Geo Redundancy Overview

This chapter contains the following topics:

Disclaimer

The chapters in this part explains the requirements and processes to install or upgrade Geo Redundancy in the Crosswork Network Controller solution.

Attention Geo Redundancy is a limited feature in Crosswork Network Controller 6.0 release. For any assistance, please contact the Cisco Customer Experience team.

Introduction

The geo redundancy solution ensures business continuity in case of a region or data center failure for on-premise deployment. It adds another layer of protection in the high availability stack for Crosswork through geographical or site redundancy. Geo redundancy protects against entire site failure, reduces disruption during system upgrades, and reduces overall data loss.

Geo redundancy involves placing physical servers in geographically diverse availability zones (AZ) or data centers (DC) to safeguard against catastrophic events and natural disasters. Availability Zones are multiple, isolated locations in a region with independent sources for power, cooling, and networking.

Some of the key factors that ensure geo redundancy are:

- *VM Node availability:* At least 3 VM nodes are deployed in each cluster to ensure optimal availability of infrastructure and applications. This provides physical compute availability and is the industry standard number suggested for running services for high availability. Deploying 3 VM nodes address split-brain problems, supports RAFT-based services, and allows for support of various in-service maintenance by supporting single VM failure.
- *Geo availability of Nodes:* The VM nodes are recommended to be placed in different AZ/regions to avoid a central point of failure that could bring down all the VM nodes.

- *Network Availability:* The VM nodes are connected to the network that meet link availability and latency requirements of the users.