyzer console, see the section called “Disable trusted access”. To disable integration using the AWS CLI or an API, see How to enable or disabled trusted access in the *AWS Organizations User Guide*.

To delete the service-linked role using IAM

Use IAM to delete the **AWSServiceRoleForReachabilityAnalyzer** role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

AWS managed policies for Reachability Analyzer

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed

policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

AWS managed policy: AmazonVPCReachabilityAnalyzerFullAccessPolicy

Provides permissions to create, analyze, and delete paths, and to describe path resources, such as EC2 instances, firewalls, internet gateways, load balancers, NAT gateways, network interfaces, transit gateways, VPC endpoint services, VPC endpoints, VPC peering connections, and virtual private gateways.

To view the permissions for this policy, see AmazonVPCReachabilityAnalyzerFullAccessPolicy in the *AWS Managed Policy Reference*.

Reachability Analyzer does not support resources from Direct Connect (service prefix: `directconnect`) or AWS Global Accelerator (service prefix: `globalaccelerator`). If you use this policy as a model for your own policies, you can omit these actions.

AWS managed policy: AmazonVPCReachabilityAnalyzerPathComponentReadPolicy

This policy is attached to the role the section called "IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess". This role is deployed to the member accounts in an organization when the management account enables trusted access for Reachability Analyzer using the console. It provides permissions to view resources from across your organization using the Reachability Analyzer console. For more information, see Cross-account access roles.

To view the permissions for this policy, see AmazonVPCReachabilityAnalyzerPathComponentReadPolicy in the *AWS Managed Policy Reference*.

AWS managed policy: AWSReachabilityAnalyzerServiceRolePolicy

This policy is attached to a service-linked role that allows Reachability Analyzer to perform actions on your behalf. For more information, see Use service-linked roles.

To view the permissions for this policy, see AWSReachabilityAnalyzerServiceRolePolicy in the *AWS Managed Policy Reference*.

Reachability Analyzer updates to AWS managed policies

View details about updates to AWS managed policies for Reachability Analyzer since this service began tracking these changes.

Change	Description	Date
AWSReachabilityAnalyzerServiceRolePolicy – Update to an existing policy	Removed actions related to AWS Global Accelerator (service prefix: `globalaccelerator`).	September 10, 2024
AmazonVPCReachabilityAnalyzerFullAccessPolicy – Update to an existing policy	Added the action `elasticloadbalancing:DescribeTargetGroupAttributes` , which grants permission to describe the attributes of a target group.	May 15, 2024
AWSReachabilityAnalyzerServiceRolePolicy – Update to an existing policy	Added the action `elasticloadbalancing:DescribeTargetGroupAttributes` , which grants permission to describe the attributes of a target group.	May 15, 2024
AmazonVPCReachabilityAnalyzerFullAccessPolicy – Update to an existing policy	Removed resource ID prefixes from the resource ARNs used to allow tagging Reachability Analyzer resources on create.	November 3, 2023
AmazonVPCReachabilityAnalyzerFullAccessPolicy – New policy	Added a policy that provides full access to Reachability Analyzer for single account use.	June 14, 2023

Change	Description	Date
AmazonVPCReachabilityAnalyzerPathComponentReadPolicy – New policy	Added a policy that grants member accounts permission to view resources from across your organization. The policy is attached to a role that is deployed to member accounts when the management account enables trusted access for Reachability Analyzer using the console.	May 1, 2023
AWSReachabilityAnalyzerServiceRolePolicy – New policy	Added a policy that is attached to a service-linked role that allows it to access AWS resources and integrate with AWS Organizations on your behalf.	November, 23, 2022
Reachability Analyzer started tracking changes	Reachability Analyzer started tracking changes for its AWS managed policies.	March 1, 2021

Cross-account access roles for Reachability Analyzer

When you enable trusted access for Reachability Analyzer, we use CloudFormation StackSets to deploy the IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess IAM role to all member accounts in the organization. This role allows the management account and delegated administrator accounts to specify resources from member accounts in path analyses.

Reachability Analyzer creates the custom IAM role automatically when you turn on trusted access using the Network Manager console. We strongly recommend that you use the console to turn on trusted access, as alternate approaches require an advanced level of expertise and are more prone to error.

Deregistering a delegated administrator removes it from the account list so that it can no longer assume this custom IAM role. If you turn off trusted access, we delete the StackSets.

IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess

This IAM policy role enables cross-account read-only access to resources through role switching. For more information, see AmazonEC2ReadOnlyAccess and AWSDirectConnectReadOnlyAccess in the IAM console.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Enables Console Access role
Resources:
  ConsoleRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: IAMRoleForReachabilityAnalyzerCrossAccountResourceAccess
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
        - Effect: Allow
          Principal:
            AWS:
            - arn:aws:iam::management-account-id:root
            - arn:aws:iam::delegated-admin-1-account-id:root
            - arn:aws:iam::delegated-admin-2-account-id:root
          Action:
          - sts:AssumeRole
      Path: "/"
      ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AWSDirectConnectReadOnlyAccess
      - arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess
      - arn:aws:iam::aws:policy/AmazonVPCReachabilityAnalyzerPathComponentReadPolicy
```

Manage IAM role deployments

If you make changes to your role policies, or if you've updated a self-managed role, you can deploy the updated policy to the accounts in your organization.

With a self-managed deployment, you are responsible for attaching the required policies and managing the trust relationship required for the delegated administrator and management accounts to use cross-account analyses.

Troubleshoot self-managed role deployments

If the StackSets deployment to an account fails and the message is "IAM role exists", delete the IAM role from the member account and then retry the role deployment in the management account.

To retry the IAM role deployments

1. Sign in to the management account.
2. Open the Network Manager console at https://eusc-de-east-1.console.amazonaws-eusc.eu/networkmanager/home.
3. From the navigation pane, choose **Reachability Analyzer**, **Settings**.
4. Under **IAM role deployments status**, choose **Retry role deployment**. The deployments can take several minutes to complete, depending on the number of member accounts in your organization.

For a message other than "IAM role exists", open a case with AWS Support. For more information, see Creating a support case in the *Support User Guide*.

Logging Reachability Analyzer API calls using AWS CloudTrail

Reachability Analyzer is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, a role, or an AWS service in Reachability Analyzer. CloudTrail captures all API calls for Reachability Analyzer as events. The calls captured include calls from the Reachability Analyzer console and code calls to the Reachability Analyzer API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Reachability Analyzer. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Reachability Analyzer, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the *AWS CloudTrail User Guide*.

Reachability Analyzer information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Reachability Analyzer, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail Event history.

For an ongoing record of events in your AWS account, including events for Reachability Analyzer, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple regions and Receiving CloudTrail log files from multiple accounts

Supported API calls

For Reachability Analyzer, you can use CloudTrail to log two types of events:

- **Reachability Analyzer API calls** — All API calls used to create, read/describe, update, delete, and list (CRUDL) Reachability Analyzer resources are logged by CloudTrail and are documented in the Amazon EC2 API Reference. In this scenario, `ec2.amazonaws.com` is the event source.
- **AWS Network Manager Chat API calls** — CloudTrail also records all Network Manager Chat API calls as events. The Network Manager Chat API provides an interface and methods with which users can interact and have conversations with Reachability Analyzer through Amazon Q. Calls to the following API methods generate entries in the CloudTrail log files:
  - `CreateConversation`
  - `ListConversations`
  - `DeleteConversation`
  - `NotifyConversationIsActive`
  - `SendConversationMessage`
  - `ListConversationMessages`
  - `CancelMessageResponse`

  In this scenario, `networkmanager-chat.amazonaws.com` is the event source.

Identity information

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding Reachability Analyzer log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, the request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `DeleteNetworkInsightsPath` action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAZR5EMTJKE753U4ZDS:test-user",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/test-user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAZR5EMTJKE753U4ZDS",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-23T19:01:21Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-23T19:04:18Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "DeleteNetworkInsightsPath",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "1.1.1.1",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
 Firefox/115.0",
    "requestParameters": {
```

```
        "DeleteNetworkInsightsPathRequest": {
            "NetworkInsightsPathId": "nip-068b3d73d1EXAMPLE"
        }
    },
    "responseElements": {
        "DeleteNetworkInsightsPathResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
            "requestId": "ca28860f-504a-4f2d-9f3f-f9cfb4ba0491",
            "networkInsightsPathId": "nip-068b3d73d1EXAMPLE"
        }
    },
    "requestID": "122b3164-b75c-4158-892b-ddfdfecff2d3",
    "eventID": "216247c4-8644-4f63-8b26-171d9d412a22",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ec2.us-west-2.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```


The following example shows a CloudTrail log entry that demonstrates the `SendConversationMessage` action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAZR5EMTJKE753U4ZDS:test-user",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/test-user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAZR5EMTJKE753U4ZDS",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
```

```
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-19T19:55:45Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-19T19:57:29Z",
    "eventSource": "networkmanager-chat.amazonaws.com",
    "eventName": "SendConversationMessage",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.1.1.1",
    "userAgent": "python-requests/2.31.0",
    "requestParameters": {
        "conversationId": "52c59d5f-932b-94c9-90bb-385454d3c3f9",
        "clientToken": "1234abcabefaaa",
        "message": "***"
    },
    "responseElements": {
        "conversationMessage": {
            "MessageContent": "***",
            "MessageContentType": "TEXT",
            "MessageId": "c6c5a4c1-d817-a153-4ac8-b9d96b22748d",
            "MessageState": "AVAILABLE",
            "MessageType": "USER",
            "Timestamp": 1697745449007
        }
    },
    "requestID": "d78c47a4-1b51-4823-bd4d-9c88d00a5dc6",
    "eventID": "4cae0020-429f-4958-b823-11d4afeeec4c",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Quotas for 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 Reachability Analyzer.

Name	Default	Adjustable
Paths	1,000	Yes
Analyses	10,000	Yes
Concurrent analyses	100	Yes

Troubleshooting Reachability Analyzer

The following error messages are returned by Reachability Analyzer:

The request failed due to insufficient permissions

Verify that you have the required permissions. For more information, see the section called "Required API permissions".

The network configuration is not supported

Verify that you are using resources that are supported by Reachability Analyzer. For more information, see the section called "Intermediate components".

The request failed due to modifications in network resources during the analysis

You can't update your network while the analysis is running.

The request failed due to missing component [*component*]

Verify that the resource ARNs are correct. For more information, see the Service Authorization Reference.

The request failed due to inaccessible resource [*resource*]

Verify that you have permission to access the specified resource.

The request failed due to throttling errors from [*service*]

Check for other applications or services that are currently consuming read capacity for the specified service.

Document history for Reachability Analyzer

The following table describes the releases for Reachability Analyzer.

Change	Description	Date
Removed Amazon Q network troubleshooting	Reachability Analyzer no longer supports Amazon Q troubleshooting.	June 10, 2025
Filter a resource from analysis	Added a new option to Reachability Analyzer that allows you to filter an AWS resource from analysis.	May 8, 2025
AWS managed policy updates	Reachability Analyzer updated one existing policy.	September 10, 2024
AWS managed policy updates	Reachability Analyzer updated two existing policies.	May 15, 2024
Amazon Q network reachability analysis	Public preview release of Amazon Q networking reachability analysis, a generative AI feature of Amazon Q that works with Reachability Analyzer.	November 28, 2023
AWS managed policy updates	Reachability Analyzer updated one existing policy.	November 3, 2023
AWS managed policy updates	Reachability Analyzer updated one existing policy.	June 30, 2023
AWS managed policy updates	Reachability Analyzer added one new policy.	June 14, 2023

AWS managed policy updates	Reachability Analyzer added one new policy.	May 1, 2023
New feature	You can specify VPC endpoints as sources and destinations, and Network Firewall firewalls as intermediate path components.	March 21, 2023
Multi-account support	Reachability Analyzer supports reachability analysis between AWS resources in different AWS accounts within an organization from AWS Organizations.	November 27, 2022
New feature	You can specify transit gateways as sources, destinations, and intermediate path components.	March 25, 2022
Initial release	This release introduces Reachability Analyzer.	December 10, 2020