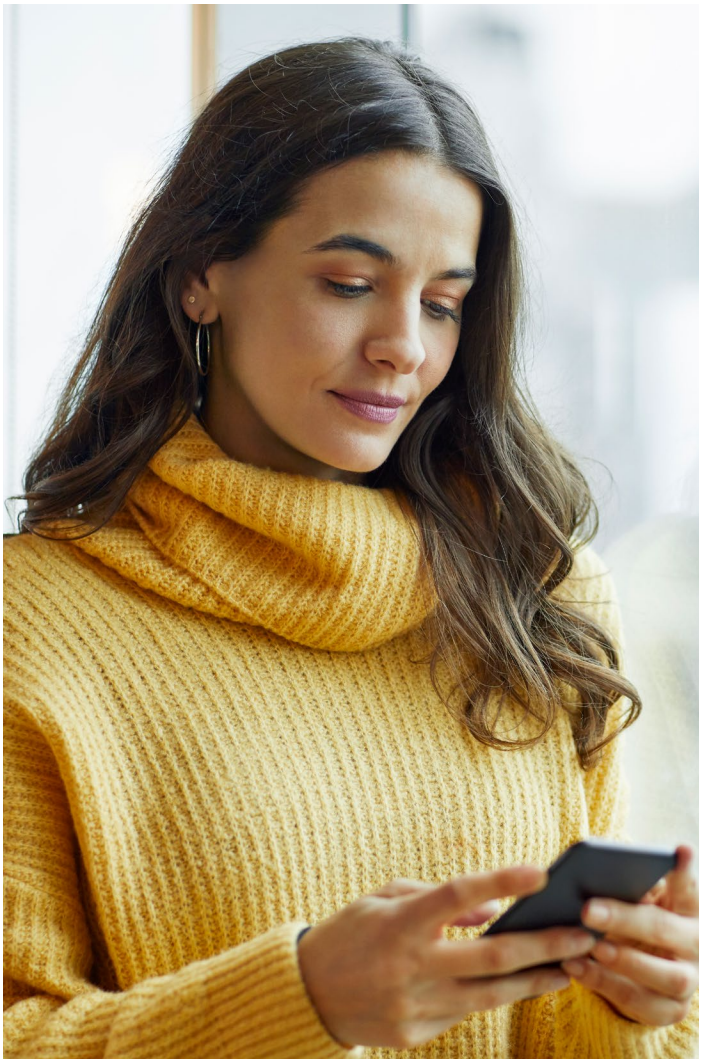
# IBM Cloud for Telecommunications: Technical overview

# Table of contents



# Introduction



Communications service providers (CSPs) are undergoing a major digital transformation as new technologies, such as 5G, edge, and AI come together. As a result, many CSPs are in the process of building a 5G network infrastructure, assessing their multiaccess edge computing (MEC) strategy and moving more of their IT workloads to the cloud. CSPs must evolve their business models to transform from traditional network and content services, such as voice, internet, TV and so on, to high-value industry services, including manufacturing, financial services, healthcare and more. So how do CSPs serve those in other industries? By providing highly differentiated services that redefine a CSP's true potential. To succeed with digital transformation, CSPs need to:

- Deliver on the promise of next-generation edge and 5G services
- Deploy and manage new cloud capabilities
- Enrich relationships with AI-driven engagement

The fact is CSPs must modernize, but they must do so while managing cost and risk effectively. The mistake would be to embrace point solutions that make bold promises. Point solutions may address one need, but they add to the burdens of management and infrastructure that are already weighing down businesses.

By contrast, IBM is announcing the first high trust, unified architecture that addresses the fundamental transformation challenges facing CSPs today. We've announced multiple products and services that run on premises that can be used to provide network function virtualization infrastructure (NFVI) and MEC. These services allow telecommunication providers to connect their on-premises environments to the cloud in a security-rich environment and achieve the high availability and performance they require.

This paper touches on the business imperatives of this transformation, as well as the technical challenges facing CSPs. Specifically, the paper describes the IBM Cloud® options that are available, and highlights important performance, networking and connectivity options between on-premises telecommunication environments and public cloud environments.

# History and background

Over the past 10 years CSPs have been moving from a model of using appliances built on custom hardware and supporting specific network functions to a software-based model where the same functions are delivered by virtualized software residing on generic hardware. Virtualizing network functions reduced the need for specialized networking hardware which, in turn, offered the potential to drastically reduce costs for CSPs. Network cloudification involves moving these virtualized network functions (VNFs) and, in the very near future, containerized network functions (CNFs) over to cloud platforms. This transfer to cloud platforms provides the flexibility to make the best placement decision on edge clouds, private clouds or public clouds according to network topology, performance, high availability and cost requirements.

The move to network cloudification means that network functions can run on the same cloud as IT and other workloads. It also means that workloads can be automatically provisioned to run wherever they're best suited, either near the end user, known as edge computing, in core private data centers or on public clouds. This evolution offers the promise of greatly reduced operational costs. It also provides a new level of flexibility and agility for CSPs, allowing them to innovate and deploy new services as quickly and inexpensively as their new competitors: the over-the-top (OTT) companies.

This evolution by CSPs toward network cloudification isn't without its problems. The traditional network equipment providers (NEPs) know that if CSPs can make this move, they stand to lose a significant amount of revenue and strategic control over CSP technology decisions. This opportunity has resulted in a new crop of startups and challengers entering the market with cloud-native functions, but it remains to be seen how fast operators adopt these new entrants or continue to push their traditional suppliers and NEPs to help them make the transformation to cloud environments.

## Why is network cloudification so important?

Network cloudification is important to CSPs that are seeking to stave off increased competition, which is lowering both revenue and operating margins at a time when data usage is exploding, particularly for video traffic. CSPs need a way to quickly and efficiently scale network capacity to meet demands in a cost-effective way. They can no longer rely on traditional services to grow revenue, so they need a network that will allow them to rapidly develop and deploy new revenue-generating services.

## What's special about telecommunications NFV workloads?

When considering executing telecommunications workloads on the public cloud, there are a few important considerations. With NFV deployments, telecommunication providers have specific requirements, such as:

- Secure logical partitioning of workloads, controlled by access control lists and security groups
- Control over the provisioning of subnets and routing configuration
- The ability to configure secure VPNs for management and connectivity

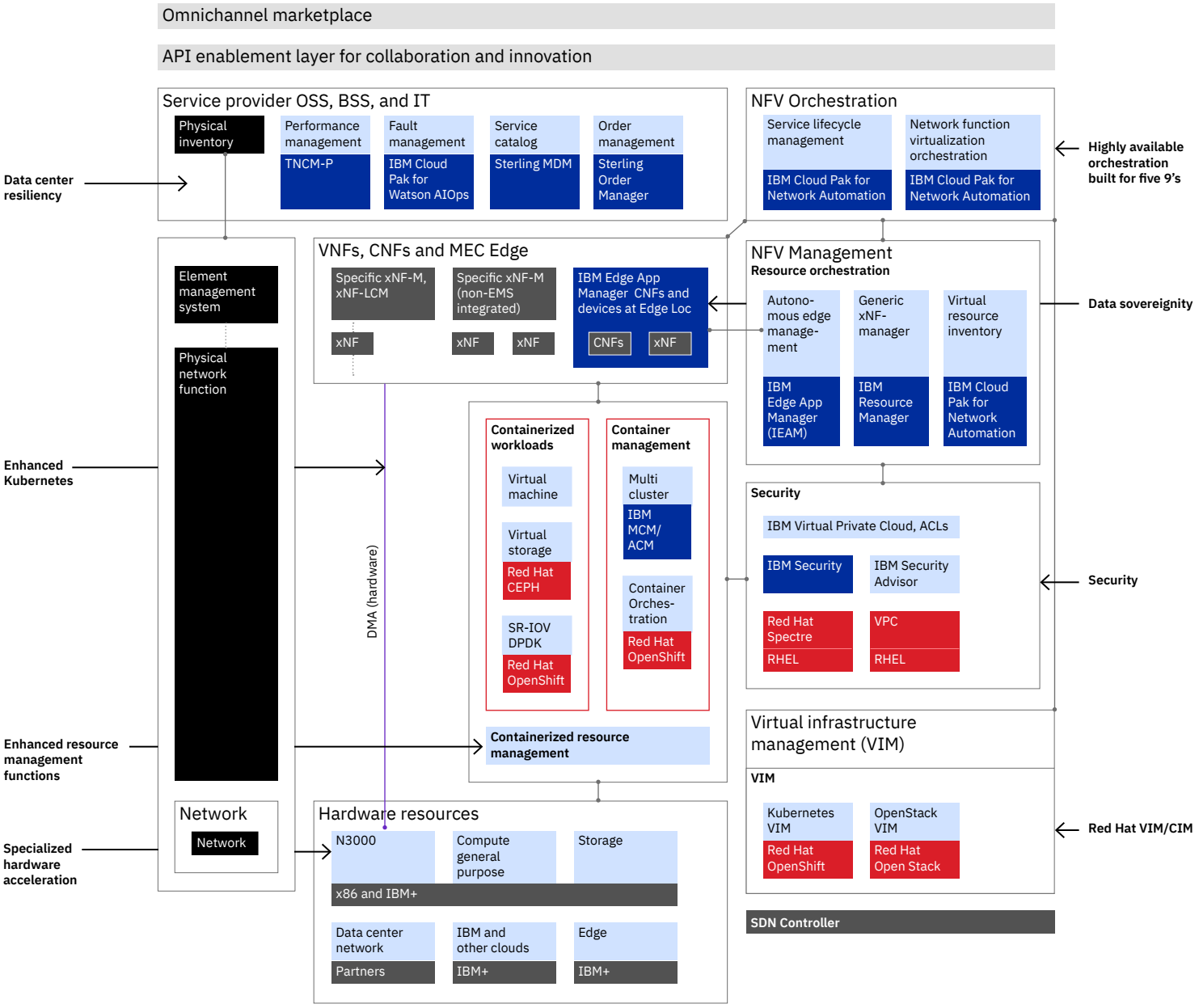
Other features, such as single-root input/output (I/O) virtualization (SR-IOV), Data Plane Development Kit (DPDK), anti-affinity group support, non-uniform memory access (NUMA), and CPU pinning are all features found in telecommunications NFV infrastructure (NFVi), as well as specifications for packet processing speeds and strict latency requirements.

# What are the features of IBM Cloud for Telecommunications?

IBM has implemented several unique functions into IBM Cloud for Telecommunications. Using experiences gained in the financial services industry, IBM has carried over its expertise in regulatory compliance, which for CSPs translates into support for General Data Protection Regulation (GDPR) compliance and data sovereignty. In addition, a number of enhancements have been made to the Red Hat OpenShift environment to support the unique performance and packet processing requirements demanded by telecommunication network functions.

Telecommunication enhancements to IBM's public cloud container environment fit into several categories: enhanced Kubernetes networking functions, extended resource management, enhanced security, data center resiliency, high availability, data sovereignty and regulatory compliance. The enhancements to IBM's public cloud offering for the telecommunications industry are shown on the IBM Network Cloudification Reference Architecture.

# Reference architecture for IBM telco public cloud




- IBM capabilities
- IBM products
- Red Hat capabilities and products
- Partner capabilities

## Enhanced Kubernetes

The enhanced Kubernetes networking functions include SR-IOV, DPDK, IP address management (IPAM), media access control virtual local area network (MacVLAN), and Stream Control Transmission Protocol (SCTP) functions that allow containers to perform network actions directly on network interface cards (NICs) bypassing the host kernel and container management environment. The enhanced Kubernetes functions have been implemented by incorporating the defacto standard Multus container network interface (CNI) into Red Hat® OpenShift® software to allow an application to have a choice of CNI capabilities. In addition, there's an option to use one CNI as a master Kubernetes interface for networking and have an alternate CNI for secondary network interfaces. Multus is a meta CNI that allows CSPs to daisy chain other CNIs and is quickly being adopted by networking vendors in the core, radio access network (RAN) and deep packet inspection (DPI) markets.

**Single-root input/output virtualization (SR-IOV)** is a mechanism that virtualizes a single Peripheral Component Interconnect Express (PCIe) Ethernet controller to make it appear as multiple PCIe devices. Telecommunication providers have been deploying SR-IOV for their virtualized Evolved Packet Core (vEPC) VNFs to obtain the required performance from their applications and to share a physical NIC among multiple virtual machines (VMs).

**The Data Plane Development Kit (DPDK)** consists of a set of libraries and user-space drivers to accelerate packet processing on any CPU. Designed to run in the user space, the DPDK enables applications to perform their own packet processing operations directly on the NIC. The DPDK provides the minimum functions needed to implement performance-sensitive functions in the cloud. It delivers lower latency because it allows containerized functions to bypass the operating system kernel and associated protocol stack to perform actions directly on the underlying hardware.

## Extended resource management functions

The extended resource management functions include functionality, such as NUMA, CPU pinning and anti-affinity group support, which allows container managers to orchestrate specific telecommunication common navigator frameworks (CNFs) to run on specific host systems.

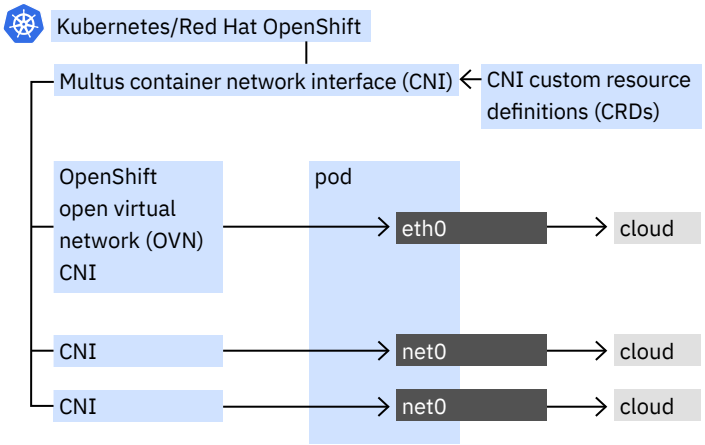
**Non-uniform memory access (NUMA)** is a shared memory architecture where a cluster of microprocessors in a multiprocessing system can be configured to share memory locally, thus improving performance and the ability of the system to be expanded. The advantage of the NUMA architecture as a hierarchical shared memory scheme is its potential to improve average case access time through the introduction of fast, local memory.

**Huge Pages** can improve performance for workloads that execute large amounts of memory access. This feature of the Linux® kernel enables processes to allocate memory pages of size 2 MB/1 GB, instead of 4 K. Additionally, memory allocated using Huge pages is pinned in physical memory and cannot be swapped out. Huge Pages support is configurable on supported instance types.

**CPU pinning** is a technique that enables the binding and unbinding of a process or thread to a CPU, or a range of CPUs, so that the process or thread will execute only on the designated CPU. This process is used to dedicate virtual central processing units (vCPUs) to VNFs and avoid sharing or dynamic rescheduling of CPUs.

**Anti-affinity group support** the ability to use a policy to drive how the nodes in a cluster are spread across the physical hardware. Using this policy, the nodes in a cluster can be colocated on the same physical machine, also known as affinity, or spread onto as many physical machines as possible, known as anti-affinity.

## Additional networks and capability



## Improved container security

IBM and Red Hat provide guidance on how to deploy on OpenShift software to maximize container image security. These guidelines cover container management, as well as service lifecycle management. In addition, RHEL keeps containers isolated from one another as part of the operating system, which keeps processes—and extension containers—from making unauthorized access to system resources.

**Host groups and container access list support and secure CNF and VNFs** is the ability to define which hosts and specific users have access to which containers. It's an enhanced security feature that's designed to restrict container access to the smallest set of users and only those with a specific need or reason for access. As telecommunication operators implement new secure services, such as remote embedded subscriber identification module (eSIM) provisioning, the need for access lists and secure containers will become paramount.

## Improved cloud security features

In designing IBM Cloud for Telecommunications, IBM was able to draw upon its extensive knowledge and experience from the financial services industry and, based upon this experience, IBM added security features that fit into several categories:

- **Access control list (ACL)** is the ability to specify which hosts or other entities have access rights to which resources in a cluster, allowed or denied. With advanced role-based access controls and secondary workflow approval, the risk of administrative error and unauthorized access is significantly reduced.

- **Virtual private cloud** is literally a private cloud hosted on a public cloud. IBM Cloud for Telecommunications implements a library of functions designed to support this capability. CSPs require this functionality to implement security-rich transactions or provide an additional measure of security for a specific function or set of containers, providing a security-rich private service.

- **Auditing of access and changes.** IBM Cloud for Telecommunications has been enhanced to include detailed tracking of access and changes to cluster and container configurations. This audit trail can be stored locally for security and data sovereignty reasons or remotely. The audit log creates a trail of changes based upon a stream of access, update and change log events. IBM Cloud for Telecommunications includes continuous monitoring, real-time reporting, audit-quality logging and automated compliance templates to help reduce audit risks and enhance compliance readiness.

- **Bring your own key (BYOK) and keep your own key (KYOK) management** for keys and data is a feature of IBM Cloud for Telecommunications that allows a service provider to provision and manage highly secure data for services without sacrificing performance. IBM Cloud BYOK and KYOK acts as an extension to IBM Cloud, adding a powerful concept where CSPs stay in control of their essential secure key infrastructure while benefiting from a seamless integration into IBM Cloud services. In the case of suspicious behavior, keys can be erased, keeping the data from being decrypted. Customers can also roll their keys to allow for reorganization of the key owners or remove access as needed.

## High availability built for telecommunications networks

**Multi-zone region (MZR) for high availability** is a feature of IBM Cloud that allows a load balancer appliance to achieve high availability and redundancy. When provisioning a load balancer, the subnet where it should be created must be specified. If that data center is part of an MZR, one appliance is deployed in the selected data center while the second is deployed in a different data center within the same region. In this way, telecommunication functions can be deployed over multiple data centers to help ensure backup, failover and redundancy.

**IBM Cloud Pak® for Network Automation** is IBM's intent-based orchestrator that's specialized for the telecommunications industry. Cloud Pak for Network Automation provides intent-based orchestration for Day 0 install, Day 1 launch and Day 2 ongoing management categories of network service workloads. A key aspect of ongoing management is service healing and service restoration in case of failure. Failures will inevitably happen, and the true resilience of a service is defined by how well it recovers from these failures. A truly resilient service needs to be capable of recovering from software, hardware and connectivity issues—in short, issues that can combine to create outage scenarios that can render a whole data center inoperable or uncontactable.

To help ensure successful recovery from outage situations, IBM Cloud Pak for Network Automation uses the IBM public cloud to help ensure that it can rapidly recover itself, and then recover all other affected services. Cloud Pak for Network Automation replicates critical stateful information reliably in the security-rich IBM public cloud so that in the event that the primary orchestration instance suffers catastrophic failure, a secondary standby instance in the cloud can take over to rapidly recover any affected network services.

## Data sovereignty: Regulatory and compliance

As has been mentioned previously, IBM was able to draw upon its extensive knowledge and experience from the financial services industry when adding features for the IBM Cloud® for telecommunications service providers. The regulatory and compliance features that were added include data sovereignty features, as well as GDPR compliance features.

**Data Sovereignty** features of IBM Cloud for Telecommunications include the IBM Cloud Satellite™ solution. The IBM Cloud Satellite solution allows CSPs to keep the data contained on the edge without ever traversing the network, meaning there can be no violation of data sovereignty regulations. IBM Cloud for Telecommunications enables administrators to set policies so that workloads can only run on proven, trusted hosts that are physically located within defined parameters. Sensitive workloads can be managed by policies to run on a trusted platform at a preferred location. In addition, IBM Cloud Secure Virtualization includes the ability to only allow virtual server data to be decrypted in authorized locations, improving compliance and security.

**IBM's commitment to GDPR readiness**

IBM Cloud underwent a comprehensive GDPR readiness program. Its robust contractual commitments to privacy and data protections are detailed at http://www.ibm.com/dpa. These protections include minimum technical and organizational measures (TOMs), data subject rights and data transfer mechanisms.

IBM is committed to providing our clients and IBM Business Partners with innovative data privacy, security and governance solutions to assist them on their journey to GDPR compliance. IBM is a recognized leader in data protection and complies with data privacy laws around the world. In preparation for the European Union's GDPR, which came into effect on May 25, 2018, IBM established a comprehensive compliance framework to help ensure GDPR compliance for all IBM products and services. As part of this global program, IBM reviewed and enhanced IBM products and services for GDPR, developed GDPR-ready contracts for clients and suppliers, and actively engaged with clients and suppliers on GDPR compliance.

# Conclusion

As discussed, the telecommunications industry is undergoing a significant transformation. As cloud, 5G, edge, and AI come together, the decisions that CSPs make now will have far-reaching implications. To succeed, CSPs need to evolve their business models and start moving from traditional network services to high-value industry services. It will not be enough to just provide voice and broadband data connectivity services. CSPs must consider highly differentiated services that are delivered through the cloud and enriched by AI-driven engagement.

IBM Cloud for Telecommunications helps providers satisfy their network workloads, plus position them for innovative cloud capabilities.

For more information visit ibm.com/industries/telecommunications/network-automation.

# About the author

**Craig Farrell**

VP and CTO Global Telecom Industry, Distinguished Engineer, IBM

craig.farrell@us.ibm.com

linkedin.com/in/craig-farrell-01665635/

Craig Farrell is currently Vice President and Chief Technology Officer, Global Telecom Industry, at IBM. Craig is responsible for Telcom industry requirements, architectures, frameworks and standards efforts. With over 25 years industry experience Craig is also a member of the Telemanagement Forum (TM Forum) collaboration sub-committee. Craig joined IBM in 2006 as part of IBM's acquisition of Micromuse (NASDAQ: MUSE) where he served as the CTO. Craig joined Micromuse as part of its 2003 acquisition of NETWORK HARMONi, a company he co-founded in Australia and served as President and CEO. Craig holds a BSc (Hons) in Computer Science from the University of Western Australia and a Ph.D. in Computer Science from Curtin University. In 2009 IBM named Craig an IBM Distinguished Engineer and in 2010 he became a member of both the IBM Industry Academy and IBM Academy of Technology.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2021