



Release Notes for Multicloud Fabric



Contents

- Multicloud Fabric 3
- Open issues..... 3
- Related resources 5
- Documentation feedback 5
- Legal information 5

Multicloud Fabric

Note: Multicloud Fabric is available as a Beta release. Refer to [Multicloud Fabric Onboarding](#) for instructions on how to activate your trial subscription.

Multicloud Fabric is Cisco's fully managed networking service for connecting site-to-cloud and cloud-to-cloud networks. It supports networks in AWS, Azure, and Google Cloud, as well as Meraki sites.

In Multicloud Fabric, you:

1. Authorize cloud access for the cloud providers you use.
2. Onboard the networks you want to include in the fabric.
3. Choose which resources should communicate.

Multicloud Fabric then provisions the routing, tunnels, and policies needed to realize those connections. It simplifies multicloud networking by enabling you to:

- Discover and manage network resources.
- Define specific connectivity between the resources you choose.
- Monitor connection health and events, including event history, to help you investigate connectivity issues.

Rather than automatically connecting every onboarded network, Multicloud Fabric's Zero Trust Routing (ZTR) capability distributes only the routes authorized by your connection choices.

Open issues

Table 1. Open issues for Multicloud Fabric

Description	Workaround
These issues were observed after applying the Last 15 minutes filter to the Event Log: • All events that occurred within this timeframe may not be displayed. • After selecting Load more, Multicloud Fabric may also retrieve logs from outside this timeframe.	None.
Unable to onboard a VPC to a Google Cloud project, even after removing an unsupported region subnet.	None.
When creating a ZTR connection between a site and a Google Cloud VPC with multiple subnet routes, only one of these routes is advertised.	To ensure that all subnet routes configured for Google Cloud VPC are advertised during the creation of a ZTR connection, set Global as the VPC's Dynamic routing mode in Google Cloud.
Onboarding a Google Cloud VPC may trigger a Google API 400 error if the MCF-generated suffix causes the VPC's name to exceed the 63-character limit.	None.
In Multicloud Fabric's overview page, the status bar may display incorrect values after you select a tab (such as Connections or VPCs).	None.

Description	Workaround
Unable to edit the regions for templated spokes that have been onboarded to Multicloud Fabric.	None.
When a template with 100 spokes (each advertising 1 route) is configured, and a VPC is onboarded in AWS along with the templated spokes and 1 hub, creating a ZTR connection between that VPC and all sites causes BGP on AWS to go down.	None.
When you create a Meraki template that uses a 10.0.0.0/8 subnet for addressing and VLANs, each spoke bound to that template receives a unique subnet carved from that range. After you onboard VPCs in AWS and Google Cloud and bind the template to both clouds, the spoke routing tables show traffic between spokes routed through a Multicloud Fabric hub. This occurs because Multicloud Fabric installs static routes, and these static routes take precedence over BGP-learned routes.	None.
In Overview > VPCs , the MCF region and AZ column displays cloud service provider VPC regions instead of MCF regions.	None.
Multicloud Fabric does not provide a warning before removing a site that is associated with a ZTR connection. This operation should also be captured in the Event Log but isn't.	None.
When the details page is open for an Azure VPC or site, Multicloud Fabric displays Unknown as its connectivity and BGP status. In Azure, its status is listed as Connected .	None.
In the Event Log, the Entity type and Entity filters may not work as expected.	None.
Onboarding limitations for Multicloud Fabric's Beta release: - You can onboard a maximum of 10 Auto VPN hubs (including multicloud regions). - When HA is enabled, you can only onboard sites to 4 regions (8 hubs with primary and secondary instances).	None.
The VPC onboarding operation can take up to 45 minutes to successfully complete.	None.
Azure VNets that are onboarded to Multicloud Fabric must not use or overlap the 10.254.0.0/16 address range. Multicloud Fabric's Beta release reserves this range for internal IPsec tunnel addressing and BGP peering. If an Azure VNet's address space overlaps this range, the VNet cannot be onboarded successfully. Choose a non-overlapping address range before onboarding.	None.

Related resources

You can access Multicloud Fabric documentation from the following website:

[Cisco Cloud Control User Content](#) (refer to the Applications section)

Table 2. Additional resources

Document	Description
Release Notes for Multicloud Fabric	The current document
Multicloud Fabric Onboarding	Introduces Multicloud Fabric and explains what it does. Describes how to activate your trial subscription and integrate your AWS, Azure, or Google Cloud accounts.
Multicloud Fabric Deployment	Explains how Multicloud Fabric discovers your cloud networks and how to onboard VPCs/VNets and MX sites. Describes how to connect onboarded resources so that only the routes you authorize are exchanged.
Multicloud Fabric Troubleshooting	Describes how to monitor the health of your onboarded networks and review activity in the Event Log. Provides guidance for resolving common Multicloud Fabric issues and contacting Support.

Documentation feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to ciscocloudcontrol-docfeedback@cisco.com.

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.