

Technical Product Description

Virtual Service-Aware Policy Controller 1

TECHNICAL PRODUCT DESCRIPTION

Copyright

© Ericsson España, S.A. 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

VMware, vCloud Director, vSphere, vCenter, ESXi

are registered trademark of VMware Inc.

OpenStack

is a registered trademark of OpenStack Foundation

Dell

is a registered trademark of Dell Inc.

HPE Helion

is a registered trademark that belongs to Hewlett-Packard Enterprise Development Company, L.P.

Vyatta

is a registered trademarks of Brocade Communications Systems, Inc.

Abstract

The Technical Product Description describes the architecture, functions, configurations, interfaces, operation, and maintenance of the Ericsson Virtual Service-Aware Policy Controller (Virtual SAPC) 1.

The Virtual SAPC is the Telco Cloud ready version of the Ericsson SAPC. The Virtual SAPC is an already proven component in the Ericsson Virtual Evolved Packet Core (Virtual EPC) solution.



Contents

1	Introduction	1
1.1	Document Purpose and Scope	1
1.2	Revision Information	1
2	NFV Environment	3
2.1	NFVI	3
2.2	NFV Management and Orchestration System	4
2.3	VNF Manager	5
3	Virtual SAPC Architecture	7
3.1	Virtualization Architecture	7
3.2	Deployment Types	8
3.3	Resilience and Redundancy	8
3.4	Networking	10
3.5	Storage	11
3.6	Security	11
4	Management and Orchestration	13
4.1	Deployment	13
4.2	HW Management	13
4.3	Scaling	13
4.4	Decommissioning	14
4.5	VMware Tools	14
5	Characteristics and Dimensioning	17
6	Requirements on the Cloud System	19
6.1	Cloud Management System Requirements	19
6.2	Cloud Infrastructure Requirements	19
6.3	Compute Host HW Requirement	20
6.4	Additional considerations	20
	Glossary	21
	Reference List	23





1 Introduction

1.1 Document Purpose and Scope

The Technical Product Description document aims to provide a technical and functional description of the Ericsson Virtual Service-Aware Policy Controller (Virtual SAPC) 1. The Virtual SAPC provides the same functions as the physical SAPC, but architected for being deployed as a Virtualized Network Function (VNF) on a Network Function Virtualization Infrastructure (NFVI) .

This document includes description of the following areas:

- The cloud environment, surrounding the Virtual SAPC.
- The Virtual SAPC architecture.
- The Virtual SAPC management and orchestration.
- Characteristics and dimensioning.
- Requirements on the cloud system the Virtual SAPC imposes.

This document does not provide a description on the common functions shared by the SAPC and the Virtual SAPC. For such information, see Reference [1].

1.2 Revision Information

A	This is the first release of this document.
---	---





2 NFV Environment

The Virtual SAPC virtualization architecture allows the deployment of the Virtual SAPC in a NFV system. Therefore the Virtual SAPC becomes a VNF, which requires virtual resources (vCPU, memory, vNICs, storage) to a cloud infrastructure. The setup of the needed virtual resources is then managed through a Cloud Orchestration System and a NFVI. The NFVI is the responsible of assigning the virtual resources (vCPU, memory, etc.) the Virtual SAPC requires for its operation

This section describes supported NFV environments for Virtual SAPC deployment.

2.1 NFVI

2.1.1 Ericsson Cloud Execution Environment (CEE)

The Virtual SAPC can be deployed on Ericsson CEE. Ericsson CEE provides a carrier grade NFVI cloud infrastructure and a Virtualized Infrastructure Manager (VIM). The CEE is based on OpenStack components and the Kernel-based Virtual Machine (KVM) hypervisor. The CEE supports Ericsson or third-party Commercial Off-The-Self (COTS) HW for compute, storage, and networking.

For further information, see Reference [7].

2.1.2 VMware

The Virtual SAPC SW is delivered for being deployed on VMware vSphere 5.5, 6.0 or 6.5 NFVI. The VMware components required to deploy the Virtual SAPC are vCenter or vCloud Director.

2.1.3 Third-Party OpenStack based NFVI

System integration with a third-party NFVI cloud infrastructure based on OpenStack is possible. The Virtual SAPC has no explicit direct interface toward the cloud infrastructure. However, the Virtual SAPC has dependencies to the following:

- The Virtual Machine (VM) environment exposed by the hypervisor (KVM).
- The infrastructure networking solution.
- The performance, characteristics, and robustness of the infrastructure.

The Virtual SAPC has been already verified with the OpenStack based HPE Helion.

For requirements on the cloud infrastructure, see Section Section 6.2 on page 19.

2.2 NFV Management and Orchestration System

2.2.1 Ericsson Cloud Manager (ECM)

ECM provides management and orchestration of virtual resources across multiple VIMs, and G-VNFM functionality for generic life cycle management of VNFs. ECM supports VNF descriptors in Open Virtualization Format (OVF) and Heat Orchestration Template (HOT).

Because of the Virtual SAPC supports OVF and HOT, ECM can be used for its management and orchestration.

For further information on ECM, see Reference [8].

2.2.2 Atlas

Atlas is a set of management tools included in CEE, that can be used as a simplified alternative to ECM. It is based on the OpenStack components Horizon dashboard and Heat orchestration.

Atlas supports VNF packages in OVF and HOT formats.

Because of the Virtual SAPC supports HOT, Atlas can be used for its management and orchestration.

For further information on Atlas, see Reference [7].

2.2.3 Third-Party Cloud Management System

System integration with a third-party cloud management system is possible.

The Virtual SAPC has no direct interface toward the cloud management system. However, the Virtual SAPC has dependencies to the following:

- The VM image and the VNF Descriptor supported by the cloud management system. For instance, the provided OVF package may be translated, if needed, to a different one (e.g. TOSCA).
- Procedures for lifecycle management: The Virtual SAPC is pre-integrated with Ericsson OSS-RC and Ericsson Network Manager (ENM). A third-party VNF Manager (VNFM) would require system integration.
- The policy requirements for the Virtual SAPC deployment: For instance, the Virtual SAPC requires anti-affinity rules (see Section 3.3.2 on page 9).

For requirements on the cloud management system, see Section 6.1 on page 19.



2.3 VNF Manager

The Virtual SAPC has the same northbound interfaces as the physical SAPC. Therefore Either OSS-RC or ENM may be used as the Element Manager (EM) for both the physical and the Virtual SAPC.

OSS-RC and ENM also provide S-VNFM functionality for specific life cycle management of Ericsson VNFs, including the Virtual SAPC.





3 Virtual SAPC Architecture

3.1 Virtualization Architecture

The Virtual SAPC virtualization architecture consists of several VMs taking different function roles.

- System Controllers (SC) VMs: 2 VMs implementing system controllers function. These VMs provide the north-bound access to the Virtual SAPC and the cluster membership and control.
- Traffic Processors (TP) VMs: “n” (at least 2, maximum 34) VMs for providing the Policy Server implementation. This VMs are also referred as Payload (PL) VMs.

Note: The maximum of 34 TP VMs limit is a testing limit in the Virtual SAPC 1 release.

Both the 2 SC VMs and the TP VMs configure the Virtual SAPC cluster. However, the SW delivery includes an additional type of VM:

- Virtual Router (VR): 4 VMs providing the Virtual Routing Service (based on Vyatta VR). These VMs are optional and may be removed by System Integration. 2 of the VR VM are responsible for Operation and Maintenance (OAM) tasks, and the other 2 for addressing the control plane traffic the Virtual SAPC manages.

Note: If the VR VMs are removed by System Integration, the Virtual SAPC routing must be provided by physical Open Shortest Path First (OSPF) routers.

Figure 1 displays the described the Virtual SAPC virtualization architecture.

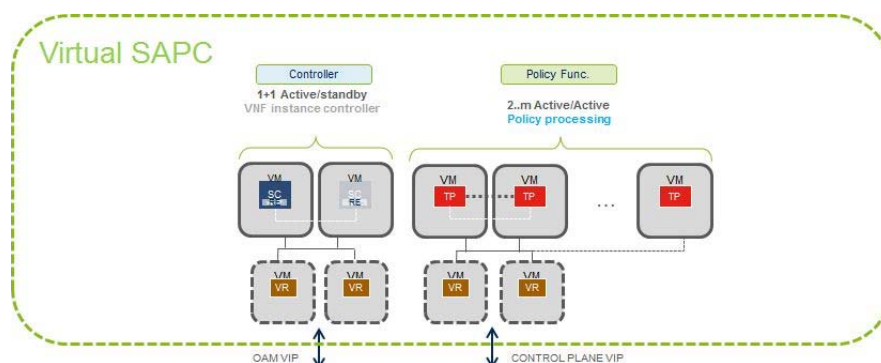


Figure 1 The Virtual SAPC virtualization architecture



3.2 Deployment Types

The Virtual SAPC provides validated deployment types. The validated deployment types specify VM sizes, number of VMs, and distribution of VMs over the available compute hosts of the Virtual SAPC.

- Multi-host Virtual SAPC: This deployment targets scalability and high capacity, with full SW and HW redundancy.
- Single-host Virtual SAPC This deployment targets small footprint with limited capacity. The deployment has small VM sizes, all collocated on one compute host . It supports full SW redundancy including VM redundancy. The deployment does not support HW redundancy. However, network level redundancy can be achieved through a pair of the Virtual SAPC instances configured as 1+1 IP Geographical Redundant.

Note: The VM sizes and numbers in Table 1 and Table 2 have been validated. However, other VM sizes and numbers can be used, depending on the dimensioning needs.

Table 1 The Virtual SAPC minimum size configuration

VM Role	Number of VMs	vCPU	RAM Memory (MB)	Hard Disk (GB)
SC	2	2	6144	40
TP	2-34	2	7168	0
VR	4	2	1024	4

Table 2 The Virtual SAPC normal-size configuration

VM Role	Number of VMs	vCPU	RAM Memory (MB)	Hard Disk (GB)
SC	2	4	6144	60
TP	2-34	16	20480	0
VR	4	2	1024	4

The Virtual SAPC is also part of Ericsson Virtual EPC offerings. Virtual EPC deployments are not described in this document.

3.3 Resilience and Redundancy

All the Virtual SAPC software components are supervised by the Virtual SAPC middleware. Recovery actions for SW components are triggered by the Virtual SAPC middleware when needed. Supervision and redundancy handling does not depend on specific HW failure notifications from the virtualization and infrastructure layers. This means that mechanisms such as session resilience work the same way as they do in the SAPC Physical Node Function (PNF).



3.3.1 VM Redundancy

The VM redundancy models are as follows:

Table 3 VM redundancy models

VM Role	Redundancy Model
SC	1+1 active-standby
TP	1+1 active-active
VR OAM	1+1 active standby
VR Traffic	1+1 active standby

3.3.2 Anti-affinity rules

High availability implementation requires the definition of anti-affinity rules. These rules must be considered for any Multi-host Virtual SAPC deployment (as it was defined in Section 3.2 on page 7).

- The 2 SC must not be collocated in the same physical host.
- Each TP must be collocated in a different physical host.
- The 2 VR for OAM must not be collocated in the same physical host.
- The 2 VR for Traffic must not be collocated in the same physical host.

In case the anti-affinity rules are not implemented, the consequences are the following:

- The Virtual SAPC reboots in case of physical host failure: This happens if either the 2 SC are down for more than 15 minutes, or at least 2 TP VM are collocated in the failing physical host.
- Lack of external connectivity towards the Virtual SAPC: It is the result of having either the 2 VR for OAM or the 2 VR for Traffic are in the failing physical host.

3.3.3 Physical Link Redundancy

The Virtual SAPC is not aware of the cloud network topology. Therefore, it does not perform failover between two virtual NICs (vNICs) on the same VM. It is the responsibility of the cloud infrastructure to provide physical link redundancy.

3.3.4 Storage Redundancy

The Virtual SAPC has redundant storage on the SC VMs.



3.3.5 IP Geographical Redundancy

The Virtual SAPC supports geographical redundancy by a two VNFs 1+1 active-standby implementation. The IP Geographical Redundancy solution is the same one in the SAPC PNF and in the Virtual SAPC.

Further information is available in Reference [1].

3.4 Networking

3.4.1 Internal networking

The detailed description of the Virtual SAPC internal networking is available in the SAPC Cloud Network Configuration Guide (Reference [6]).

3.4.2 External networking

The detailed description of the Virtual SAPC external networking is available in the SAPC Cloud Network Configuration Guide (Reference [6]).

3.4.3 Characteristics per Virtual Network

The following table specifies the purpose and characteristics of the different Virtual Networks (VN) used by the Virtual SAPC.

Table 4 Virtual Network Characteristics

	Internal VNs	External OAM VN	External Traffic VNs
Purpose of VNs	The Virtual SAPC VM-to-VM	OAM	The Virtual SAPC external traffic
Possibility to share the VN with other VNF instances	No	No	No
Externally connected to networks outside the cloud	No	Yes	Yes
vNIC IP address assignment	SC VM will do IP address assignments using the internal DHCP	Configured through cloud injected file in the Virtual SAPC	Configured through cloud injected file in the Virtual SAPC



Supported IP versions	IPv4 and IPv6	IPv4 and IPv6	IPv4 and IPv6
IP MTU size	Manually configured Default: 1500 bytes	Manually configured Default: 1500 bytes	Manually configured Default: 1500 bytes
IP routing	Handled internally by the Virtual SAPC	Through VR OAM VM. If the VR are not in the system, physical OSPF routers are needed	Through VR Traffic VM. If the VR are not in the system, physical OSPF routers are needed
vNIC MAC address assignment	Value defined by the Virtual SAPC (no option to configure it)	Value defined by the Virtual SAPC (no option to configure it)	Value defined by the Virtual SAPC (no option to configure it)
Support for application VLAN tagging (trunk vNIC)	No	Not provided by default	Not provided by default

3.5 Storage

The Virtual SAPC storage is on the SC VM root disk, thus the VM disk image, which is used to boot the VM. The storage includes SW data, configuration data, backup information, log files and performance monitoring files.

The VR VMs also includes storage. The storage includes just the Vyatta VR SW image.

The TP VMs use only the local VM disk image for booting. They do not write to the local disk, but manage their data (both provisioning and dynamic) in memory.

The Virtual SAPC storage capacity can be modified at deployment time, but cannot be changed during operation. For information about storage requirements on the cloud infrastructure, see Section 6.2 on page 19.

The cloud infrastructure is responsible for implementing the storage back end, which is transparent to the Virtual SAPC.

3.6 Security

The Virtual SAPC is delivered with default hardening. For more information about hardening and security of the Virtual SAPC, see Reference [2].



The security of the Virtual SAPC strongly depends on the underlying security of the cloud infrastructure.



4 Management and Orchestration

The main OAM functions (Configuration Management, Data Provisioning, Fault Management, Performance Management, log management, backup & restore, troubleshooting and upgrade) are the same ones in the SAPC PNF and in the Virtual SAPC. However, there are some differences in other OAM functions. They are described in the following sections.

4.1 Deployment

There are two methods to deploy the Virtual SAPC.

- An OVF package is created using a tool (script) and the Virtual SAPC SW images from the delivered SW. The OVA package is then deployed in the cloud manager. Different OVA packages are provided for ECM or VMware vSphere/vCenter.
- OpenStack Orchestration (Heat): A HOT is created using a tool (script) and the Virtual SAPC SW images from the delivered SW. The Virtual SAPC SW images are uploaded to OpenStack (Glance), and the HOT is then applied in OpenStack.

When the cloud system boots the VMs, the Virtual SAPC automatically starts to run on the SW that is pre-installed on the SW images.

Configuration information can be injected into the VNF at deployment time by cloud injection.

Detailed information is available in Reference [3] and Reference [4].

4.2 HW Management

The Virtual SAPC is a NFV-ready SW, so it has no direct coupling to the physical HW it is deployed on. Therefore the Virtual SAPC cannot provide any status, alarms, or counters related to the physical HW. The cloud infrastructure needs to provide this information for the operator.

However, the VMs in the Virtual SAPC are considered as equipment. So the VMs can be monitored and can for example, be restarted, locked, and unlocked.

4.3 Scaling

The Virtual SAPC can be scaled-out or scaling-in dynamically due to application capacity needs. The scaling out consists of adding additional TP VMs to the Virtual SAPC. The scaling-in means to remove TP VMs from the Virtual SAPC. The



maximum and minimum sizes for scaling-out/in is indicated in Section 3.1 on page 7.

Note: SC VMs and VR VMs does not scale.

After scaling-out or scaling-in, the traffic is automatically rebalanced across all the TP VMs in seconds.

Scaling-up (increasing dynamically the VM size) and scaling-down (decreasing dynamically the VM size) is not supported.

4.4 Decommissioning

The Virtual SAPC can be easily decommissioned from operation in just seconds. This is done via VNF de-instantiation through the cloud management system.

4.5 VMware Tools

The Virtual SAPC includes Open VM Tools (OVT) in the guest OS. OVT is an open source implementation of VMware Tools. It consists of virtualization utilities that improve the functionality and management of VMs within a VMware environment.

Table 5 describes how the Virtual SAPC supports OVT.

Table 5 OVT Support in the Virtual SAPC

OVT Feature	Support in the Virtual SAPC
Synchronize the guest OS clock with the virtual infrastructure	Disabled. SAPC synchronizes the clock with an external NTP server
Enable the virtual infrastructure to perform graceful shutdown of the VM	Enabled
Enable the virtual infrastructure to quiesce the file system of the VM before taking a VM snapshot	Disabled
Provide a heartbeat from the guest to the virtual infrastructure to support vSphere High Availability	Enabled
Publish information about the guest OS to the virtual infrastructure, including resource use and networking information	Enabled
Provide a secure and authenticated mechanism to perform various operations within the guest OS from the virtual infrastructure	Disabled. The Virtual SAPC OAM interfaces provide accountability logging and enforcement of role-based access rights on VNF level, and must therefore be used



Customize the guest OS when deploying a new VM	Disabled
Improve the interaction with the guest desktop environment	Disabled. The Virtual SAPC does not provide a desktop environment





5 Characteristics and Dimensioning

Ericsson has a set of tools for capacity planning, including dimensioning guidelines and a dimensioning calculation tool. The tools are available for Ericsson personnel who can assist the customer with capacity planning scenarios. Inputs for the dimensioning are cloud system and HW characteristics, control plane and user plane traffic models, and the used the Virtual SAPC feature set.

The dimensioning calculation tool has reference models of the cloud system and hardware. Deviations from the reference model and the cloud system requirements can have an impact on the Virtual SAPC characteristics and lead to degraded performance. The requirements are described in Section 6 on page 19. Each deviation compared to the stated requirements can require more HW resources than the reference model indicates, or can require system integration work to fill any performance gaps.

For more information about characteristics and dimensioning, see Reference [5].





6 Requirements on the Cloud System

This section describes the requirements on the cloud system components.

Deviations from the requirements can have an impact on the Virtual SAPC characteristics and can risk both performance and robustness. Deviation from the requirements can require system integration to fill any design gaps.

6.1 Cloud Management System Requirements

The Virtual SAPC has the following requirements on the cloud management system:

- Support VM anti-affinity policies or a solution to control the VM placement on the physical compute hosts.
- Support pre-defining of the vNIC MAC address.
- Optionally support OpenStack configuration drive using ISO 9660 file system for injection of configuration data.
- Only cloud management system users with appropriate authority should have access to the Virtual SAPC and its virtual resources.

6.2 Cloud Infrastructure Requirements

6.2.1 Compute

- Cloud service model: IaaS.
- Deployment unit: VM.
- Hypervisors: KVM or VMware ESXi 5.5/6.0.
- The cloud infrastructure must not overcommit CPU, memory, or disk resources.

For optimal performance of the Virtual SAPC, the recommendation is to enable the hyper-threading.

6.2.2 Networking

- VM vNIC Ethernet adapter types: KVM: VirtIO; VMware ESXi: vmxnet3.
- Minimum number of vNICs per VM: 2 per VR VM; 4 per TP VM; 5 for SC1 VM and 4 for SC2 VM.
- Number of vNICs for the smallest the Virtual SAPC cluster configuration: 29.



- L2 virtual networks must be supported.
- The cloud infrastructure must provide physical Ethernet link redundancy for each vNIC.
- Recommended maximum link failover time in the cloud infrastructure: 0.5 seconds.

6.2.3 Storage

- VM virtual disk controller: KVM: VirtIO; VMware ESXi: IDE.
- If centralized storage is used, it must provide High Availability in all aspects including the SAN network.
- If local storage is used, see Section 6.3 on page 20 for detailed storage requirements.

6.3 Compute Host HW Requirement

This section specifies the compute host HW requirements for the Virtual SAPC.

- CPU architecture: x86_64.
- Minimum number of logical CPUs (hyper-threads) for VM use: 2.
- Minimum amount of RAM for VM use: 1 GB per VR VM, 6 GB per SC VM, 7 GB per TP VM.
- Minimum disk space for VM use: 4 GB per VR VM, 40 GB per SC VM, 0 GB per TP VM.
- Minimum NIC HW for VM use: 2 x 10GE.

One the Virtual SAPC instance must be deployed on compute hosts within the same site. All the compute hosts should be connected to the same switch, or at least with minimal number of network hops between the compute hosts.

6.4 Additional considerations

Being a control plane application, the Virtual SAPC is not a performance critical telecommunications application. Then it does not require Single Root Input/Output Virtualization (SR-IOV), Data Plane Development Kit (DPDK) or similar utilities.

The Virtual SAPC is not Non-Uniform Memory Access (NUMA) aware. Therefore it is not recommended to define VMs whose size may imply the VM is deployed in more than one NUMA cell.



Glossary

CEE
Cloud Execution Environment

COTS
Commercial Off-The-Self

DHCP
Dynamic Host Configuration Protocol

DPDK
Data Plane Development Kit

ECM
Ericsson Cloud Manager

EM
Element Manager

ENM
Ericsson Network Manager

EPC
Evolved Packet Core

G-VNFM
Generic VNFM

HOT
Heat Orchestration Template

HW
Hardware

IP
Internet Protocol

KVM
Kernel-based Virtual Machine

MAC
Media Access Control

MTU
Maximum Transmission Unit

NFV
Network Functions Virtualization

NFVI
NFV Infrastructure

NIC
Network Interface Card

NUMA
Non-Uniform Memory Access

OAM
Operation and Maintenance

OSPF
Open Shortest Path First

OSS
Operations Support Systems

OVA
Open Virtualization Alliance

OVF
Open Virtualization Format

OVT
Open VM Tools

PL
Payload

PNF
Physical Node Function

SC
System Controller

SR-IOV
Single Root Input/Output Virtualization

S-VNFM
Specific VNFM

SW
Software

TP
Traffic Processor



vCPU

Virtual Central Processing Unit

VIM

Virtualized Infrastructure Manager

Virtual SAPC

Ericsson Virtual Service-Aware Policy Controller

VLAN

Virtual Local Area Network

VM

Virtual Machine

VN

Virtual Networks

VNF

Virtualized Network Function

VNFM

VNF Manager

vNIC

Virtual Network Interface Card

VR

Virtual Router



Reference List

Ericsson Documents

- [1] Technical Product Description: Service-Aware Policy Controller 1, 1/221 02-FGC 101 3390/1
- [2] Security Management Guide, Service-Aware Policy Controller, 29/1553-CSH 109 215/7
- [3] SAPC VNF Deployment Instruction for CEE , 3/1531-CSH 109 215/7
- [4] SAPC VNF Deployment Instruction for VMware, 4/1531-CSH 109 215/7
- [5] SAPC 1 Network Impact Report, 109 48-FGC 101 3390/1
- [6] SAPC VNF Network Configuration Guide, 20/1553-CSH 109 215/7
- [7] CEE Technical Description, 221 02-FGC 101 3270 Uen
- [8] Product Overview. Ericsson Cloud Manager, 1/1550-CSH 109 232 Uen E