



Multicloud Fabric Deployment

Table of Contents

Multicloud Fabric Deployment	1
About cloud discovery	2
What Multicloud Fabric discovers	2
How discovery works	3
When discovery runs	3
Configure and verify discovery	4
About attachments	5
How attachment works	5
Onboarding requirements and limitations	5
Onboard a VPC or VNet	7
Remove a VPC or VNet	9
Onboard an MX hub or spoke network	10
Remove an MX hub or spoke network	12
What Multicloud Fabric creates in your cloud	13
AWS	13
Azure	13
Google Cloud	14
Routing and policy	15
About Zero Trust Routing	15
What happens after you create a connection	15
Create a connection	16
Edit a connection	19
Remove a connection	19

Multicloud Fabric Deployment

About cloud discovery

A cloud account integration gives Multicloud Fabric permission to read an approved provider scope, but Multicloud Fabric still needs a current, provider-authoritative map of the networks inside that scope. Discovery provides an inventory that Multicloud Fabric can use to:

- Show the correct VPCs and VNets.
- Preserve immutable provider relationships.
- Evaluate region and CIDR context.
- Supply accurate inputs to onboarding and later connection workflows.

Its intent is to identify what could be connected, and to keep that view current as your cloud topology changes.



Discovery reads and catalogs cloud network control-plane metadata in the scope that you authorize. It does not create gateways, tunnels, or BGP sessions. It does not onboard a VPC/VNet. Nor does it advertise routes. These actions require separate onboarding and a connection/ZTR intent.

What Multicloud Fabric discovers

Refer to this table for a description of the provider data that Multicloud Fabric collects during the discovery process.

Inventory category	Provider data that Multicloud Fabric records	Purpose
Provider scope	• AWS account • Azure subscription and resource-group relationships • Google Cloud project or supported parent scope	Proves that Multicloud Fabric is reading the intended boundary.
Placement	Provider regions and, where applicable, availability zones	Determines where a network exists and whether it is eligible for a supported Multicloud Fabric region
Cloud networks	VPC/VNet name, immutable external ID, provider and account, default-network flag, CIDR blocks, and tags or labels	Creates the selectable network inventory shown in Multicloud Fabric
Subnets	Subnet name and ID, CIDR, parent VPC/VNet, region or zone, and related metadata	Shows the address and placement detail used by onboarding and by later topology reconciliation
Routing metadata	Route tables and provider-specific network relationships or attributes, where supported	Provides context for eligibility, onboarding, and post-change comparison

Inventory category	Provider data that Multicloud Fabric records	Purpose
Freshness and lifecycle	Discovery status, last-run and completion time, normalized error, and resource-change hashes	Lets Multicloud Fabric distinguish current, delayed, failed, or stale inventory

How discovery works

Here is a high-level summary of the discovery process:

1. Multicloud Fabric begins by querying the provider control plane. Using the identity configured for the integration, Multicloud Fabric calls the approved AWS, Azure, or Google Cloud inventory APIs for accounts and projects, placement, networks, subnets, routing metadata, and identifiers.
2. Multicloud Fabric then normalizes and compares the results. Provider-specific results are converted into a common Multicloud Fabric inventory, related to your organization and integration, compared with the prior resource hashes, and stored with status and freshness timestamps.
3. Finally, Multicloud Fabric presents the result. The expected resources appear in Multicloud Fabric's **Overview** as well as in the supported onboarding workflows.

When discovery runs

There are four situations when Multicloud Fabric performs a discovery:

- **Initial discovery:** Runs automatically after a new integration validates. Multicloud Fabric scans the authorized scope and builds the first normalized inventory, so the integration status advances and discovered resources become visible.
- **Manual refresh:** Triggered when you select **Refresh** for a cloud integration in **Cloud Access**. Multicloud Fabric updates the integration's last-run status and resource inventory.
- **Auto-discovery:** When enabled, This is triggered when Multicloud Fabric observes a supported provider change in AWS CloudTrail, Azure Activity Log, or Google Cloud Admin Activity. Multicloud Fabric identifies the affected resource and triggers a targeted rediscovery instead of waiting for another full scan. This way, a new or changed supported resource is folded into Multicloud Fabric's inventory without manual re-entry.
- **Periodic reconciliation:** This scheduled full discovery acts as a safety net. Multicloud Fabric rescans the authorized scope to recover changes missed by provider signals, advancing inventory freshness and converging missed resources.

Configure and verify discovery

1. After discovery completes, return to Multicloud Fabric's **Overview** and compare the expected provider inventory with the items displayed in your provider's console.

Discovery is complete when Multicloud Fabric reflects the current provider scope, regions, VPCs/VNets, immutable IDs, CIDRs, subnets, and related metadata under the correct integration. Once this data is current, eligible resources become available for selection and onboarding.

2. Verify your inventory in your provider's console.



For integration, discovery, and onboarding permissions, open the appropriate workflow and use the embedded provider-specific requirements it indicates. **Cloud Access** remains the release-specific authority for required rights.

AWS

- a. In the VPC console, confirm that the expected VPC, CIDRs, subnets, route tables, and region exist in the account connected with Multicloud Fabric.
- b. If **Cloud Access** identifies a missing permission, select **IAM > Roles** in AWS and compare the role with the checklist.

Azure

- a. With the target subscription selected, select **Virtual networks** to confirm the expected VNet, address space, subnets, region, and subscription.
- b. For permission or auto-discovery errors, select **Access control (IAM) > Check access** for the Multicloud Fabric service principal.

Google Cloud

- a. Select the target project.
- b. Select **VPC network > VPC networks** and **Subnets** to confirm the expected project, network, CIDRs, regions, and subnets.
- c. Check IAM and enabled APIs when **Cloud Access** reports a permission or API error.

About attachments

Cloud account integration gives Multicloud Fabric authorized provider access, and cloud discovery catalogs the networks that exist, but neither connects your cloud network to the Multicloud Fabric fabric. Onboard a specific VPC or VNet when you want that network to become an Multicloud Fabric connectivity endpoint. Onboarding creates the supported cloud-side attachment, establishes redundant encrypted paths and BGP control connectivity to an Multicloud Fabric region, and makes the network operationally visible in Multicloud Fabric. This is the transport foundation you need before you can create connections and use Zero Trust Routing (ZTR) to exchange selected routes.

How attachment works

Here is a summary of what takes place when an attachment is created between Multicloud Fabric and a VPC or VNet:

1. Multicloud Fabric begins by validating the eligibility of the selected network, confirming that it meets these [requirements](#).
2. It then determines which region to connect the MX hub with. An MX hub is connected to every participating Multicloud Fabric region in which the organization has an onboarded VPC or VNet. An MX spoke is connected to the selected Multicloud Fabric regions, subject to limitations listed [here](#).
3. Next, Multicloud Fabric prepares regional Multicloud Fabric hubs, ensuring that the required hub networks and fabric-side placement are available for the selected topology.
4. Multicloud Fabric establishes redundant AutoVPN and BGP, building the redundant AutoVPN paths between the selected MX and the applicable Multicloud Fabric hubs. It then establishes BGP control connectivity. Multicloud Fabric learns supported BGP routes from the MX. Static MX routes are not imported.
5. And finally, Multicloud Fabric records onboarding progress and makes the resulting site, placement, current health, historical health, and events available for verification.

Onboarding requirements and limitations

- Confirm that any MX site you want to onboard meets these requirements:
 - The site is online.
 - The site uses a supported MX model and firmware.
 - Site-to-site VPN is enabled for the hub or spoke, with the intended participating VLANs enabled.
 - Multicloud Fabric's public Beta supports SL0 connectivity mode only. Any MX model and firmware combination that can operate only in SL2 mode – including some second-generation MX models – is unsupported. These combinations can appear selectable but never come online.
 - Multicloud Fabric does not support spoke-only organizations. Do not attempt to work around the topology requirement by onboarding spokes without an eligible MX hub.
- A spoke can connect to a maximum of five regions.
- Multicloud Fabric supports the onboarding of these regions:

- AWS: **us-west-2**, **us-east-1**, and **eu-west-1**
- Azure: **westus2**, **eastus**, and **westeurope**
- Google Cloud: **us-west2**, **us-east1**, and **eu-west1**

Networks outside these regions are discoverable but disabled for onboarding.

- Also confirm that these cloud-specific requirements have been met:
 - The eligible AWS VPC, Azure VNet, or Google Cloud VPC must be visible under the intended provider scope.
 - When configuring an Azure VNet, it must contain a correctly named and sufficiently sized **GatewaySubnet**. Without it, Multicloud Fabric cannot place the Azure VNet Gateway that terminates the redundant VPN attachment. You create, size, and own this subnet; Multicloud Fabric does not tag or own it.

Onboard a VPC or VNet

1. From the left navigation, select **Overview**. Then select **Onboard network > VPCs**.

Onboard VPCs
Onboard cloud networks to the Multicloud Fabric.

Cloud integrations
Add cloud integrations to let Multicloud Fabric view and onboard cloud networks. You can also add, edit, or remove accounts in [Cloud Access](#).

Q Search Provider 3 results + Add cloud integration

Name	Provider	Accounts	VPCs	Credentials	Access rights	Status
59018	AWS	1	17 4 in MCF	IAM role	Onboarding resources	Connected
110762953	Google Cloud	1	3 2 in MCF	Access keys	Onboarding resources	Connected
8d87cf7b-94b4-	Azure	1	3 3 in MCF	Access keys	Onboarding resources	Connected

Cancel Next

2. Confirm that your cloud integration is listed. Then select **Next**.
3. Select the VPCs or VNets you want to onboard, then select **Next**.

Onboard VPCs
Onboard cloud networks to the Multicloud Fabric.

VPC selection
Select VPCs to deploy an endpoint into the VPCs that give your resources access to the Multicloud Fabric.

Q Search Provider Show default VPCs Filters Download

1 item selected Select all 5 items Cancel

	VPC name	VPC ID	Tags	Subnets	Provider	Cloud region	Account name
☒	—	vpc-		3	AWS	eu-west-1	MCN-PMLab
☐	—	vpc-		3	AWS	ap-southeast-2	MCN-PMLab
☐	—	vpc-		3	AWS	ap-south-1	MCN-PMLab

4. Review the onboarding settings that are displayed, then select **Next**.



For public Beta, you will not be able to change any of these settings.

Onboard VPCs

Onboard cloud networks to the Multicloud Fabric.

1 Cloud integrations
2 VPC selection
3 Onboarding settings
4 Summary
5 Onboarding VPCs
2 of 2 sub-steps

Onboarding settings

Review and update VPCs' route table propagation, onboarding technology, and NAT configurations. All settings can be updated later as well.

i During this demo period, onboarding settings can't be changed. Feel free to continue to the next screen.

☐ Overlapping subnets only

☒	Name	Tags	Subnets	Route table propagation	Onboarding technology	Cloud region	Actions
☒	—		3 unique subnets	Specific routes	Virtual Private Gateway (VGW)	eu-west-1	NAT

Rows per page 10
1-1 of 1
1

- Confirm that the VPCs or VNets you selected are displayed, then select **Execute VPC onboarding**.

Onboard VPCs

Onboard cloud networks to the Multicloud Fabric.

1 Cloud integrations
2 VPC selection
3 Onboarding settings
4 Summary
5 Onboarding VPCs
2 of 2 sub-steps

Summary

Review the VPCs and (if applicable) new regions to be onboarded into MCF.

Deploy MCF regions

1 new region will be deployed to onboard the selected VPCs.

AWS
eu-west-1

Onboard VPCs

1 VPC will be onboarded to Multicloud Fabric.

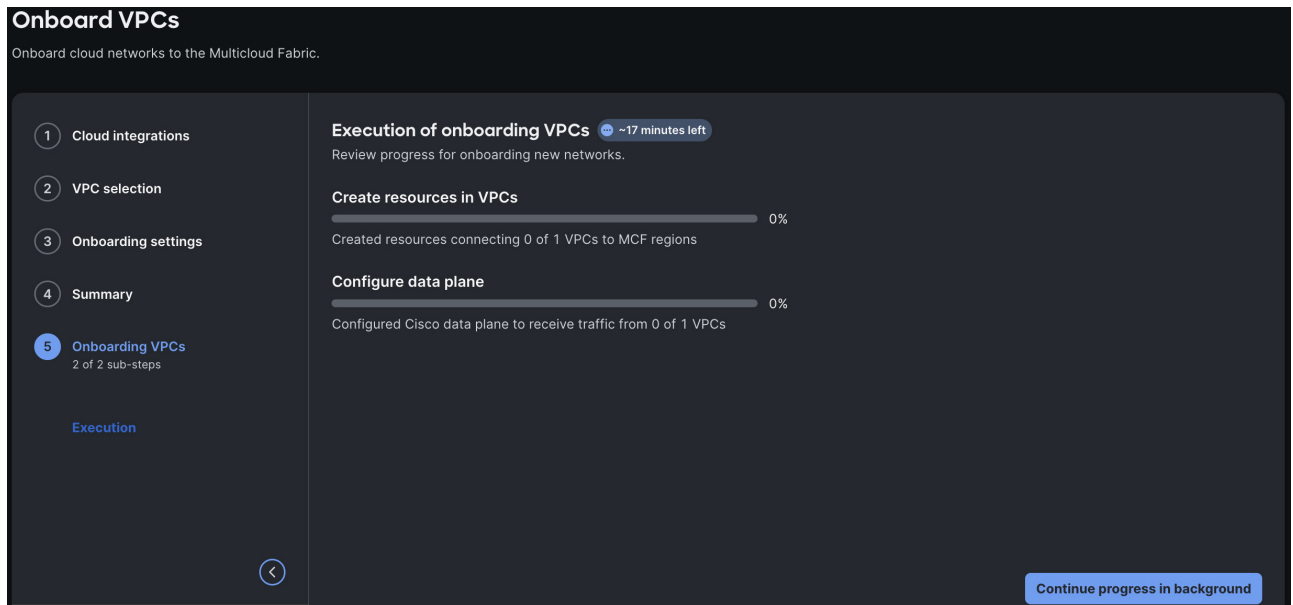
1 result

VPC name	Tags	Provider	Cloud region	Subnets	Route table propagation	Onboarding technology
—		AWS	eu-west-1	3	Specific routes	Virtual Private Gateway (VGW)

Rows per page 10
1-1 of 1
1

- Monitor the progress of the operation, capturing any errors that occur.

8



- o This operation typically takes around 10 minutes to complete for both AWS and Google Cloud, and around 45 minutes for Azure. If the operation takes much longer than this, do not retry it while the original operation is still active. Repeated retries can obscure the original operation.
- o Select **Continue progress in background** to close the wizard.

7. Verify that onboarding was successful:

- From the left navigation, select **Overview**. Then select **VPCs**.
- Select the link for the relevant VPC or VNet to open its details page.
- Confirm that its status is listed as **Onboarding** and has connectivity with Multicloud Fabric.

Remove a VPC or VNet

Follow these steps if you need to remove a VPC or VNet that was onboarded previously.

- From the left navigation, select **Overview**.
VPCs should already be selected, by default.
- For the VPC/VNet you want to remove, select **...** > **Remove**.
You can also select the VPC/VNet you want to remove to open its details page. Then select **Offboard VPC**.
- Select **Remove VPC**.

Onboard an MX hub or spoke network

Before you begin

The proposed region set is derived from your existing cloud attachments. If you have not already onboarded a VPC or VNet, do so before before you complete this procedure.

Follow these steps to onboard an MX hub or spoke network to Multicloud Fabric.



There are four use cases for MX hub/spoke network onboarding:

- Onboard hub networks
- Onboard spoke networks
- Onboard templated hub networks
- Onboard templated spoke network

Be aware that you cannot onboard an individual hub network. All hub networks are onboarded across all deployed regions to create a full mesh topology.

1. From the left navigation, select **Overview > Onboard network > Meraki networks**.
2. Select the Meraki spoke networks you want to onboard, then select **Next**.

Onboard Meraki Networks

1 Select networks

2 Assign regions
Spoke networks only

3 Summary

4 Onboarding Meraki networks

Select networks

Select MX networks to onboard. If you don't see a network below, make sure it has site-to-site VPN enabled.

Hubs are pre-selected, because they **must** be included to onboard any Meraki networks. If your organization adds hubs in the future, they'll automatically get onboarded as well. Templated Meraki spokes are filtered out. Already onboarded hubs and spokes are not listed here. To update an onboarded spoke, open its detail on the Overview and use Edit.

Q Search

6 results

	Name	Type	Location	Subnets	Tags	MX model	
☒	▼ All Meraki hubs 3	Meraki hub	--	--	--	--	
	MX68-Branch-	Meraki hub	--	2	--	--	NAT
	MX68-Branch-	Meraki hub	--	2	--	--	NAT
	MX-Branch-	Meraki hub	--	1	--	--	NAT
☒	MX-Branch-	Meraki spoke	--	1	--	--	NAT
☐	MX-Branch-	Meraki spoke	--	--	--	--	NAT
☒	MX-Branch-	Meraki spoke	--	1	--	--	NAT

Cancel

Next

Hubs are already selected because they must be included to onboard Meraki networks. If your organization add hubs later, they will also be automatically onboarded.

3. Select the regions to which you want to onboard the spoke networks you selected, then select **Set regions**.

10

Onboard Meraki Networks

1 Select networks

2 **Assign regions**
Spoke networks only

3 Summary

4 Onboarding Meraki networks

Assign regions

Choose where to onboard your **spoke** networks.
Hubs are always onboarded across all deployed regions to create a full mesh topology. When new regions are deployed, hubs automatically get added to those regions as well.

Set initial regions for spoke networks

After this initial selection, you can adjust per-network details.

AWS Region

Azure Region

GCP Region

Set regions

Q Search

5 results

☐	Name	AWS region	Azure region	GCP region
☒	> All Meraki hubs 3	eu-central-1 us-east-1 us-west-2	eastus westeurope westus2	us-west2
☐	MX-Branch-	--	--	--
☐	MX-Branch-	--	--	--

Cancel

Back

Next



Hub networks are automatically added to any new regions that are deployed.

4. Select **Next**.

5. Confirm that the selections you made are displayed, then select **Execute onboarding**.

Onboard Meraki Networks

1 Select networks

2 Assign regions
Spoke networks only

3 **Summary**

4 Onboarding Meraki networks

Summary

Review the regions for onboarding your networks.

Regions

Q Search

5 results

Name	AWS region	Azure region	GCP region
✓ All Meraki hubs 3	eu-central-1 us-east-1 us-west-2	eastus westeurope westus2	us-west2
MX68-Branch-AZ-H2T	eu-central-1 us-east-1 us-west-2	eastus westeurope westus2	us-west2
MX68-Branch-LA-H3	eu-central-1 us-east-1 us-west-2	eastus westeurope westus2	us-west2
MX-Branch-SFO-vH1	eu-central-1 us-east-1 us-west-2	eastus westeurope westus2	us-west2
MX-Branch-Uth-vS1H2T	us-west-2	westus2	us-west2
MX-Branch-NM-vS2H2T	us-west-2	westus2	us-west2

Cancel

Back

Execute onboarding

Multicloud Fabric validates, places, and connects the site as described in [How attachment works](#). Route exchange begins only when an applicable connection/ZTR intent exists. The wizard updates after the network is successfully onboarded.

Onboarding Meraki networks

Review progress for onboarding new networks.



Meraki networks successfully onboarded

Add applications hosted in new Meraki networks and connect resources to allow traffic between VPCs, sites, and applications.

You may also exit now and connect resources later.

[Add applications →](#)

[Connect resources →](#)

[Exit to Multicloud Fabric Overview](#)

6. Select **Connect resources** to connect VPCs, Vnets, and sites. Refer to [Create a connection](#).
If you want to do this later, select **Exit to Multicloud Fabric Overview** to return to Multicloud Fabric's **Overview**.

Remove an MX hub or spoke network

Follow these steps if you need to remove an MX hub or spoke network that was onboarded previously.

1. From the left navigation, select **Overview**.
2. Select **Sites**.
3. For the hub or spoke network you want to remove, select **...** > **Remove**.
4. Check the check box to confirm that you want to remove this network.
5. Select **Remove**.

What Multicloud Fabric creates in your cloud

The Multicloud Fabric fabric needs a provider-native, encrypted, and redundant attachment to the selected network. The objects below form the cloud half of that attachment, and they do not publish your routes until a separate connection or ZTR intent exists. Resource counts can vary with the active HA plan.



Use the exact provider resource ID plus the metadata in this section before you treat an object as Multicloud Fabric-owned. A deterministic name alone is not proof, so never infer ownership from a display name, and never delete by name alone. Shared, reused, pre-existing, and customer-created resources must not be removed as Multicloud Fabric residuals.

AWS

AWS requires a customer-side gateway anchor, a representation of the remote Multicloud Fabric regional peer, and Site-to-Site VPN objects that join them. Multicloud Fabric also enables route propagation on the applicable VPC route tables, so routes learned later through BGP can enter the VPC routing domain after a Connection or ZTR intent exists.

CSP resource or configuration	Why it is required	Multicloud Fabric ownership and correlation metadata
Customer gateways	Represent the Multicloud Fabric regional public IP and BGP peer in AWS.	Name=<MCF resource name>; created_by_mcn=true; onboarding_id=<onboarding UUID>
Virtual private gateway (VGW)	Attaches the VPN endpoint to the selected VPC and terminates the AWS side of the attachment.	Name=<MCF resource name>; created_by_mcn=true; onboarding_id=<onboarding UUID>
Site-to-site VPN connections and tunnels	Create the encrypted IPsec paths and BGP sessions between the Customer Gateway and the VGW.	Name=<MCF resource name>; created_by_mcn=true; onboarding_id=<onboarding UUID>
VGW route propagation	Allows route tables to learn BGP routes from the VGW.	This is a configuration change on a route table. It is not a separately tagged resource.

Azure

Azure places a route-based, BGP-enabled Virtual Network Gateway in your **GatewaySubnet**. Public IPs provide the Azure tunnel endpoints, Local Network Gateways describe the remote Multicloud Fabric peers, and connections bind both sides into the redundant IPsec attachment.

CSP resource or configuration	Why it is required	Multicloud Fabric ownership and correlation metadata
Local network gateways	Represent the remote Multicloud Fabric regional gateway addresses and BGP peers.	Name=<MCF resource name>; created_by_mcn=true; OnboardingID=<onboarding UUID>

CSP resource or configuration	Why it is required	Multicloud Fabric ownership and correlation metadata
Public IP addresses	Provide Azure-side public endpoints for the active-active VPN gateway.	Name=<MCF resource name>; created_by_mcn=true; OnboardingID=<onboarding UUID>
Virtual network gateway	Terminates route-based IPsec in the selected VNet and establishes BGP. Multicloud Fabric configures active-active behavior for redundancy.	Name=<MCF resource name>; created_by_mcn=true; OnboardingID=<onboarding UUID>
Virtual network gateway connections	Bind the VNet gateway to the Local Network Gateways and hold the IPsec connection relationship.	Name=<MCF resource name>; created_by_mcn=true; OnboardingID=<onboarding UUID>

Google Cloud

Google Cloud uses an HA VPN Gateway on the selected VPC, an External VPN Gateway representation of the Multicloud Fabric regional peers, and a Cloud Router for BGP. VPN tunnels, router interfaces, and BGP peers join those objects into redundant encrypted paths and dynamic route exchange.

CSP resource or configuration	Why it is required	Multicloud Fabric ownership and correlation metadata
External VPN gateway	Represents the Multicloud Fabric regional external peer interfaces in Google Cloud.	Label: created_by_mcn=true . It may be shared across relationships, so it intentionally has no onboarding_id label.
HA VPN gateway	Provides redundant Google Cloud-side tunnel endpoints attached to the selected VPC.	Labels: created_by_mcn=true and onboarding_id=<onboarding UUID>
Cloud router	Terminates BGP and dynamically exchanges routes for the VPN attachment.	Description: Multicloud Fabric Managed . The current implementation does not apply the per-onboarding labels used on the HA gateway and tunnels.
VPN tunnels	Create encrypted IKEv2 paths between the HA VPN Gateway and the Multicloud Fabric external peer interfaces.	Labels: created_by_mcn=true and onboarding_id=<onboarding UUID>
Router interfaces and BGP peers	Bind each tunnel to the Cloud Router and establish the corresponding BGP session.	This is a child configuration on the Cloud Router rather than separately tagged resources.

Routing and policy

About Zero Trust Routing

Onboarding a VPC, VNet, or MX site establishes its encrypted transport and BGP attachment to Multicloud Fabric. However, Multicloud Fabric intentionally does not publish routes simply because an endpoint has been onboarded. You create a connection when you want two specific onboarded networks – and the eligible address scopes represented by that intent – to exchange routes. ZTR realizes that explicit relationship, so Multicloud Fabric distributes only the routes that your intent authorizes instead of automatically creating broad connectivity between every attached network.

What happens after you create a connection

After you create a connection in **Overview**, Multicloud Fabric completes these actions:

1. Multicloud Fabric begins by validating the intent. It verifies that:
 - The selected source and destination are supported.
 - The endpoints are onboarded, and that the requested address scopes belong to those endpoints.
 - No visible overlap or eligibility error blocks realization of the connection.
Multicloud Fabric either accepts the connection or presents a rolled-up configuration/conflict error.
2. Multicloud Fabric then records your policy, storing the connection name, enabled state, endpoint relationship, and the selected network, VLAN, or prefix scope as your desired route-exchange policy.
3. Next, Multicloud Fabric computes ZTR route authorization. It maps your intent to the currently learned and eligible prefixes for both endpoints, and computes the route policy that permits those prefixes to be exchanged.
4. Multicloud Fabric then distributes authorized routes, applying the ZTR policy across the endpoints' existing AutoVPN or IPsec/BGP attachments that are healthy.
5. And finally, Multicloud Fabric reports and reconciles the result. It updates the connection's status and events. It then reconciles supported topology changes against the saved intent. A new resource may require discovery convergence before its prefixes can be realized.



A realized connection authorizes routes. It does not guarantee application traffic. At the end of a successful connection or ZTR operation, Multicloud Fabric has authorized and distributed the intended route set across endpoint attachments that are already healthy. ZTR is not a firewall, and it does not override any of these items:

- AWS security groups or NACLs
- Azure NSGs or firewalls
- Google Cloud firewall policy
- MX ACL/firewall behavior
- An intervening NVA

- NAT
- The destination service
- The return path

If the routes are present but traffic fails, troubleshoot those layers that you control before treating the symptom as an Multicloud Fabric route-realization issue.

Create a connection

1. Confirm that the required VPCs, VNets, and MX sites are integrated, discovered, or onboarded, and that they are healthy.
2. From the left navigation, select **Overview**. Then select **Connect resources**.

Connect Resources

Connect cloud resources and sites through the Multicloud Fabric. Please allow up to 5 minutes for new resources to be available to connect.

⚠ Applying changes may briefly disrupt existing traffic
Typically up to ~30 seconds while configuration converges. Existing traffic may be affected for any participating sites or VPCs, including for other Connections that use any of these participating resources. Plan changes during a maintenance window where possible.

Connection name
Name the connection

Description
Describe the connection

i Bi-directional connectivity
Connectivity is bi-directional. Once established, traffic will flow freely between selected clients and resources in both directions.

Clients
No clients selected yet
[+ Select clients](#)

Multicloud Fabric
☐ Enable connection
Advanced security profile ⓘ
 None
Observability features
 None

Resources
No resources selected yet
[+ Select resources](#)

[Review connection](#) [Show API](#) [Cancel](#)

3. Define the intent:
 - a. Name the connection.
 - b. (Optional) Enter a short description of the connection.
 - c. Select the clients and resources you want to pair.
 - When selecting sites, select **Edit** to specify which subnets to include site for a particular site.

Select Sites

Select one or more sites with all or some subnets.
If all subnets selected, future additions will be automatically included.

Select sites and subnets

All Multicloud fabric regions ▾
5 results

1 item selected Select all

☐	Name	Subnets	Multicloud fabric region
☐		1	—
☒		2 Edit	eu-central-1 us-east-1 us-west-2 eastus westeurope westus2 us-west2
☐		1	—
☐		2	eu-central-1 us-east-1 us-west-2 eastus westeurope westus2 us-west2
☐		0	us-east-1 us-west-2 westus2 us-west2

Rows per page 10 ▾
1-5 of 5
< 1 >

Cancel Apply

- When selecting VPCs:
 - You can instruct Multicloud Fabric to connect the VPCs configured with a particular tag. Choose an existing tag, or define a new one by specifying its account scope, key, and value.

Select VPCs

Connect VPCs dynamically by tag, select specific VPCs, or use both.

☒ [Connect dynamically based on tag](#)

Select or define a tag to automatically include matching VPCs. Newly discovered matching VPCs will also be connected.

☒ Select existing tag
 ☐ Define tag

Select accounts and tag

Account scope

AWS
 ⊗ ▾

Tag

Name: app-inventory-aws-use1
 ⊗ ▾

☐ [Connect specific VPCs](#)

Cancel Apply

- You can also select the specific VPCs to include.

Select VPCs

Connect VPCs dynamically by tag, select specific VPCs, or use both.

☐ Connect dynamically based on tag

☒ **Connect specific VPCs**

Select one or more VPCs. All subnets in each selected VPC will be connected.

Provider ▼

All tags ▼

9 results

☐	Name	Tags	Subnets	Multicloud fabric...	Account name
☐			1		
☐			1		
☐		func: analytics	1	us-west-2	

- Multicloud Fabric does not support site-to-site or site-to-VLAN connections. To add a site or VLAN as a resource, you must first remove all sites and VLANs currently selected as a client.
- Ensure that you set the **Enable connection** option.

4. Select **Review connection** to check that the selected endpoints and address scopes match the traffic to be permitted.

Summary

Connection name	Description
csp to csp	—

Source

Destination

VPCs
 Specific VPCs (2)

Connection enabled

VPCs
 Specific VPCs (2)

Advanced security

Visibility

None

None

[Back](#)
[Confirm and save connection](#)

5. Select **Confirm and save connection**.
Multicloud Fabric validate the intent and realizes the ZTR route policy.
6. Verify the connection:
 - a. Open the detail pages for the connection and endpoints. Compare the tunnel, BGP, route

visibility, and event history with the intended path.

- b. Test the configured protocol and port. Security policy and a valid return path are still required.
- c. Confirm route visibility on the MX or CSP side.

Edit a connection

Follow these steps to update the settings for a connection that has already been configured.

1. From the left navigation, select **Overview**.
2. Select **Connections**.
3. Select the connection's name.
You can also select .
4. Make the necessary setting changes in **Edit Connection**.
5. Select **Review connection**.
6. Confirm that the changes you made are reflected in **Summary**. Then select **Confirm and save connection**.

Remove a connection

Follow these steps to remove an active connection from Multicloud Fabric.

1. From the left navigation, select **Overview**.
2. Select **Connections**.
3. For the connection you want to remove, select .
4. Check the check box to confirm that you want to remove this connection.
5. Select **Remove**.