

Envisioning Service Management and Orchestration for 5G

Toward a Modular Multi-Vendor, Multi-Cloud SMO Spanning Beyond RAN to Core and Edge

Table of Contents

Introduction	3
SMO in the O-RAN Alliance's Architecture	4
O-RAN Components	5
O-RAN Interfaces	5
SMO Capabilities in O-RAN	6
Defining the Functional Areas of the SMO Layer	6
How VMware Supplies SMO Capabilities for O-RAN	8
Flexible SMO Components	8
VMware Telco Cloud Automation	8
VMware Centralized RIC	9
VMware Telco Cloud Service Assurance	10
Extending the SMO to Manage Domains Beyond the RAN	11
Multi-Cloud Automation and Orchestration	11
Resource Optimization	12
Multi-Cloud Operational Consistency	12
Multi-Layer Automation	12
Multi-Vendor Applications from the Edge to the Core	13
Managing Multi-Vendor Applications	13
Orchestration and Workload Placement with Scale-out Capability	13
Support for Kubernetes Lifecycle Functions	13
Separation of Concerns	13
Capabilities for creating a CSAR file	13
Service Assurance for Networks and Systems	14
Integration with Other SMO Components	14
Automated Discovery and Topology Mapping	14
Fault and Performance Management	14
Automated Root Cause and Service Impact Analysis	14
Conclusion: Toward a Multi-Vendor, Multi-Cloud, Multi-Domain SMO	15
Resources and References	15

Introduction

Service providers want to improve flexibility and speed up 5G deployments by adopting architectures that can deploy multi-vendor services and tailor customer experiences in a dynamic, multi-cloud environment. In the O-RAN Alliance’s architecture for open radio access networks, the architectural element that ties together the complex layer of platforms and software for deploying and managing decomposed radio access networks is called Service Management and Orchestration, or SMO. It manages the RAN domain.

Many communications service providers have combined existing management functions, open source tools, and new capabilities into their own version of a RAN management layer. At any given CSP, existing RAN management functions and systems often take the form of complex custom solutions cobbled together over time in house. Open source tools and new capabilities were typically added in stages to address requirements as they emerged.

The shift toward 5G, of course, only heightens this complex combination of old and new solutions at the same time that rolling out and managing 5G solutions requires efficient operations and far-reaching automation across multi-vendor radio access networks and multiple clouds. Automation is seen as the key to minimizing the cost of operating complex networks and systems as they evolve from 4G to 5G.

Monetizing 5G hinges on automation and orchestration. They help increase revenue by fostering on-demand communication services tailored to new use cases and customer requirements, such as network slicing and personalized SLAs. With information about each component’s state and performance, automation and orchestration can significantly improve the management of network resources and customer experiences by acting in near real-time to dynamically allocate resources, optimize networks, and resolve issues.

The open RAN architecture of the O-RAN Alliance charts a course for SMO. It points toward a virtualized, containerized, disaggregated, and standardized open radio access network that supports multiple vendors and clouds by using an SMO layer to automate and optimize the RAN and its applications. The O-RAN Alliance’s work to disaggregate, define, and standardize the SMO layer for the RAN is in progress, and engineers from VMware are actively participating in the O-RAN Alliance’s efforts.

But what if the vision for SMO can be extended beyond the RAN to govern the other key domains of service providers’ networks: the core, transport network, and edge?

ABOUT THIS WHITE PAPER

This white paper sets forth a vision for the SMO layer that combines open interfaces and cloud-native technology with a modular, component-based architecture extensible enough to support multiple vendors, applications, and clouds across not only the RAN but also the core and edge.

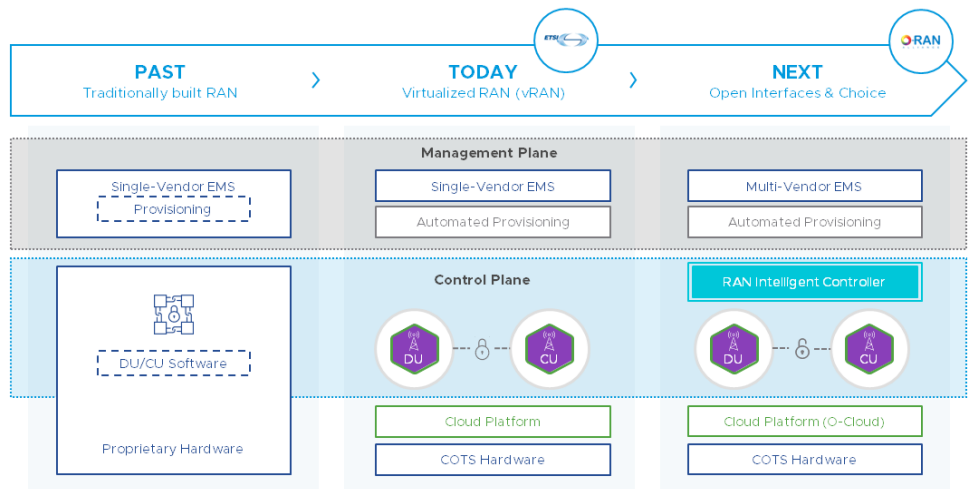


Figure 1: The path to a disaggregated, open radio access network.

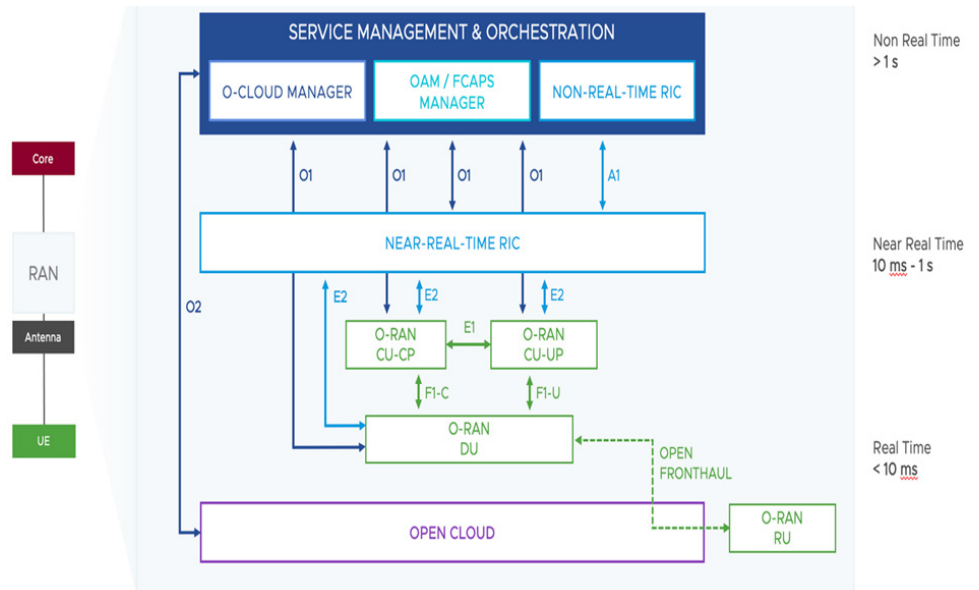


Figure 2: The O-RAN Alliance's logical architecture and its interfaces. Source: O-RAN Alliance.

This white paper sets forth a vision for the SMO layer that combines open interfaces and cloud-native technology with a modular, component-based architecture extensible enough to support multiple vendors, applications, and clouds across not only the RAN but also the core and edge.

SMO in the O-RAN Alliance's Architecture

The O-RAN Alliance's architecture extends the 3GPP's open RAN architecture to further disaggregate the radio access network and open it up to multiple vendors. As such, the O-RAN architecture not only splits many of the components of the 3GPP architecture, it also introduces a new component: the RAN intelligent controller, commonly referred to as the RIC.

In the O-RAN architecture, there are two logical forms of the RIC, and each performs a different function.

- The near-real-time RIC is a distributed RIC that runs extensible microservices from third-party vendors, called xApps by the O-RAN Alliance, to manage and optimize resources for network functions.
- The non-real-time RIC is a centralized RIC that hosts rApps to do such things as collect data, build machine learning models, and send optimization policies to the near-RT RIC for execution.

Both the near-real-time RIC (near-RT RIC) and the non-real-time RIC (non-RT RIC) are virtualized or containerized logical components that play a role in controlling and optimizing RAN elements and resources.

Here is a short overview of the O-RAN architecture; for details, see the [O-RAN Alliance's white papers](#) and [specifications](#).

- **O-Cloud:** A cloud computing platform composed of physical infrastructure nodes meeting O-RAN requirements to host O-RAN network functions, whether virtualized or containerized, including the near-RT RIC, the CU control plane (O-CU-CP), the CU user plane (O-CU-UP), and the O-DU. The O-Cloud furnishes a distributed containers as a service (CaaS) layer to support RAN workloads.
- **SMO:** The Service Management and Orchestration layer manages the components and network functions of an open RAN. This layer includes the non-RT RIC.

O-RAN Components

The O-RAN architecture also includes the following network functions and components.

COMPONENT	DESCRIPTION
O-CU-CP/UP	The centralized unit of the RAN and its control plane and user plane.
O-DU	The distributed unit of the RAN.
O-RU	The radio unit processes radio frequencies from antennas and other equipment.
O-eNB	The open evolved NodeB refers to hardware supporting 4G RAN as well as PNFs.

O-RAN Interfaces

In the O-RAN architecture, the following interfaces come into play; some of them are specified by the 3GPP.

INTERFACE	DESCRIPTION
A1 Interface	This interface supports workflows between the Non-RT RIC and Near-RT RIC. For example, the non-RT RIC can use this interface to deploy configuration and optimization policies to the near-RT RIC and the applications running on it.
O1 Interface	This interface connects the SMO to the Near-RT RIC, one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.
O2 Interface	This interface is between the SMO layer and the O-Cloud to support orchestration of O-Cloud infrastructure and the deployment of network functions.
E2 Interface	This interface connects the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, one or more O-DUs, and one or more O-eNBs. The E2 Interface allows the near-RT RIC to control the procedures and functionality of the E2 nodes.
R1 interface	This interface supports the portability of multi-vendor rApps and delivers services to rApp developers.
Open Fronthaul CUS-Plane Interface	The interface between the O-RU and O-DU.
Open Fronthaul M-Plane Interface	The interface between the O-RU and O-DU as well as between the O-RU and SMO

These components, network functions, or interfaces can be supplied by, or governed by, various vendors.

DECONSTRUCTING THE RIC

The O-RAN Alliance's architecture decouples the RIC:

- The non-real time (Non-RT) control functions of greater than 1 second typically reside in the non-RT RIC
- The near-real time (near-RT) control functions of between 10 milliseconds and 1 second reside in the near-RT RIC

The non-RT functions are located in a centralized SMO layer. Non-RT functions typically include service and policy management, RAN analytics, and training for machine-learning models.

Trained machine-learning models, artificial intelligence-enabled policies, and real-time control functions produced in the non-RT RIC are distributed to the near-RT RIC for runtime execution. The near-RT RIC resides outside the SMO layer in a distributed environment.

The O-RAN A1 interface connects the the non-RT RIC in the SMO layer with the near-RT RIC.

As a result, you can modify the RAN and program your network according to models optimized to meet your network's unique policies and objectives.

VMWARE RIC

- VMware Centralized RIC is a non-RT RIC that resides in the SMO.
- VMware Distributed RIC is a near-RT RIC that resides outside the SMO.

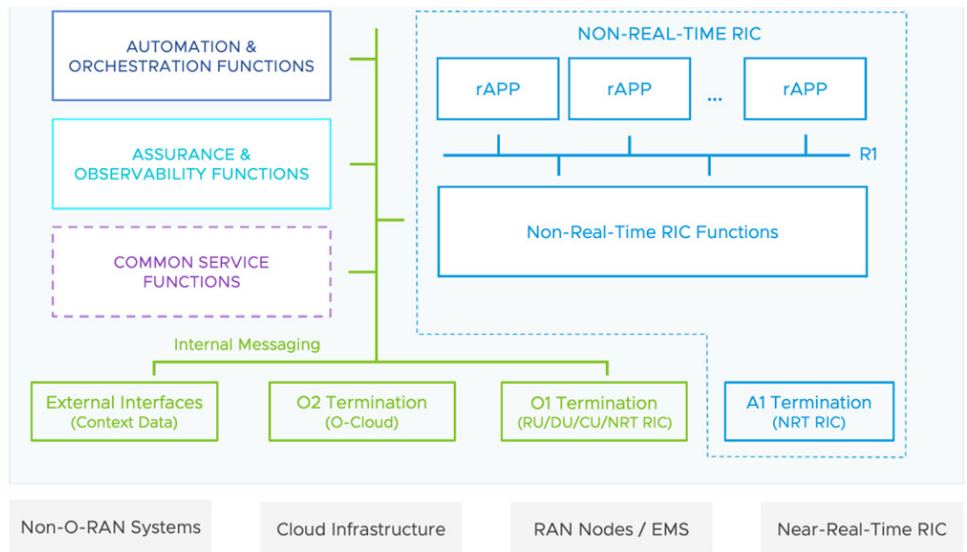


Figure 3: The components and interfaces of the O-RAN SMO organized by function.

For 5G, the SMO is likely to contain a combination of systems and infrastructure from various vendors, including connections to multiple clouds.

SMO Capabilities in O-RAN

The role of the SMO in the O-RAN Alliance's architecture is to oversee the orchestration, automation, and control of RAN functions and infrastructure. The key capabilities of the SMO in the O-RAN architecture are as follows:

- Termination and management of the Fault, Configuration, Administration, Performance, and Security management interface (FCAPS) from the RAN network.
- Management of the non-RT RIC. The non-RT RIC manages RAN functions and resources by providing higher-layer procedure optimization, policy optimization in the RAN, and guidance, parameters, policies, and AI/ML models to support the operation of near-RT RIC functions in the RAN to meet higher-level, non-real-time objectives.
- O-Cloud management and orchestration through the FCAPS interface and data model.
- Overall orchestration and workflow management for the RAN.

The SMO performs these services through four key interfaces with the O-RAN elements:

- A1 interface between the Non-RT RIC in the SMO and the Near-RT RIC for policy management, information enrichment, machine-learning model management services.
- O1 interface between the SMO and the O-RAN network functions for FCAPS support.
- In the hybrid model, Open Fronthaul M-plane interface between SMO and O-RU for FCAPS support.
- O2 interface between the SMO and the O-Cloud for infrastructure and deployment orchestration and management.

Defining the Functional Areas of the SMO Layer

The following definition of an SMO layer includes the functions defined by the O-RAN Alliance's reference architecture, namely the orchestration and management functions and the non-real-time RIC. The O-RAN Alliance's SMO definition, however, can be extended beyond O-RAN to include the management of the core, edge, and transport domains as

well as the legacy RAN domain. Extension of the SMO layer to incorporate these other domains is discussed in more detail later.

Keep in mind that this section seeks to define the domains of the SMO layer, not to describe the domains for which VMware necessarily has solutions; VMware solutions for the SMO layer are presented in a later section. It is assumed that some of the following services are to be delivered by integrating VMware components with components from other vendors, VMware partners, or a CSP's custom system. The VMware vision of SMO sees the following functional areas being loosely coupled with defined APIs for flexibility, ease of integration, and multi-vendor support:

- Orchestration and Management
- Analytics and optimization
- Centralized end-to-end assurance and observability
- Common services
- Domain management

Here is a description of each of these functional SMO areas.

Orchestration and Management functions (O&M) enable you to automate provisioning and lifecycle management of network functions and infrastructure software in a multi-cloud environment. This functional area should include the following:

- Onboarding and lifecycle management of RAN network functions, including network functions for the RU, DU, CU, and the RIC
- Service and slice design
- Provisioning and management of the CaaS and IaaS layers over registered clouds
- Onboarding and lifecycle management of rApps hosted on the non-RT RIC and xApps hosted on the near-RT RIC
- Catalogs and inventories of onboarded and instantiated software across every site
- Dynamic resource allocation for the placement of RAN network functions

Analytics and optimization functions enable you to improve resource management and customer experiences through data-driven network optimization delivered through a suite of multi-vendor rApps. The non-RT RIC, which hosts rApps, should perform open-loop or closed-loop control and conflict mitigation over the R1 interface defined by the O-RAN Alliance.

Assurance and observability functions should drive centralized end-to-end observability and service assurance across domains, including not only the RAN but also the core, transport, and edge domains. Assurance and observability functions should support such capabilities as end-to-end network monitoring, root-cause analysis, and the ability to set remediation procedures that reduce MTU and MTTR of issues. The assurance and observability functions should apply to the O-RAN architecture's physical, transport, virtual, software, and service layers.

- Collection and normalization of data across multi-vendor deployments
- FCAPS functions for the O-Cloud infrastructure
- Observability and assurance of PaaS and CaaS layers, Kubernetes clusters, workload orchestration, and FCAPS
- Correlation and root cause analysis
- Trigger remediation

Common service functions can centralize data collection from the RAN as well as external sources, such as NWDAF, data lakes, and AI/ML platforms. Common services can also distribute data and analytics to the other SMO functional domains.

THE MULTI-CLOUD SMO LAYER FOR 5G

Capitalizing on the opportunities of 5G in a multi-cloud world hinges on two key SMO ingredients: cloud-native technology and cloud-specific automation.

Cloud-native technology decouples containerized functions from the infrastructure so they can be deployed quickly, shared among services, updated easily, and managed independently. Orchestration and automation dynamically scale network functions to meet changes in demand. With containers as a service (CaaS), CSPs can use the same technology to meet different requirements across their 5G networks, fostering the design of more efficient 5G networks.

Cloud-focused automation unites multi-cloud resources in a centralized Service Management and Orchestration system and then uses intent-based placement for optimization. With cloud-specific-automation, which continuously synchronizes with registered clouds, CSPs obtain context-aware information about their diverse set of sites, the state of these sites, the applications running there, the embedded technologies available to foster service delivery, and the cloud resources available for allocation.

With this information, the orchestrator can dynamically place network services and functions in a way that aligns requirements with cloud resources and capabilities. In this way, cloud-specific automation plays a central role in a SMO layer to simplify the deployment and management of 5G network functions.

Domain management functions support legacy and proprietary interfaces to domain-level network elements, legacy RAN components, transport networks, edge nodes, and the core. For example, there can be a manager for each domain: a RAN manager, an edge manager, a transport manager, and a core manager.

The next sections describe how VMware Telco Cloud Automation, VMware RAN Intelligent Controller (VMware RIC), and VMware Telco Cloud Service Assurance deliver a solid foundation of flexible components for the SMO layer.

How VMware Supplies SMO Capabilities for O-RAN

For an open RAN, VMware supplies SMO components for domain orchestration, infrastructure management, and service assurance as well as a non-RT RIC for network programmability and optimization. The SMO framework from VMware strives to support multiple RAN vendors, applications, and clouds:

- **Multi-vendor radio access networks:** Any vendor's O-RAN-compliant network functions can be onboarded and managed through their life-cycle by VMware components using standard interfaces.
- **Multi-vendor applications:** rApps from other vendors and developers can be onboarded and deployed in the non-RT RIC from VMware by using a standardized set of APIs. A software-development kit (SDK) for rApps helps vendors get their RAN applications up and running on the non-RT RIC from VMware.
- **Multi-cloud deployments:** VMware components support deployments on private, hybrid, and public clouds. The near-RT RIC from VMware, for example, can run on a public cloud.

The SMO framework from VMware is designed to manage resources and network functions that are deployed on various cloud environments, including not only the VMware cloud but also AWS and Google Cloud. The SMO framework from VMware connects with other services, such as NWDAF services, that go beyond the RAN domain by using O-RAN's external enrichment interface. A high-speed message bus interconnects the principal SMO components.

Flexible SMO Components

VMware has flexible solutions for the SMO components defined by the O-RAN alliance. Figure 4 maps VMware solutions to the O-RAN architecture. The three VMware products that play a role in the SMO layer defined by the O-RAN Alliance are as follows:

- VMware Telco Cloud Automation
- VMware Centralized RIC
- VMware Telco Cloud Service Assurance

VMware Telco Cloud Automation and VMware RIC can interact with a fourth product, VMware Telco Cloud Platform RAN, which supplies infrastructure and resources for the RAN, especially the O-Cloud defined by the O-RAN Alliance.

VMware Telco Cloud Automation

In the O-RAN architecture, VMware Telco Cloud Platform RAN and VMware Telco Cloud Automation supply aspects of the cloud computing platform (O-Cloud) and the SMO layer as well as the ability to connect these components with other components, clouds, and network functions, including the CU, the DU, the non-RT RIC, and the near-RT RIC.

VMware Telco Cloud Automation manages and orchestrates resources, network functions, and rApps. In the SMO layer, the automation component from VMware performs life-cycle management for containers as a service, containerized network functions (CNFs), virtual network functions (VNFs), and rApps. VMware Telco Cloud Automation can integrate with FCAPS systems from VMware partners to support a multi-vendor RAN.

VMWARE RIC AT A GLANCE

VMware RIC™ is a multi-RAN, multi-cloud platform that simplifies the operations of the underlying RAN infrastructure through programmability and intelligence. The platform can host both near-real-time applications (xApps) and non-real-time applications (rApps). These apps introduce new use cases — automation, optimization, and service customization — that fuel innovation across a telco network.

KEY BENEFITS

- Multi-vendor interoperability establishes a vendor- and technology-agnostic platform for existing and new RAN vendors.
- RAN programmability fosters flexibility and agility to dynamically support new applications and services.
- Network-wide observability and automated optimization from AI/ML algorithms improve efficiency.
- Applications from an ecosystem of partners optimize the RAN, reduce energy consumption, and improve spectrum utilization.

RAN PROGRAMMABILITY



Demo Video: Activating Network Programmability with VMware RIC

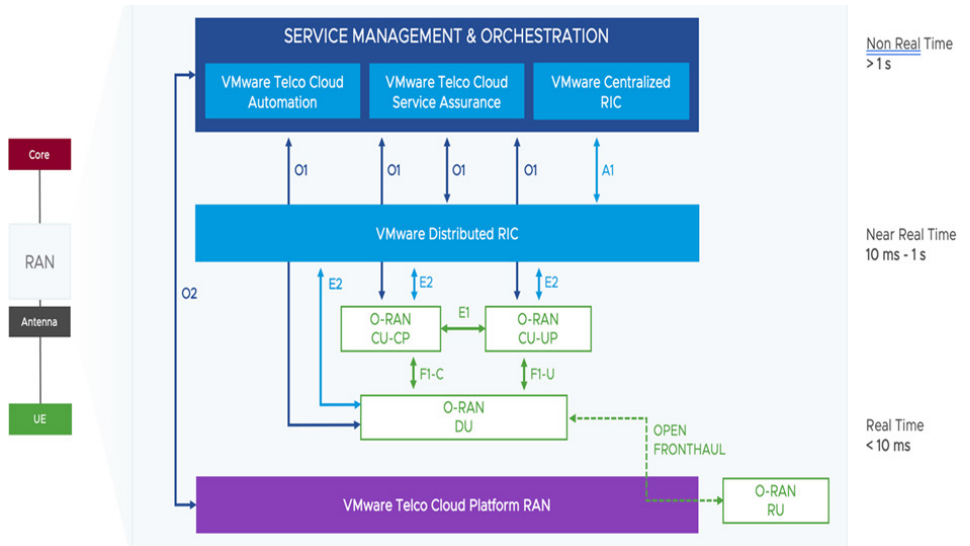


Figure 4: The VMware products as components of the O-RAN architecture.

VMware Telco Cloud Automation performs the following SMO functions:

- End-to-end automation for IaaS, containers as a service (CaaS), network functions, network services, and slice management
- Supplies containers as a service with a carrier-grade Kubernetes distribution that is extended to meet RAN acceleration and networking requirements
- Manages cloud infrastructure
- Performs lifecycle management of Kubernetes clusters, RAN functions, and 5G services at scale
- Optimizes the placement of DUs and CUs by allocating resources dynamically
- Optimizes Kubernetes clusters and the underlying infrastructure to match a network function’s requirements by *allocating resources dynamically*, an automated process also known as *late binding*

VMware Centralized RIC

VMware Centralized RIC is an implementation of the non-real-time RIC in the O-RAN Alliance reference architecture. VMware Centralized RIC supports policy-based guidance, data analytics, AI/ML model management, and enrichment information for underlying RAN elements.

VMware Centralized RIC uses the southbound O1 and A1 interfaces to manage the RAN data plane (that is, the RAN baseband software that includes the CU-CP, CU-UP, and DU) and the RAN control plane (Near-RT RIC) respectively. It exposes open northbound APIs for RAN management-plane applications from various vendors.

VMware Centralized RIC supports traditional RAN, virtualized RAN, and O-RAN environments. By working with both traditional RAN and virtualized RAN environments, VMware Centralized RIC runs rApps without requiring significant changes to an existing RAN architecture.

VMware Centralized RIC includes a software development kit with resources, tools, and services that speed up rApp development, improve application portability, and bolster

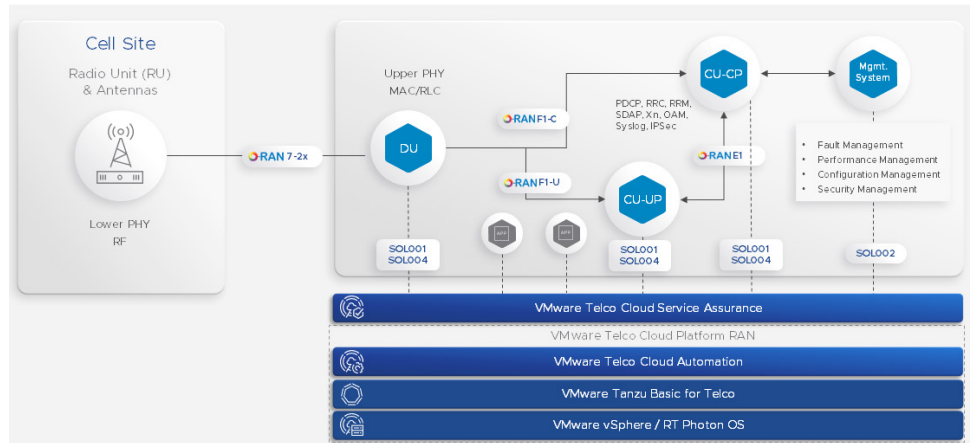


Figure 5: The O-RAN logical architecture and interfaces with VMware Telco Cloud Platform RAN running the CU, DU, and other RAN components from a hypothetical vendor. VMware Telco Cloud Automation performs many of the SMO functions. It also onboards and manages systems from third-party vendors that can provide additional SMO functionality, such as FCAPS.

security. The SDK contains libraries and data structure definitions that abstract user applications from the complexities of networking and communicating with the RIC, the E2 nodes, and other apps.

The following table lists the key services of VMware Centralized RIC.

SERVICE	DESCRIPTION
R1 exposure services	Support communication between rApps and VMware Centralized RIC.
O1-related services	Support APIs to read performance management counters and read or write configuration management parameters.
FCAPS services	Collect performance and health metrics from RIC services and rApps.
rApp lifecycle management services	Support lifecycle management of rApps.
A1-related services	Interfaces with the near-RT RIC.

VMware Telco Cloud Service Assurance

VMware Telco Cloud Service Assurance supports RAN observability and assurance by monitoring the following O-RAN resources and functions from a centralized location in the SMO layer:

- Physical equipment like servers, transport mechanisms, and radio units
- Virtual machines, containers, and service layers
- CUs and DUs

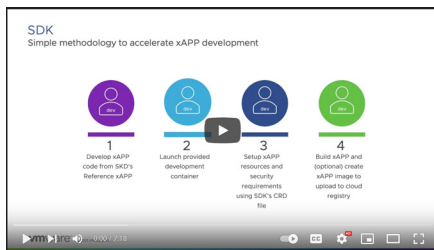
VMware Telco Cloud Service Assurance uses machine learning to find and fix network and service issues. After a root cause is identified, the system can trigger a series of actions, from identifying business impacts to initiating a closed-loop remediation workflow.

VMWARE RIC SDKS

VMware RIC includes software development kits with resources, tools, and services that speed up xApp and rApp development, improve application portability, and bolster security. T

The SDKs for VMware Distributed RIC and VMware Centralized RIC contain a set of libraries and data structure definitions that abstract user applications from the complexities of networking and communicating with VMware RIC, the E2 nodes, and other apps.

VIDEO DEMO



Demo video: [Accelerating app development by using the VMware RIC SDK](#)

RIC SDK PARTNER PROGRAM

VMware RIC SDK Partner Program gives developers access to the VMware Centralized RIC SDK and the VMware Distributed RIC SDK, both of which include sample code that helps jump-start app development. VMware RIC runs on various types of cloud infrastructure, giving app developers the confidence that developing their applications for VMware RIC will have broad industry appeal and interest. For more information, see the [RIC SDK Partner Program](#).

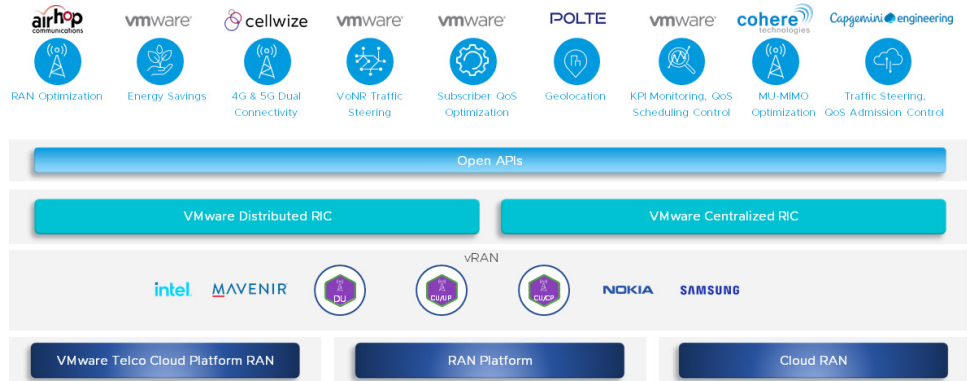


Figure 6: Solutions from a vibrant ecosystem of partners put open RAN use cases into action so you can optimize and monetize 5G.

Extending the SMO to Manage Domains Beyond the RAN

With 5G, telecommunications providers are shifting from using traditional, proprietary hardware stacks running custom software to embrace hybrid clouds that include not only virtualized compute but also the public clouds of hyperscalers.

As part of this shift, cloud-native technology lays the foundation for a multi-cloud strategy. The fundamental concepts driving a cloud-native approach include such things as loose coupling, microservices, low overhead, and immutable infrastructure as well as a declarative consumption model and APIs across layers. Critically, cloud-native systems are designed for portability and automation.

In extending the concept of SMO beyond the RAN, automation is axiomatic. With automation, you can optimize the use of computing resources to improve agility, adaptability, and innovation. Here are some of the benefits of cloud-native principles for telecommunications platforms and networks:

- Consolidate servers and reduce costs through efficient resource utilization.
- Speed up application deployment.
- Streamline software development processes by fostering DevOps, site reliability engineering (SRE), and continuous integration and delivery (CI/CD).
- Decouple applications from machines for portability, flexibility, and interoperability.
- Easily modify, update, extend, or redeploy applications without affecting other workloads.
- Improve resilience through automation.
- Dynamically scale infrastructure and applications to meet changes in demand.
- Improve flexibility and agility for your organization and business.

As such, cloud-native technology is a driving force in being able to extend the SMO layer from the RAN to the rest of a telecommunications network, resulting in centralized yet flexible orchestration and management across hybrid and public clouds.

Multi-Cloud Automation and Orchestration

By solving the problems that undermine the architecture of existing telecommunications networks—monolithic stacks marred by complexity, silos, and vendor lock-in—VMware Telco Cloud Automation extends management and orchestration beyond the RAN to include multiple clouds.

With VMware Telco Cloud Automation, all the layers — from infrastructure to domain orchestration (NFVO) — are coupled for consistency and optimized for deployment and

VMWARE TELCO CLOUD AUTOMATION AT A GLANCE

VMware Telco Cloud Automation™ accelerates time to market for network functions and services while igniting operational agility through unified automation across clouds — making it the quintessential component of cross-domain SMO.

KEY BENEFITS AND CAPABILITIES

- Integrate 5G network capabilities alongside existing NFV architectures and manage them from a centralized, cross-domain SMO layer
- Enhance the service experience through workload mobility, dynamic scalability, closed-loop healing, and improved resilience
- Improve agility with Kubernetes, cloud-native patterns, and CaaS automation
- Innovate faster and reduce complexity with validated solutions from various vendors in the VMware Ready for Telco Cloud program
- Onboard network functions using standards-based templates and model network services based on multi-vendor network functions
- Centralize the creation, optimization, and management of Kubernetes clusters with CaaS automation
- Improve service quality and issue resolution by integrating with the AI-driven workflows of VMware Telco Cloud Service Assurance

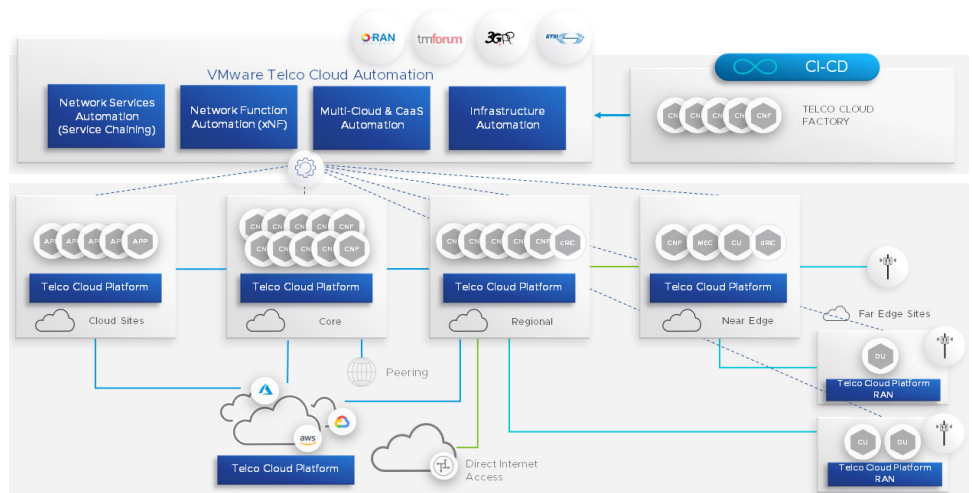


Figure 7: The key capabilities of VMware Telco Cloud Automation—including cloud-native technologies and automation—deliver flexible solutions for 5G. Access to CNFs, VNFs, and applications from multiple vendors supply extensible building blocks to deploy new services and explore emerging use cases.

workload management across multiple clouds. VMware Telco Cloud Automation is a foundational element of VMware Telco Cloud Platform.

VMware Telco Cloud Automation includes capabilities for resource optimization, multi-cloud operational consistency, and multi-layer automation. Amid the monumental shift that is taking place with 5G rollouts, the following capabilities empower you to embrace a multi-cloud strategy from a centralized SMO layer:

Resource Optimization

With the cloud-native architecture of VMware Telco Cloud Automation, you can deploy, orchestrate, and optimize cloud resources and CNFs with intent-based placement and dynamic resource allocation.

In addition, network resiliency, cross-cloud application continuity, and multi-tenant service isolation help address business requirements and compliance regulations, such as high availability and SLAs.

Multi-Cloud Operational Consistency

Unified management is key to being able to manage complex networks and multiple domains with consistency. With VMware Telco Cloud Automation, you can manage both VNFs and CNFs from a centralized location that, in effect, becomes a multi-cloud SMO.

Carrier-grade Kubernetes supplies another piece of the puzzle so you can capitalize on a microservices architecture. You can use microservices with a resource-optimized Kubernetes runtime for device attachment, NUMA alignment, resource reservation, and placement. This architecture delivers the capability to roll out 5G networks with Multus, DPDK modules, an SR-IOV plugin, CPU/Topology Manager, and Kubernetes cluster automation tailored for telco use cases.

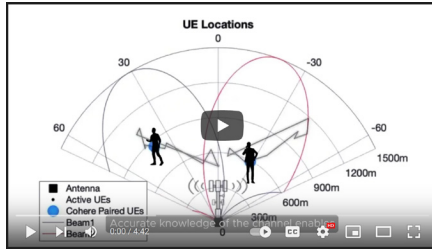
Multi-Layer Automation

With VMware Telco Cloud Automation, you can also automate the onboarding and upgrading of network functions and infrastructure components with zero-touch provisioning.

Full lifecycle management can define and apply policies using a decision-making engine to automate deployments, operations, and maintenance. Standards-driven modular components can integrate with a multi-vendor MANO architecture.

MULTI-VENDOR APPS ON VMWARE RIC

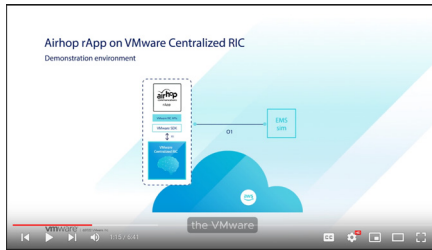
Here are videos that show multi-vendor applications running on VMware RIC.



Activating Sustainable Broadband with VMware RIC and Cohere Technologies



Democratizing 5G Device Location with VMware and Polte



Mitigating PCI Collisions with the AirHop rApp on VMware RIC



Transforming any RAN into a Multi-Services Hub with VMware and Cellwize

Multi-Vendor Applications from the Edge to the Core

By extending the SMO layer beyond the RAN to manage and orchestrate applications running on different clouds and in different domains, VMware technology gives you the flexibility to deploy and manage the applications best suited to pursue your 5G vision in not only the RAN but also the core and at the edge.

Managing Multi-Vendor Applications

VMware Telco Cloud Automation lets you manage applications and network functions from multiple vendors from a centralized location in an expanded SMO layer. Here are some of the ways in which VMware Telco Cloud Automation supports applications and network functions from various vendors.

Orchestration and Workload Placement with Scale-out Capability

The use of orchestration to manage network functions is closely related to lifecycle management. With VMware Telco Cloud Automation, multi-vendor network functions can be instantiated, terminated, scaled out, scaled in, upgraded, and healed, all of which is critical to take full advantage of cloud-native architectures. When network functions are fully orchestrated, you can also scale them out on demand.

Support for Kubernetes Lifecycle Functions

For any CNF, the most critical lifecycle functions are instantiation and termination, which are required for functional testing. In addition to supporting the instantiation and termination of network functions, VMware Telco Cloud Automation supports various lifecycle functions and NFVO workflows, including instantiate, terminate, configure, scale, heal, update, and upgrade. Lifecycle functions can be extended with workflows and integrated with a CI/CD pipeline. Custom workflows can also be run.

Separation of Concerns

Another concern is separation of the platform from the network functions. The platform on which you run network functions should be separate from the network functions themselves.

VMware Telco Cloud Automation orchestrates network functions and sets up the Kubernetes environment, which lets you separate orchestration and management from network functions. When a single orchestrator manages all the different vendor network functions in a network, it dramatically simplifies operational requirements.

Traditionally, the lifecycle functions for a network function were managed by the EMS of that network function's vendor. This approach, however, becomes cumbersome in a multi-vendor environment. For this reason, it is imperative that 5G vendor network functions can use third-party orchestration as opposed to being orchestrated by their own EMS.

Capabilities for creating a CSAR file

VMware Telco Cloud Automation offers a designer for the creation of Cloud Service Archive (CSAR) packages, which can be done as part of the VMware Ready for Telco Cloud validation process.

VMware works with vendors to test their CSAR package file to help ensure that it is appropriate for the type of deployment they want to create.

VMware Telco Cloud Automation also supports legacy CLI-based network functions, network functions requiring custom scripts, and network functions using a REST API to fetch data. If a network function uses a hard-coded artifact, the VMware process ensures that they are removed from the CSAR and replaced with reference variables. In addition, VMware Telco Cloud Automation also supports running pre- and post-custom scripts during LCM operations.

VMWARE TELCO CLOUD SERVICE ASSURANCE AT A GLANCE

VMware Telco Cloud Service Assurance™ is a multi-vendor, multi-cloud solution that monitors, analyzes, and pro-actively manages multi-vendor physical and virtual environments in a single platform.

KEY CAPABILITIES AND BENEFITS

- Simplify NOC and SOC operations with a centralized, cross-domain view.
- Gain rapid insights with integrated fault and performance management, service management, root cause analysis, and impact assessment.
- Reduce costs and complexity through automation and optimization for assurance across layers and domains.
- Use closed-loop automation and rapid remediation to reduce OpEx and optimize resources and workloads to meet surges in demand.
- Use AI-based analytics to increase operational efficiency with rapid problem isolation, automatic suppression of extraneous alarms, and automated rule updates.

Service Assurance for Networks and Systems

The cloud-native architecture of VMware Telco Cloud Service Assurance lets you monitor and manage 5G physical and virtual components from the mobile core to the RAN and the edge. From a centralized location, you get integrated operational intelligence on 5G infrastructure and components across multi-vendor domains, including physical, virtualized and containerized environments.

Network operations centers (NOCs) and service operations centers (SOCs) can manage many networks as one to rapidly resolve network performance issues. Automatic association of issues with customers enables you to remediate issues by priority and deliver a consistent level of service quality. The result reduces costs, improves operational efficiency, and boosts customer satisfaction.

Integration with Other SMO Components

VMware Telco Cloud Service Assurance (network monitoring and assurance product) integrated with VMware Telco Cloud Automation™ (network automation and orchestration product) provide the most powerful closed-loop automation and remediation in the industry. VMware Telco Cloud Service Assurance works with the underlying infrastructure and management layers such as VMware Tanzu® (container and Kubernetes automation and management product), VMware Cloud Director™ and VMware Integrated OpenStack (5G RAN and core network function deployment), and VMware Telco Cloud Infrastructure™ (virtualization and VIM layer).

Automated Discovery and Topology Mapping

Network functions are now a mix of physical, virtual and containers, making it difficult to understand interrelationships, how one function impacts others and how they relate to a 5G service or tenant. Each network slice, for example, could utilize completely different resources. To overcome this complexity, VMware Telco Cloud Service Assurance automatically discovers on-premises and cloud network resources in real time by using standard APIs.

It then provides an end-to-end topology map in a single view that shows the physical and logical connectivity and relationships between the underlying network infrastructure and the software components that compose the 5G service, including networking, hardware, virtualization, containers as a service, and application layers for multiple vendors and domains. More than 4,000 physical and virtual devices are supported.

Fault and Performance Management

Using artificial intelligence and machine learning, VMware Telco Cloud Service Assurance automatically establishes dynamic performance baselines and calculates real-time performance metrics. It identifies anomalies or performance degradation and alerts operators when anomalous behavior is detected. Operational efficiency is increased with automatic suppression of thousands of extraneous alarms and elimination of costly manual upkeep of static rules. Resources and workloads are optimized dynamically to meet changes in edge and service requirements.

Automated Root Cause and Service Impact Analysis

The platform's root cause and service impact analysis capabilities resolve problems quickly by automatically correlating symptoms from the layers of the infrastructure stack (physical, virtual, Kubernetes, CNFs, VNFs, and services) and pinpointing the problem's root cause.

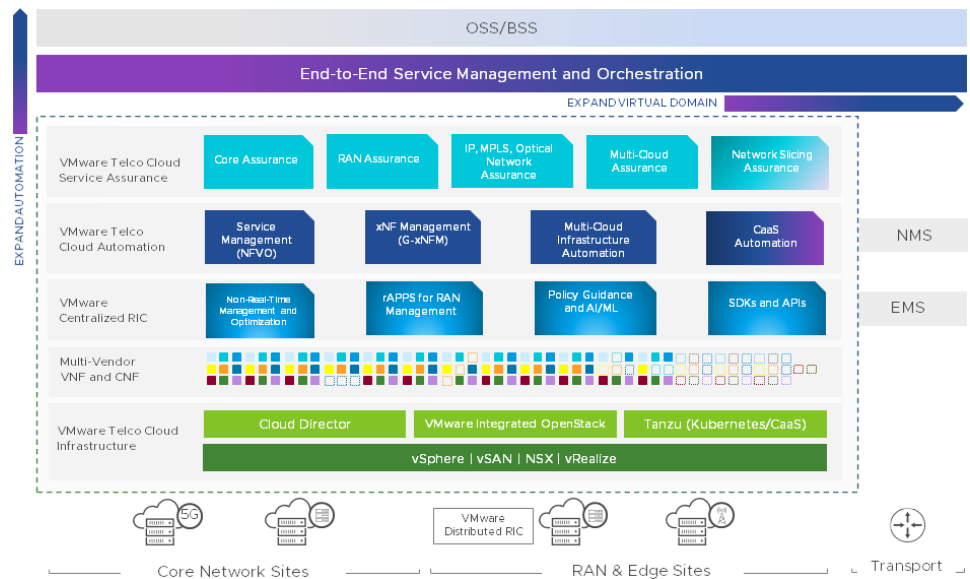


Figure 8: This diagram illustrates how an SMO layer that combines open interfaces and cloud-native technology with a modular and extensible component-based architecture can be expanded to support multiple vendors, applications, and clouds across not only the radio access network but also the core and edge domains.

Conclusion: Toward a Multi-Vendor, Multi-Cloud, Multi-Domain SMO

The open RAN architecture of the O-RAN Alliance charts a course for service management and orchestration. According to the O-RAN Alliance, the SMO layer handles RAN domain management. A disaggregated and standardized open radio access network can support multiple vendors and clouds with the help of an SMO layer that automates and optimizes the RAN and its applications.

Engineers from VMware are actively participating in the O-RAN Alliance’s ongoing work to disaggregate and standardize the SMO layer.

But what if the O-RAN Alliance’s vision of SMO can be extended beyond the RAN to govern the other key domains of service providers’ networks, such as the core and edge domains?

This white paper illustrated how an SMO layer that combines open interfaces and cloud-native technology with a modular and extensible component-based architecture can support multiple vendors, applications, and clouds across not only the radio access network but also the core and edge domains.

Resources and References

O-RAN Alliance *specifications* and *resources*:

- O-RAN.WG1.O-RAN-Architecture-Description-v04.00. See <https://www.o-ran.org/specifications>.
- O-RAN white paper: *O-RAN Use Cases and Deployment Scenarios: Towards Open and Smart RAN*, February 2020.

RAN Programmability: Tapping RIC Use Cases to Monetize 5G Services 12 RAN Intelligent Controller Use Cases to Optimize Radio Access Networks and Boost Telco Revenue, by VMware

Ignite Your 5G Deployments with the VMware Telco Cloud Operate and Monetize 5G

LEARN MORE

For more information about the SMO components from VMware, call 1-877-VMWARE (outside North America, dial +1-650-427-5000) or visit <https://telco.vmware.com/>

Multi-Cloud Networks with Agility, Automation, and Assurance, by VMware

Simplifying CNF Onboarding with Late Binding in VMware Telco Cloud Platform

Late Binding in VMware Telco Cloud Automation

Edge of Opportunity: Identifying Use Cases Driving Market Demand 10 Edge Computing Use Cases to Generate Revenue, Gain Efficiency and Improve Customer Experiences, by VMware

VMware RIC Datasheet

Evaluating Cloud-Native Platform Capabilities To Run Multi-Vendor CNFs: Assessing the Readiness of Telco Platforms for Automating Containerized Network Functions, by VMware

Security for Open RAN Architectures in 5G Telco Clouds: Protecting Open Radio Access Networks with Automation and Zero-Trust Architecture, by VMware

Intrinsic Security for Telco Clouds at the Dawn of 5G: An Integrated Approach to Helping CSPs Meet Emerging Security Standards, by VMware

Modernize to Monetize: Reimagine the Telco Cloud to Capitalize on 5G: Efficiently design, deploy, operate, and protect 5G networks with a common horizontal platform, by VMware

