NetApp Business Continuity and Disaster Recovery Plan Overview

January 2024

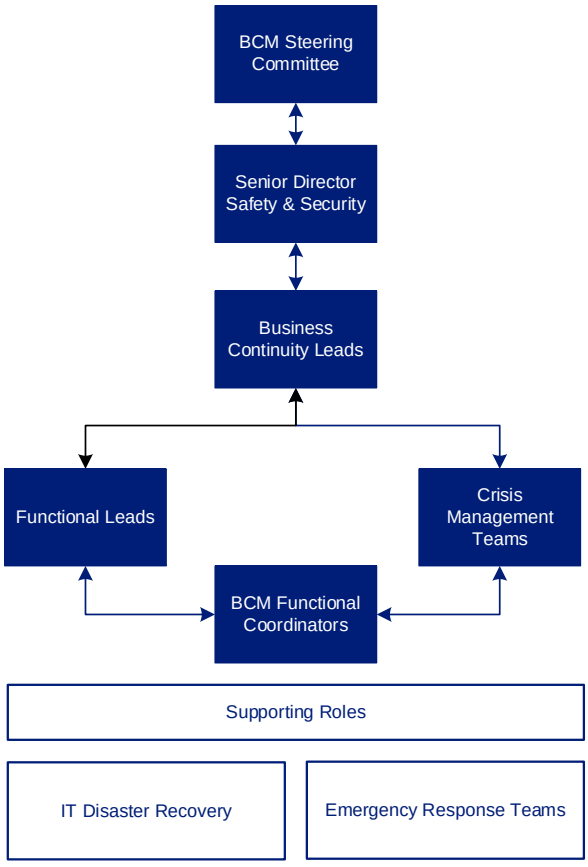
Contents

A. Business Continuity

The mission and objective of Business Continuity is to develop, implement, and maintain Business Continuity Plans that enable NetApp to deliver products and services regardless of the operating environment. In the event of an emergency, NetApp's Business Continuity Program strives to make possible an organized recovery of people, processes and technology so that NetApp's business processes can resume as quickly and efficiently as possible.

B. Governance

NetApp Business Continuity Governance Structure



BCM Steering Committee

.

The Executive Sponsor leads the BCM Steering Committee. The BCM Steering Committee oversees governance for BCM. This document is reviewed annually or as required and approved by the BCM Steering Committee.

C. NetApp's First Responders in the event of an incident.

- Global Safety and Security organization monitors global events as well as incidents near our facilities. They send out alerts to affected individuals and/or teams on a regular basis until the situation is under control or is no longer identified as a potential risk/threat.

- Crisis Management team springs into action following an incident. Based on the incident, the executive management team performs a series of predefined instructions to address the situation with internal and external stakeholders. The Crisis team is connected through email distribution lists and a Crisis App. The app helps identify task owners for the seamless execution of instructions.

- Business Recovery Team works with impacted functional owners individually to assess their situation and identify the Business Continuity Plan to restore impacted operations with minimum to zero impact to NetApp & its customers.

- IT Service Continuity Team is focused on the recovery of IT services (critical infrastructure, customer data and applications) within 24 to 168 hours. Applications reside in three production sites and are backed up to an alternate site. Production sites are in Hillsboro, OR; San Jose & Sacramento, CA. The recovery site is in Research Triangle Park, NC.

D. Key Elements

- Recovery Time: A **business impact analysis** has classified business functions, needs and priorities. Critical systems have asynchronous failover capability of data and applications to the alternate site with recovery available within 1 to 24 hours. For data and applications that must be recovered within 2 – 7 days, recovery plans and scripts are in place for most systems.

- Customer Audit and Access to NetApp Executive Leaders: NetApp provides customer executive leadership with access to their counterparts in Information Technology and Information Security to discuss business continuity and disaster recovery. Opportunities to audit NetApp processes may be discussed on an individual basis.

- Services Logistics operations are located at three main sites and geos (San Jose, CA; Bangalore; and Amsterdam). Business Recovery Plans have been developed for these sites and each site has the capability to maintain global service logistics operations independently. CSS Logistics proactively increases FRU stock in regional depots near possible impact areas to account for adverse conditions at a customer site with NetApp products. CSS has multiple 3PL (Third Party Logistics) partners (DHL and UPS for ASIA/EMEA and UPS for the Americas) and 3PR (Third Party Repair) suppliers located

globally (3 in the United States, 1 in Singapore, and 1 in The Netherland), each with the capability to perform all operations of the other sites in the event of disruption.

Service Partners	Locations
Third-Party Logistics (3PL)	DHL and UPS for APAC & EMEA and UPS for the AMERICAS
Third-Party Repair (3PR)	3 in the United States, 1 in Singapore, and 1 in The Netherlands
Third-Party Maintainers (TPM)	AMERICAS, APAC & EMEA

- Third-Party Maintainers (TPM) provide break/fix services to NetApp Customers. NetApp has documented processes (DR and BC plans) from all its major TPM's. The TPM Organization also has processes to engage NetApp SSE (Solution Support Engineer) resources, if necessary, to perform on-site break/fix services. In disaster situations, NetApp Field Services strategically request engineers and break/fix partners transfer to locations close to impact areas, as safety and local authorities will allow.

  The **Fly & Fix program** enables engineers to fly around the globe as required, to assist customers. This capability ensures NetApp is multi-sourced in all three geos.

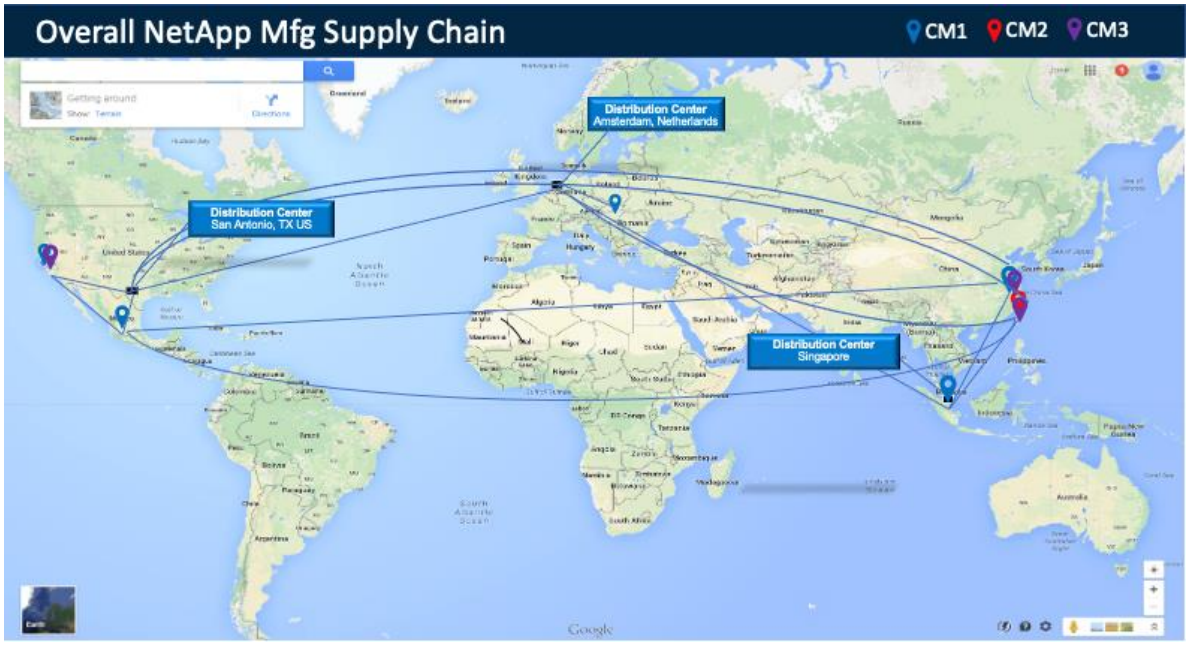
  All the TPM Service Delivery Managers (SDMs), responsible for service delivery and service quality of NetApp TPM partners can work from remote office locations. In the case of emergency, NetApp TPM staff can continue communicating with partners and managing service delivery from remote locations. Regional SDMs and Operations Managers can provide backup support and coverage if local communication channels are not available.

- NetApp Managed Services deliver storage solutions to improve operations and achieve business outcomes. **Managed Service Delivery Team** is responsible for managing the day-to-day operations of the storage controllers in scope as well as being the primary contact for the customer Storage Operations. Service Delivery Manager is responsible for Operations delivery and the primary contact for the meetings, reporting and communications between the customer and NetApp's Managed Services team. The core Managed Service Delivery team is based in India and works in shifts to provide customers 24/7 seamless service. A team chart and call tree are available on request.

  Managed services team manages customer storage operations from NetApp premises using customer interface or using a remote management tool. Customer is responsible for the upkeep of the customer remote interface such as VDI, VPN, etc. when used.

- Contract Manufacturers: NetApp produces product located in all 3 geos for strategic solutions and seamless shipment of product to our customers worldwide; each location with the capability to perform operations of the other sites in the event of disruption. Majority of critical components used in our products are dual-sourced, either from two vendors, from independent plants of a single vendor, or have existing qualified alternatives. In addition, we assume inventory positions in multiple production and supplier locations for all critical components.

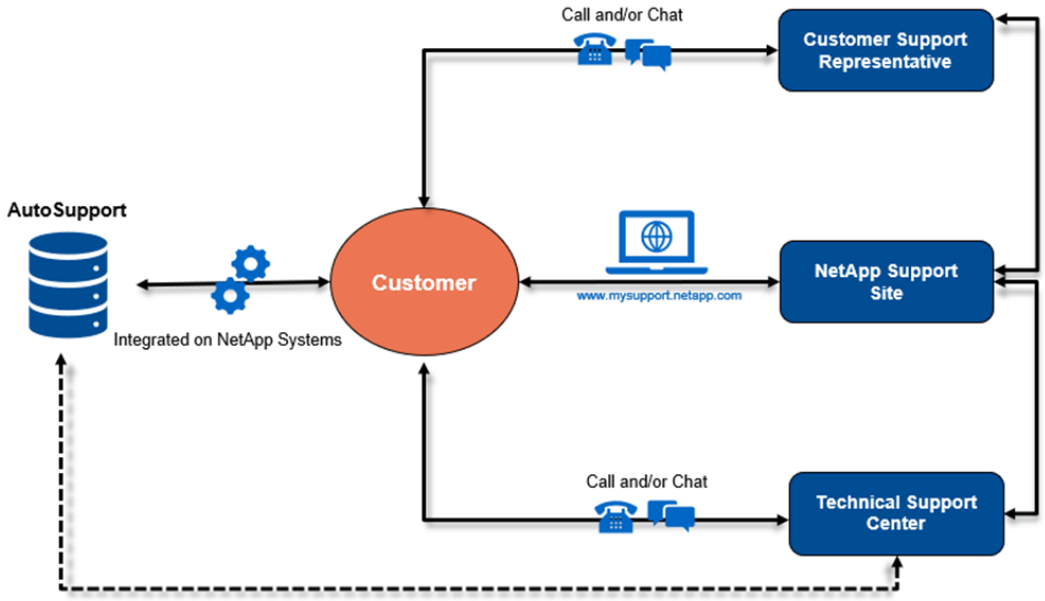
Figure 1: NetApp Manufacturing Supply Chain



- Engineering Sites and Testing Labs: Our distributed and hybrid cloud-based architecture ensures product development and customer support will continue in the event of a regional disaster. Each major engineering site (Raleigh; San Jose; Wichita, Bangalore, Tel-Aviv, and Iceland) have access to distributed remote resources whether an alternate NetApp site, Cloud or SaaS. Key repository services (bug tracking, source code management and document systems), third-party code compliance and build systems have redundancy and offsite backups, where SaaS is used, we are leveraging the SaaS provider contingencies.

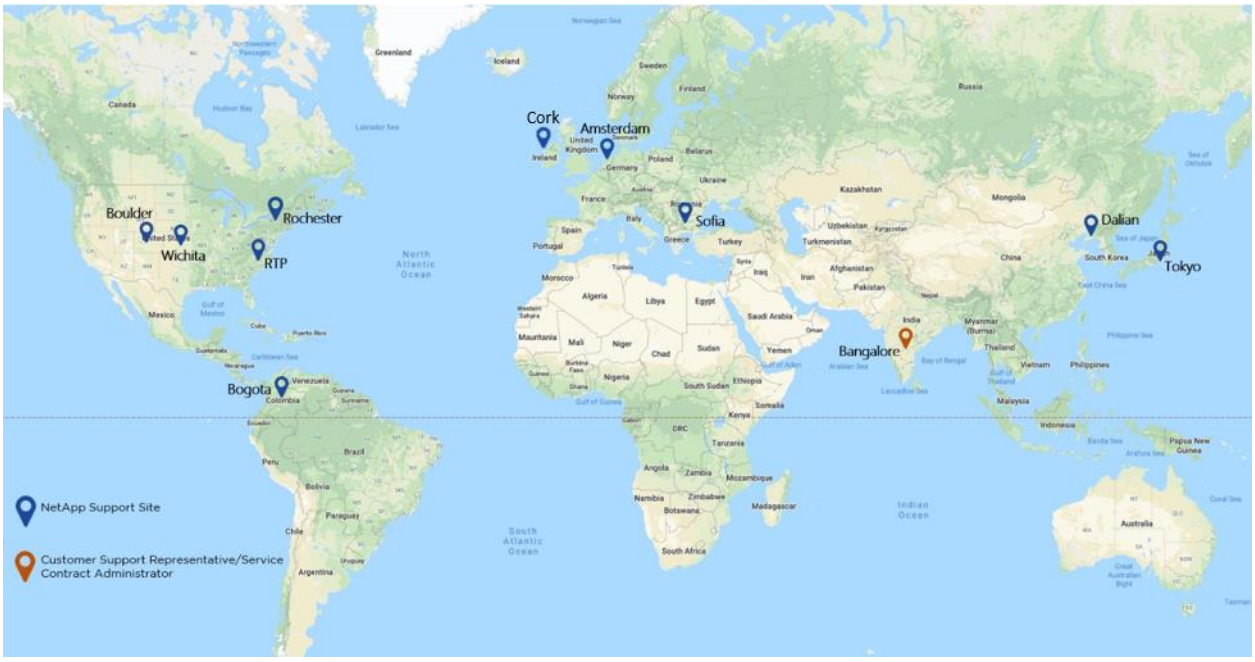
- Customer Support Services:

Figure 2: Support Services overview



- Customer Support Representatives (CSR)/Service Contract Administrator (SCA) team provides customers with assistance on non-technical transactional support including Parts Replacement (PREQ) and Field Support Order (FSO) dispatching, service entitlement issues, install base registration and location updates over the life of a support contract.
- NetApp Support Site (NSS) provides NetApp customers access to a variety of content/information and service functions such as getting a license renewed, requesting a contract renewal, opening a ticket for technical/non-technical assistance, downloading software, etc. all through a digital platform.
- AutoSupport (ASUP) is an integrated and efficient monitoring and reporting feature that constantly checks the health of NetApp systems. It is one of the most important troubleshooting tools for our customers from NetApp support. AutoSupport allows the system to send messages directly to NetApp Technical Support and customer's system administrators.
- Technical Support Center (TSC) is available 24/7, 365 days a year. The centers are coordinated for all support activities around the globe, including phone, chat, remote, and on-site actions. The TSC provides technical troubleshooting, resolution, and root cause analysis for customer product issues that cannot be solved using NSS.

Figure 3: Support Services Mapping



- Technical Support Center ensures uninterrupted customer telephone support from NetApp engineers. NetApp IT has deployed four distinct Cisco CUCM clusters (IP PBX). The sites are Research Triangle Park, North Carolina (RTP); Hillsboro, Oregon (HIO); Hong Kong (HKG); and Amsterdam, Netherlands (AMS). These sites function as hubs for the control systems and Genesys IC Media servers. In addition, the Genesys Interaction Center server, Microsoft SQL DB server, SAP Integration server, callback, chat and Marquee dashboard servers operate in the RTP and HIO data centers. Both HIO and RTP function as mutually supporting active-active nodes.

- *Resilient Telephony:* NetApp has developed a resilient telephony system that is both decentralized and geographically dispersed to ensure that any major disruption does not affect a customer's ability to reach a NetApp Customer Support Engineer who is trained to help in the resolution of technical problems.

  Figure 2 graphically depicts the architecture of NetApp Customer Support telecom architecture. As shown, the system allows for several active-active resources, or quick fail-over capabilities enabling a geographically separate resource to maintain connectivity without noticeable effects on customer support. Our primary telecom provider, Orange, offers the high-availability principal conduit for customer inbound calls with Verizon as the failover. In the event of a failover, all customer calls are immediately rerouted by NetApp, thereby mitigating call delays and subsequent customer impact.

- Contact Center Services: The Contact Center is a SASS-based communications platform and pre-integrated application suite developed specifically to handle all types of interactions in addition to phone calls: voicemails, text chats, and web call-back requests. Figure 4 provides graphical details of the architecture.

  The Genesys Cloud CX architecture is built on Amazon Web Services AWS, Genesys Cloud CX takes full advantage of the ability to have a distributed architecture where all data is replicated across multiple data centers. Using synchronous replication, Genesys Cloud CX data is automatically updated in multiple AZs. AZ locations are engineered to be insulated from failures in other AZs. This effectively results in an RTO of 0. All Genesys Cloud CX services are deployed into multiple AZs. This makes them tolerant in the event of a data center failure and ensures data is not lost if the primary AZ becomes unavailable

Figure 4: Contact Center Architecture

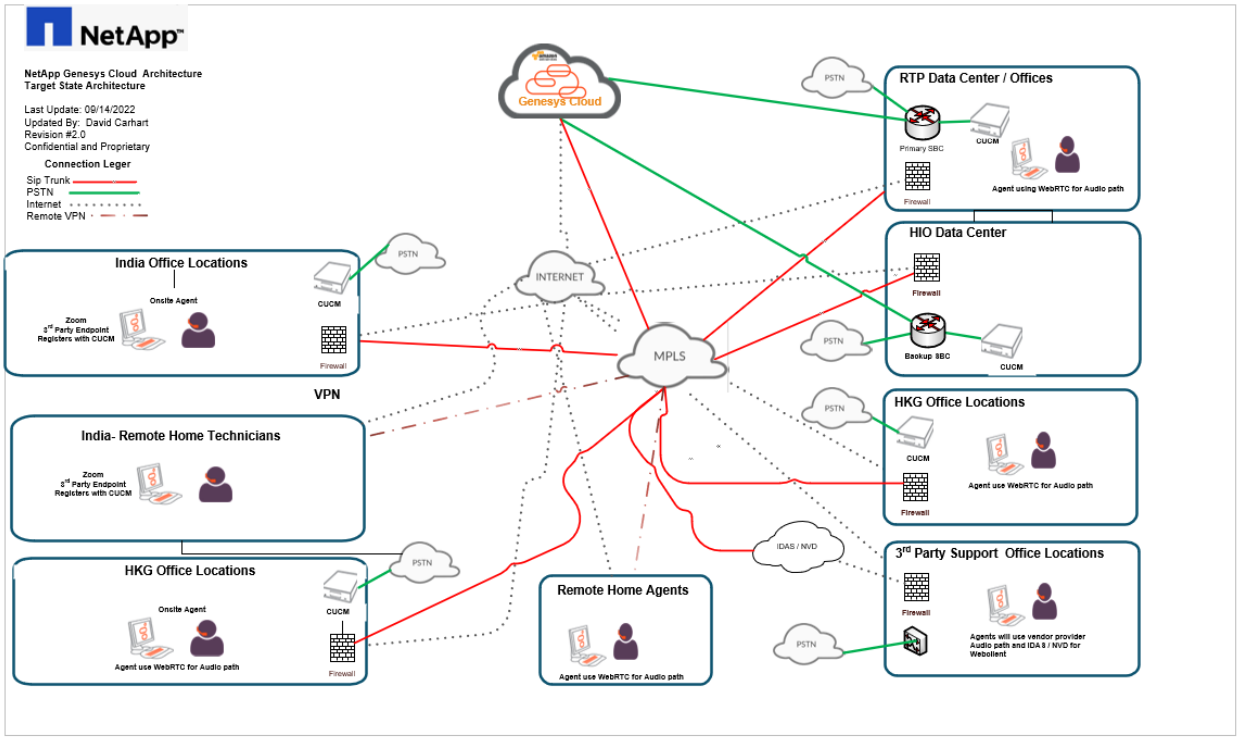
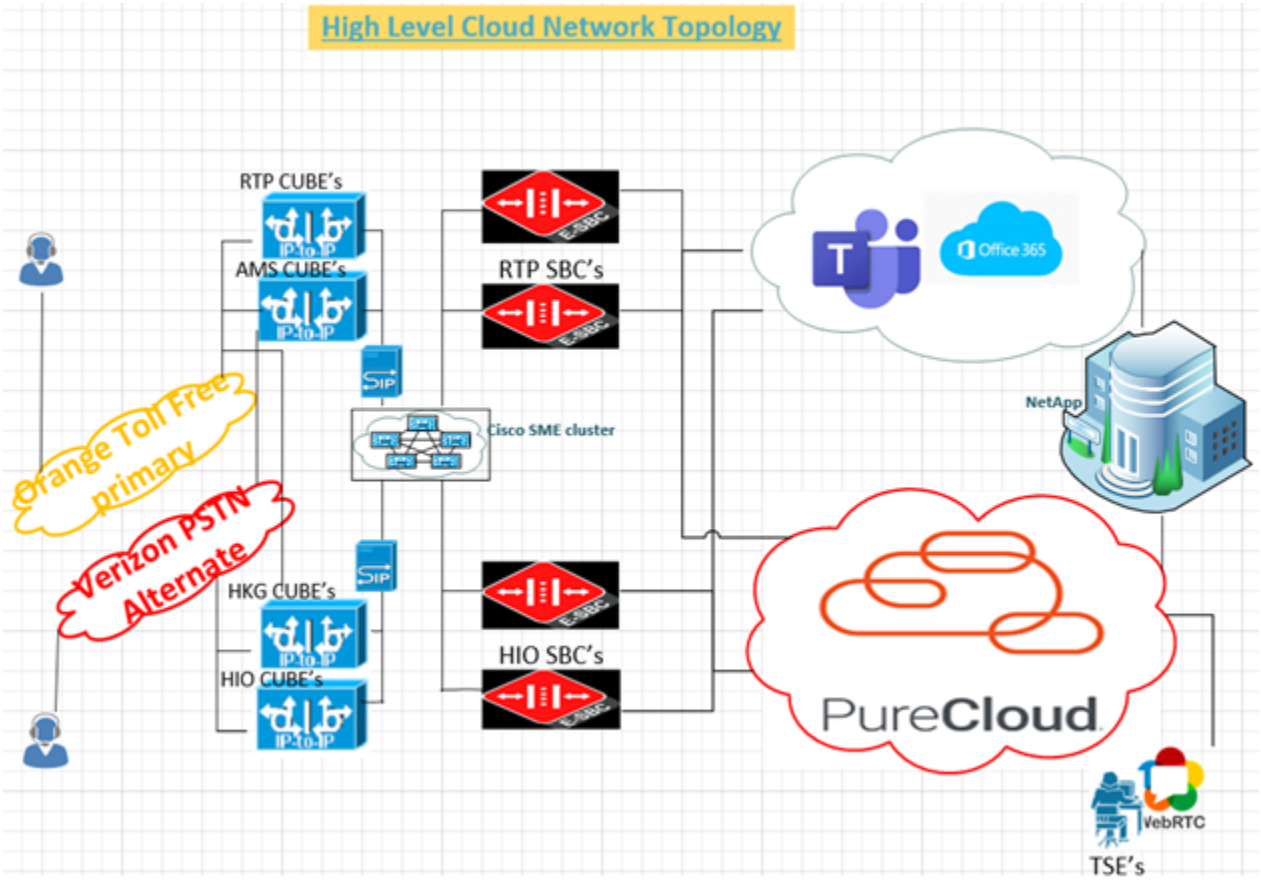


Figure 5: Resilient Telephony



- Call Tree NetApp call trees are tied to its Configurations Management Database (CMD) for our Customer Support Applications in Service Now. The IT Operations Team regularly tests the notification call tree and ensures that all members with a need to know in NetApp receive information when there is a critical issue with any customer service application.

IT Response Team tests contacts members of this call tree at least quarterly through regular updates and the contacts are updated as people change positions within NetApp.

NetApp recognizes that disasters will occur and can have the potential to affect our business. As such, we continue to invest in processes, facilities, and systems to ensure our ability to meet our customers' needs following a disruption. Further questions on this document should be directed to ng-bcdr@netapp.com.