ZSM PoC Report

1 PoC Project Details

1.1 PoC Project Review

PoC Number:	2
PoC Project Name:	Automated network slice scaling in multi-site environments
PoC Project Host:	Telefónica S.A.
Short Description:	This PoC has the aim of demonstrating the capability to automatically scale out a deployed network instance across multiple administrative domains. This will be achieved using the 5G assets of 5G-VINNI, which is a large-scale, end-to-end facility composed of several interworking sites, each deployed at a different geographic location and defining a single administrative domain. The management and orchestration capabilities of individual sites, and the enablers allowing for the interworking across them, are aligned with ZSM architectural design principles. The PoC fits the End-to-End (E2E) service management scenario category detailed in ZSM 001, considering the network slicing features specified in ZSM 003. The management and orchestration assets for this PoC, based on the combined use of Open Source MANO (OSM) and Openslice, are aligned with the ZSM architectural principles captured in ZSM 002 together with the on-boarding, fulfilment and assurance operations specified in ZSM 008.
PoC Project Status : *(Ongoing/Completed)*	Completed

1.2 PoC Team Members Review

	Organisation name	ISG ZSM participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	Telefónica S.A.	Yes	Jose Ordonez-Lucena joseantonio.ordonezlucena@telefonica.com Diego R. López diego.r.lopez@telefonica.com	X	Network/ service provider	-Use case definitions -Business model definition
2	Telenor ASA	Yes	Min Xie min.xie@telenor.com Pål Grønsund pal.gronsund@telenor.com Andres J. González andres.gonzalez@telenor.com		Network/ service provider	-Use case definitions -Business model definition
3	Universidad Carlos III (UC3M)	No	Carmen Guerrero carmen.guerrero@uc3m.es Borja Nogales bdorado@pa.uc3m.es Iván Vidal ividal @it.uc3m.es Adrián Gallego adrgalle@pa.uc3m.es		University / Supplier	-VNFs provider -Integrator
4	University of Patras (UoP)	No	Spyros Denazis sdena@upatras.gr Dimitris Giannopoulos dimit.giannopoulos@upnet.gr Panagiotis Papaioannou papajohn@upatras.gr Yiannis Chatzis ioannis.chatzis@upatras.gr		University / Supplier	-VNFs provider -Integrator
5	Openslice	No	Christos Tranoris tranoris@ece.upatras.gr Kostis Trantzas ktrantzas@upnet.gr		Open source project	-Openslice framework

(*) Identify the PoC Point of Contact with an X.
(**) The Role will be network operator/service provider, infrastructure provider, application provider or other.

All the PoC Team members listed above declare that the information in this report is conformant to their activities during the PoC Project.

1.3 PoC Project Scope Review

1.3.1 PoC Topics

Report the status of all the PoC Topics and Expected Contributions anticipated in the PoC Proposal

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)

2	Automation in Multi-Stakeholder Ecosystem	ZSM 004(**)	ZSM(21)000162 "ZSM004 Add Openslice to Section 6" (***)
			ZSM(21)000163 "ZSM004 Openslice in ZSM architecture" (***)
				30/04/2021	Completed

(*) Planned, On-going, Completed, delayed (new target date), Abandoned

(**) The planned contribution was made to ZSM 004, as it was not possible to contribute to the ZSM 001 and ZSM 003 (WIs officially linked to the PoC topic #2, see https://zsmwiki.etsi.org/index.php?title=Topic2_-_Automation_in_Multi-Stakeholder_Ecosystems):

- ZSM 001 -> this WI was dormant (no active revision) during the PoC project lifetime.
- ZSM 003 -> by the time when the PoC results were available for contribution, ETSI ZSM started the approval process for ZSM 003 final draft, meaning no further contributions were allowed.

(***) These contributions propose Openslice as a solution to automate network slice out operation, where different administrative domains (each managed by a different stakeholder) participate in the scaling out operation, as planned in the PoC proposal. The multi-domain and multi-stakeholder nature of Openslice, as well as the mapping of its services into ZSM framework, is captured in these contributions. Section 2 of the present report describes the solution in different scenarios, and identifies some gaps in ZSM 008.

1.3.2 Other topics in scope

Report the status of all the additional PoC Topics and Contributions anticipated in the PoC Proposal.

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)
(*) Planned, On-going, Completed, delayed (new target date), Abandoned					

“Automation in Multi-Stakeholder Ecosystem” was the only PoC topic which was active during the PoC lifetime.

1.4 PoC Project Milestones Review

PoC Milestone	Milestone description	Target Date	Additional Info	Completion Date
P.P.1	PoC Presentation	02/12/2020	Presentation to ZSM NOC	15/11/2020
P.S	PoC Proposal submission	15/12/2020	Official PoC proposal submission	29/11/2020
P.P.2	PoC Public Announce	15/01/2021	Public Web announce in 5G-VINNI media (web, twitter, etc.). *Once it is approved.	11/01/2020
P.PU	PoC user story detailed	22/01/2021	Detailing use case, specifying actors, pre-conditions & post-conditions and exceptions.	03/02/2020
P.PT	PoC Test Plan	03/03/2021	Testbed setup and running	23/03/2021
P.D1	PoC Demo	17/03/2021	Demo for showcasing at ETSI endorsed Webinar	16/04/2021
P.C1	PoC Expected Contribution	17/03/2021	Propose contributions to several topics at ZSM meeting	30/04/2021 (to be presented in ZSM-14m Tech Call)
P.R	PoC Report	01/04/2021	PoC-Project-End Feedback	30/04/2021
P.E	PoC Project End	01/04/2021		30/04/2021

1.5 Confirmation of PoC Event Occurrence

Due to COVID-19 restrictions, the PoC was showcased in a free-of-charge, ETSI endorsed webinar which took place in April 16th, 2021. More details of this webinar can be found below:

- ETSI site for webinar registration: https://www.etsi.org/events/1905-webinar-zsm-poc-2-showcase-automated-network-slice-scaling-in-multi-site-environments?jjj=1619193312791
- Platform: ETSI BRIGHTTLAK CHANNEL
- Webinar title: “ZSM PoC#2 showcase: Automated network slice scaling in multi-site environments”
- Webinar duration: 105 min (15h00 – 16h45 CEST)
- Webinar statistics: 46 people attended live out of 90 pre-registered.

ETSI The Standards People

ZSM PoC#2 showcase: Automated network slice scaling in multi-site environments

Presented by: Jose Ordonez-Lucena, Christos Tranoris, Borja Nogales For: Webinar

16/04/2021

© ETSI 2021 – All rights reserved

1.6 Other dissemination activities

In order to reach a wider audience, the PoC team participated in the OSM Ecosystem Day at OSM-MR10 (https://osm.etsi.org/wikipub/index.php/OSM-MR10_Hackfest), with a 25-min presentation that provided an overview of this PoC#2. This presentation is publicly available at this following OSM website: http://osm-download.etsi.org/ftp/osm-9.0-nine/OSM-MR10-hackfest/EcosystemDay/OSM-MR10%20ED1%20-%20Telefonica.pdf

Open Source MANO

OSM-MR10, OSM Ecosystem Day

On the use of OSM to allow for automated network slice scaling in multi-site environments

Jose Ordonez-Lucena (Telefónica)

© ETSI

ETSI

2 ZSM PoC Technical Report

2.1 General

2.1.1 PoC motivation

The PoC#2 focuses on the management of a network slice when deployed across multiple administrative domains. Specifically, this PoC aims at demonstrating how to automatically scale out a network slice instance in multi-site environments. The rationale of the demonstration is as follows:

- There is an existing (running) network slice instance. This instance is deployed across two different 5G-VINNI facility sites: Madrid (Spain) and Patras (Greece), each hosting a portion of the entire network slice.
  - From a functional viewpoint, the network slice consists of multiple NFV network services, each corresponding to a network slice subnet.
  - From an operational viewpoint, the network slice is deployed as a multi-site network slice instance.
  - From a network viewpoint, there exists L3 connectivity between Madrid and Patras, so that in-slice connectivity can be ensured along the entire data path.
- The behavior of existing (running) network slice instance is continuously monitored
  - Policy-based performance management on individual facility sites
  - There are pre-defined policy rules that allow triggering the need for scaling out operation based on collected metrics.
- When certain policy rules are met at Madrid facility site, a scaling out operation is triggered. This operation applies to the entire network slice instance.
  - This means that although the scaling out operationally is triggered at Madrid facility site, this operation needs to be propagated to Patras facility site accordingly.
  - Consistency is a must: increasing capacity of one network slice subnet on one facility site requires modifying the capacity of the network slice subnet accordingly.

According to this rationale, the PoC#2 requires a use case that justifies (i) having a multi-site network slice instance; (ii) the triggering of scaling out operation at Madrid facility site, and (iii) the need to propagate the scaling out operation to the Patras facility site. The selected use case is based on vertical industry related (e.g. e-Health, PPDR) NetApps hackathon involving developers from Spain and Greece. For this short-lived event, a network slice instance is deployed.

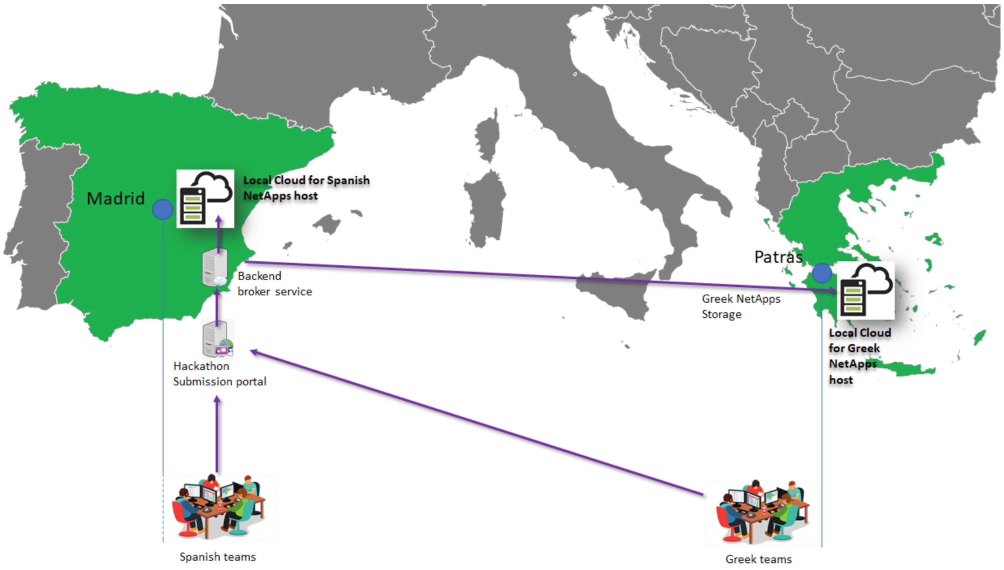

Madrid
Local Cloud for Spanish NetApps host
Backend broker service
Hackathon Submission portal
Spanish teams
Patras
Greek NetApps Storage
Local Cloud for Greek NetApps host
Greek teams

Figure 1

The logic of the in-scope use case, illustrated in Figure 1, is as follows:

- There is a NetApp submission service where developers continuously upload their solutions. The NetApps submission portal and the backend service broker are hosted in Madrid facility site.
- Due to EU defined General Data Protection Regulation (GDPR) policy, NetApps binaries and data must be hosted in the home country. Therefore, the services for managing the NetApps catalogue repositories need to be located at both Madrid and Patras facility sites.
- During the hackathon days, there is a sudden high demand of portal interaction, due to an unexpected prize to winner developers. The demand is first detected in Madrid, thus the backend hosts of NetApps catalogue repository will be automatically scaled there.
- The scaling out operation triggered in Madrid is propagated to the Patras facility site, since this sudden high demand of portal interaction is also expected at Greece side. Unlike Madrid, where the scaling out was a reactive corrective action, the scaling out operation triggered at Patras facility site is a pro-active corrective action (due to forecasting reasons).

2.1.2 PoC architecture

The architecture for this PoC is illustrated in Figure 2. As seen, the setup consists of two identical orchestration stacks, one for each 5G-VINNI facility site involved: Openslice (Service Orchestrator) + OSM (NFV Orchestrator) + Openstack (VIM). To allow for multi-site network slice orchestration, interworking between both stacks is a must. In the PoC, this interworking occurs at the Service Orchestration layer, with “Madrid-Openslice” and “Patras-Openslice” communicating using TMF Forum Open APIs.

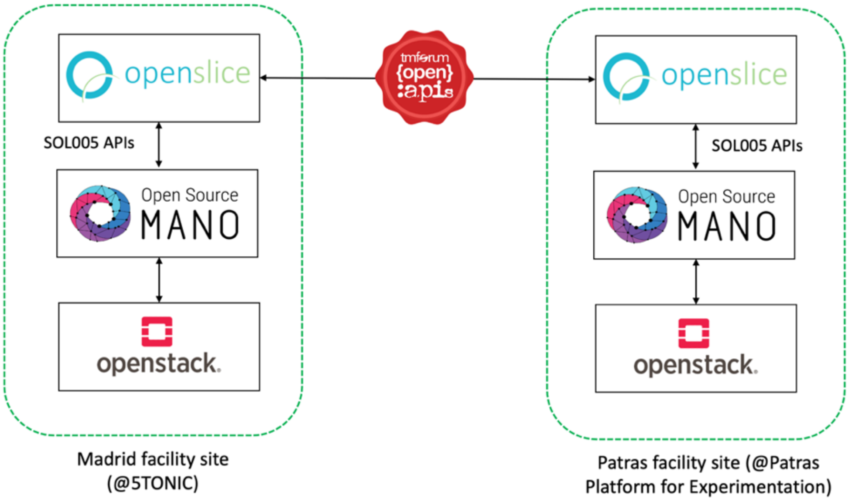


Figure 2

In ZSM architectural framework, OSM is mapped to a ZSM management domain (MD), while Openslice plays the role of E2E service MD. Figures 3 and 4 provide a more detailed view of OSM and Openslice internal architectures, illustrating how their modules are related to ZSM grouping data and management services. More details of these relationships can be found in the first PoC#2 report [1].

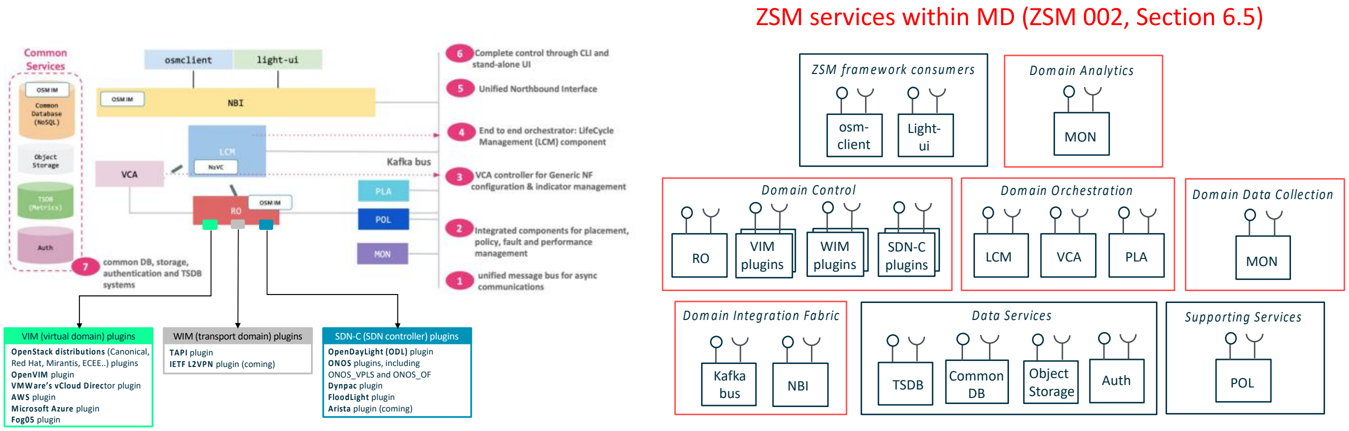

Common Services
OSM IM
Common Database (NoSQL)
Object Storage
TSDB (Metrics)
Auth
7 common DB, storage, authentication and TSDB systems
osmclient
light-ui
OSM IM
NBI
LCM
N2VC
VCA
Kafka bus
RO
OSM IM
PLA
POL
MON
6 Complete control through CLI and stand-alone UI
5 Unified Northbound Interface
4 End to end orchestrator: LifeCycle Management (LCM) component
3 VCA controller for Generic NF configuration & indicator management
2 Integrated components for placement, policy, fault and performance management
1 unified message bus for async communications
VIM (virtual domain) plugins
OpenStack distributions (Canonical, Red Hat, Mirantis, ECEE..) plugins
OpenVIM plugin
VMWare's vCloud Director plugin
AWS plugin
Microsoft Azure plugin
Fog05 plugin
WIM (transport domain) plugins
TAPI plugin
IETF L2VPN plugin (coming)
SDN-C (SDN controller) plugins
OpenDayLight (ODL) plugin
ONOS plugins, including ONOS_VPLS and ONOS_OF
Dynpac plugin
FloodLight plugin
Arista plugin (coming)
ZSM services within MD (ZSM 002, Section 6.5)
ZSM framework consumers
osm-client
Light-ui
Domain Analytics
MON
Domain Control
RO
VIM plugins
WIM plugins
SDN-C plugins
Domain Orchestration
LCM
VCA
PLA
Domain Data Collection
MON
Domain Integration Fabric
Kafka bus
NBI
Data Services
TSDB
Common DB
Object Storage
Auth
Supporting Services
POL

Figure 3

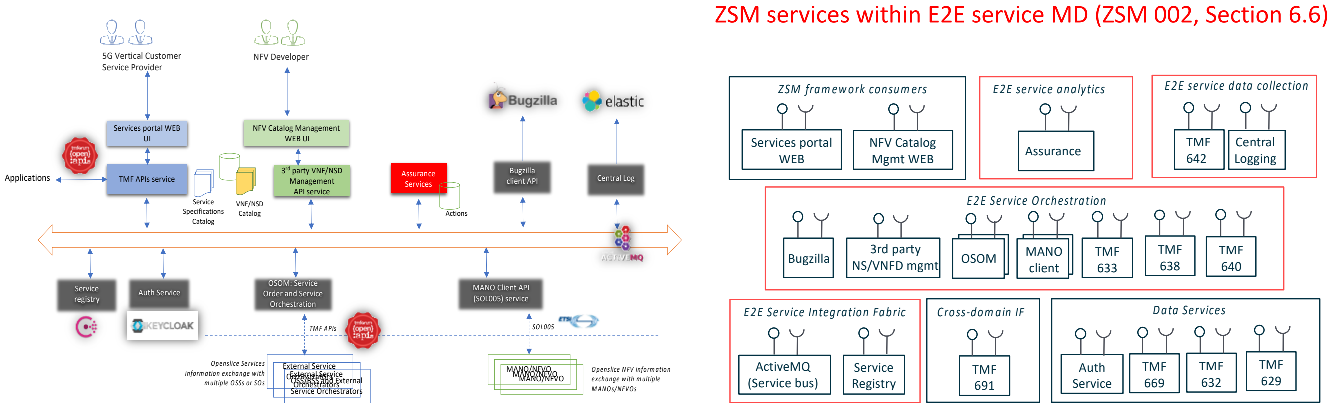

5G Vertical Customer Service Provider
NFV Developer
Bugzilla
elastic
Services portal WEB UI
NFV Catalog Management WEB UI
Applications
TMF APIs service
Service Specifications Catalog
VNF/NSD Catalog
3rd party VNF/NSD Management API service
Assurance Services
Actions
Bugzilla client API
Central Log
ACTIVEMQ
Service registry
Auth Service
KEYCLOAK
OSOM: Service Order and Service Orchestration
MANO Client API (SOL005) service
TMF APIs
SOL005
ETSI
Openslice Services information exchange with multiple OSSs or SOs
External Service Orchestrators
OSS/BSS and External Service Orchestrators
MANO/NFVO
Openslice NFV information exchange with multiple MANOs/NFVOs
ZSM services within E2E service MD (ZSM 002, Section 6.6)
ZSM framework consumers
Services portal WEB
NFV Catalog Mgmt WEB
E2E service analytics
Assurance
E2E service data collection
TMF 642
Central Logging
E2E Service Orchestration
Bugzilla
3rd party NS/VNFD mgmt
OSOM
MANO client
TMF 633
TMF 638
TMF 640
E2E Service Integration Fabric
ActiveMQ (Service bus)
Service Registry
Cross-domain IF
TMF 691
Data Services
Auth Service
TMF 669
TMF 632
TMF 629

Figure 4

2.1.3 PoC user story

The NetApps hackathon event captured in Figure 1 requires deploying a network slice across Madrid and Patras facility sites. This means that each facility site hosts a portion of the slice. The internal composition of this slice and the geographical distribution of their functional components is illustrated in Figure 5. As seen, the network slice consists of three network slice subnets, each modelled as a separate Network Service Descriptor (NSD).

- **Network Slice Subnet A (NSS-A),** deployed in Madrid according to NSD_F. The NSD_F is composed of four VNFs, including two Load Balancers (LB-1 and LB-2), one Web Server and one backend API brokering service.
- **Network Slice Subnet B (NSS-B),** deployed in Madrid according to NSD_{SRV}. The NSD_{SRV}, consisting of three VNFs, including one Load Balancer (LB-3), one repository catalogue and one catalogue DB.
- **Network Slice Subnet C (NSS-C),** deployed in Greece according to NSD_{SRV}. Like NSS-B, NSS-C holds the repository catalogue and its supported DB, together with the LB-3 as an entry point of requests.

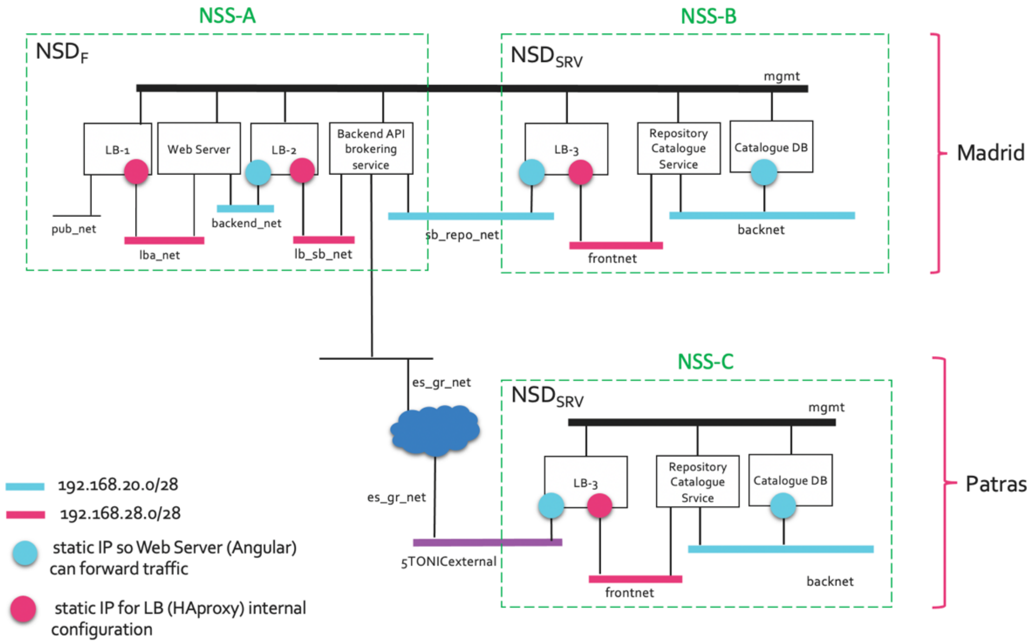


Figure 5

Madrid-Patras connectivity is based on a multi-site NFV and data communication pipe enabled through a VPN-based overlay solution. For more details of the specific solution used, see [2].

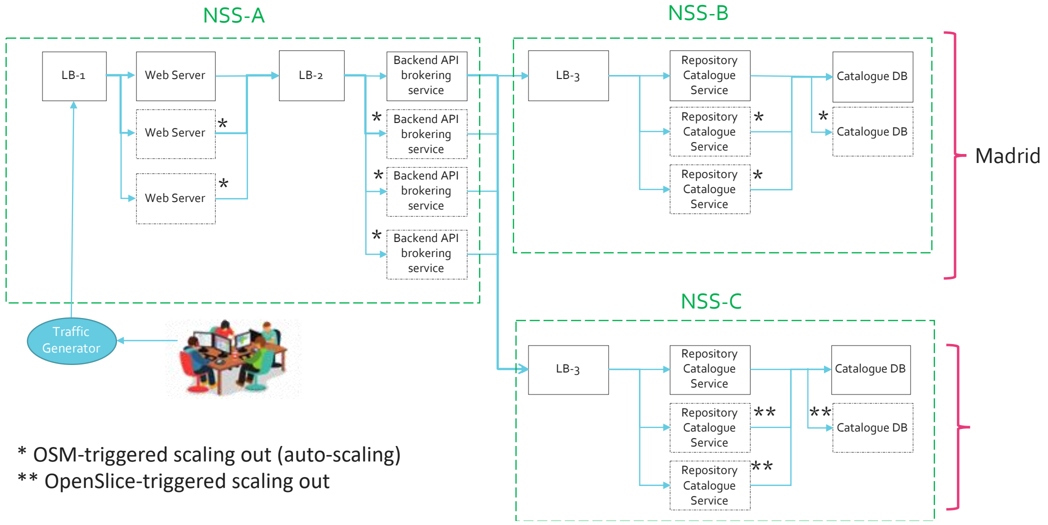
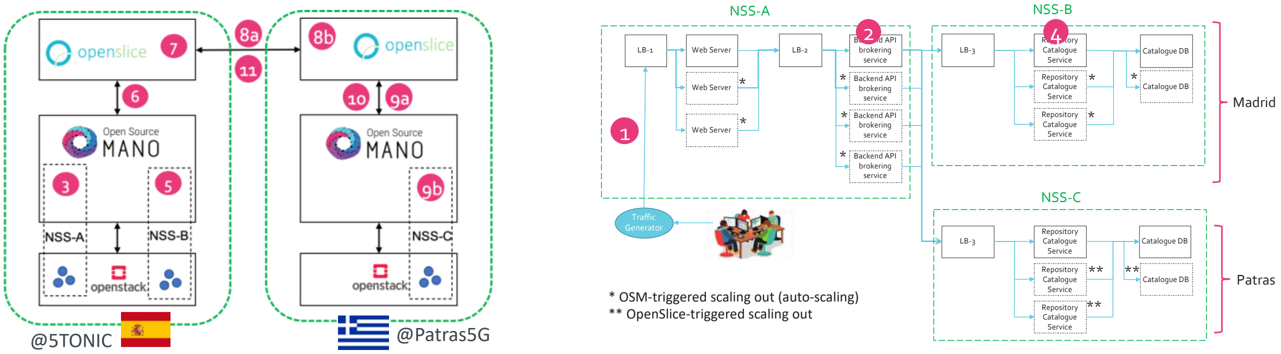

NSS-A
NSS-B
LB-1
Web Server
Web Server
Web Server
LB-2
Backend API brokering service
Backend API brokering service
Backend API brokering service
Backend API brokering service
LB-3
Repository Catalogue Service
Repository Catalogue Service
Repository Catalogue Service
Catalogue DB
Catalogue DB
Madrid
Traffic Generator
NSS-C
LB-3
Repository Catalogue Service
Repository Catalogue Service
Repository Catalogue Service
Catalogue DB
Catalogue DB
* OSM-triggered scaling out (auto-scaling)
** OpenSlice-triggered scaling out

Figure 6

Figure 6 illustrates the impact of the scaling operation over the running slice instance. The white-colored part of the figure captures the slice instance as originally deployed for the NetApps hackathon (PoC pre-conditions), while the full picture shows the state of the slice instance after being scaled out (PoC post-conditions). The user story that explains this transition is depicted in Figure 7. For more details, see the first PoC#2 report in [1].


8a
8b
11
openslice
7
openslice
6
10
9a
Open Source MANO
Open Source MANO
3
5
9b
NSS-A
NSS-B
NSS-C
openstack
openstack
@5TONIC
@Patras5G
NSS-A
NSS-B
NSS-C
LB-1
Web Server
Web Server
Web Server
LB-2
Backend API brokering service
Backend API brokering service
Backend API brokering service
Backend API brokering service
2
1
LB-3
Repository Catalogue Service
Repository Catalogue Service
Repository Catalogue Service
4
Catalogue DB
Catalogue DB
Madrid
LB-3
Repository Catalogue Service
Repository Catalogue Service
Repository Catalogue Service
Catalogue DB
Catalogue DB
Patras
Traffic Generator
* OSM-triggered scaling out (auto-scaling)
** OpenSlice-triggered scaling out

1 There is a sudden high demand of portal interaction at Madrid facility site (HTTP requests represents a traffic load surge with 3:1 ratio)

2 NSS-A's backend API brokering service collapses, being not able to forward traffic to etiher NSS-B or NSS-C

3 Based on day-2 activities, "Madrid-OSM" triggers **NSS-A auto-scaling** -> Web server (2 x scale out), LB-1 (reconfiguration), LB-2 (reconfiguration)

4 NSS-A's backend API brokering service back on normal operation, and starts sending traffic to NSS-B through LB-3. NSS-B's VNFs collapse.

5 Based on day-2 activities, "Madrid-OSM" triggers **NSS-B auto-scaling** -> Repository catalogue (2x scale out), DB (1 x scale out), LB-3 (reconfiguration)

6 "Madrid-OSM" notifies "Madrid-OpenSlice" of successul steps 3 and 5

7 "Madrid-OpenSlice" decides that NSS-C needs to be scaled out as NSS-B did, to avoid collapse as in Madrid -> OpenSlice is aware of UC semantics

8 "Madrid-OpenSlice" issues NSS-C scaling request to "Patras-OpenSlice", using TMF's APIs. "Patras-OpenSlice" checks this request.

9 "Patras-OpenSlice" forwards the request to the "Patras-OSM" for enforcement. Unlike step 3 and 5, here **there is no NSS-C auto-scaling**

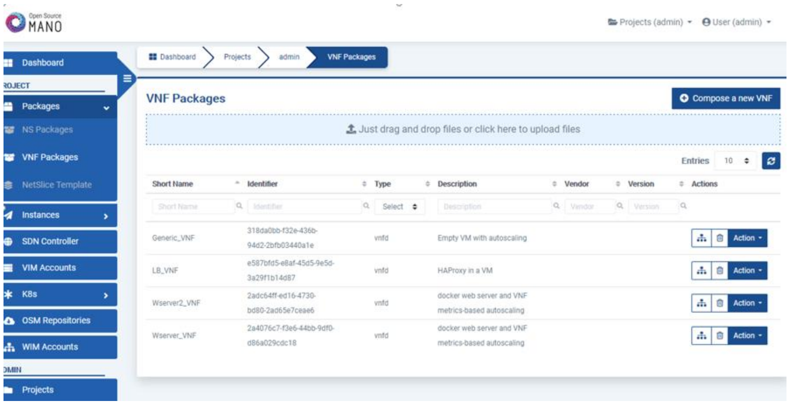
10 "Patras-OSM" notifies "Patras-OpenSlice" of NSS-C scaling out.

11 "Patras-OpenSlice" notifies "Madrid-OpenSlice" of successful NSS-C scaling out.

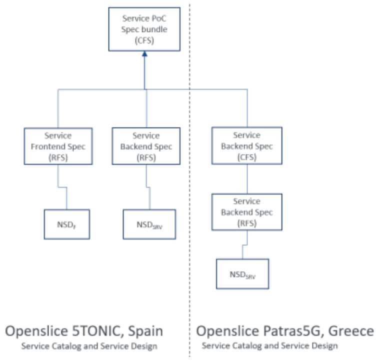
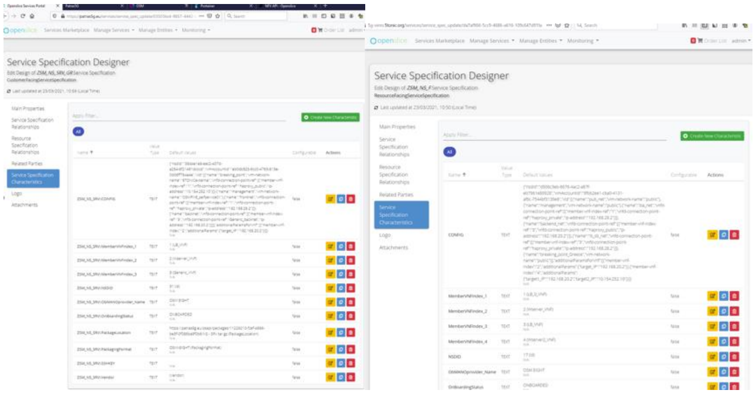
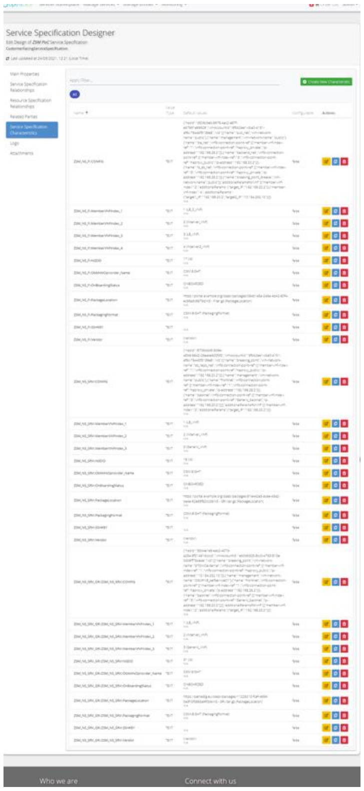
Figure 7

2.1.4 Scenarios

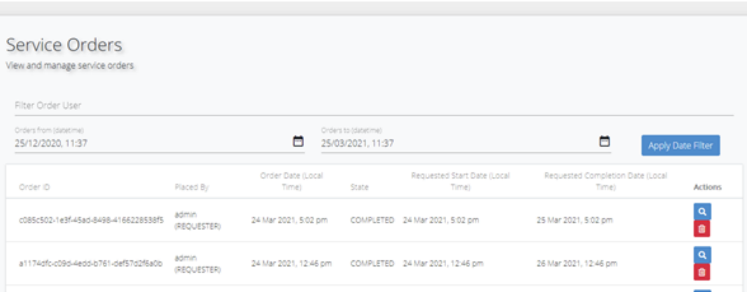
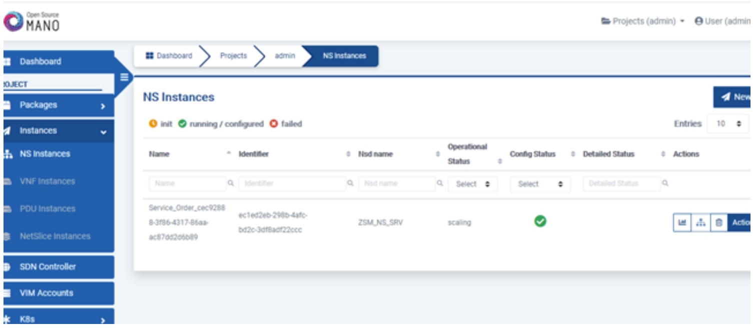
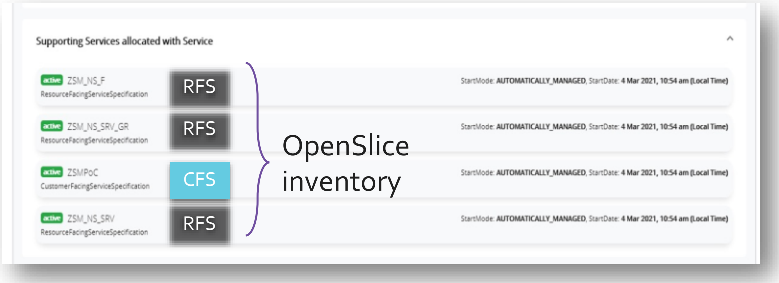
2.1.4.1 Scenario 1: Service on-boarding

<table>
<tr><td><b>Precondition</b></td><td colspan="2">Each facility site includes their management and orchestration stack (Openslice+OSM+Openstack) in operation. Both Openslice instances are configured to communicate and exchange Service Catalog management and Service Ordering management related request-response/notify-subscription messages.</td></tr>
<tr><td><b>Verification</b></td><td colspan="2">VNFDs and NSDs are onboarded to the OSM instance available in each facility. RFS and CFS specifications are onboarded to the Openslice instance available in each facility.</td></tr>
<tr><td colspan="3"><b>Sequence</b></td></tr>
<tr><td colspan="2"><b>a.</b> NSD$_F$ (and constituent VNFDs) together with NSD$_{SRV}$ (and corresponding VNFDs) are onboarded to "Madrid-OSM". These descriptors specify the NFV resource requirements of NSS-A and NSS-B, respectively.</td><td rowspan="2">

VNF Packages
Just drag and drop files or click here to upload files
<table>
<tr><th>Short Name</th><th>Identifier</th><th>Type</th><th>Description</th><th>Vendor</th><th>Version</th><th>Actions</th></tr>
<tr><td>Generic_VNF</td><td>318da0bb-f32e-436b-94d2-2bfb03440a1e</td><td>vnfd</td><td>Empty VM with autoscaling</td><td></td><td></td><td>Action</td></tr>
<tr><td>LB_VNF</td><td>e587bfd5-e8af-45d5-9e5d-3a29f1b14d87</td><td>vnfd</td><td>HAProxy in a VM</td><td></td><td></td><td>Action</td></tr>
<tr><td>Wserver2_VNF</td><td>2adc64ff-ed16-4730-bd80-2ad65e7ceae6</td><td>vnfd</td><td>docker web server and VNF metrics-based autoscaling</td><td></td><td></td><td>Action</td></tr>
<tr><td>Wserver_VNF</td><td>2a4076c7-f3e6-44bb-9df0-d86a029cdc18</td><td>vnfd</td><td>docker web server and VNF metrics-based autoscaling</td><td></td><td></td><td>Action</td></tr>
</table></td></tr>
<tr><td colspan="2"><b>b.</b> NSD$_{SRV}$ (and constituent VNFDs) is onboarded to "Patras-OSM". This descriptor specifies the NFV resource requirements of NSS-C.</td></tr>
</table>

c. The CFS and RFS specifications describing the slice subnets to be deployed for the PoC are designed in Openslice. The composition of these specifications and their relationships with the onboarded NSDs are captured in the right-side figure. This figure illustrates the diagram tree for the PoC slice specification.	 Service PoC Spec bundle (CFS) Service Frontend Spec (RFS) Service Backend Spec (RFS) Service Backend Spec (CFS) Service Backend Spec (RFS) NSD$_F$ NSD$_{SRV}$ NSD$_{SRV}$ Openslice 5TONIC, Spain Service Catalog and Service Design Openslice Patras5G, Greece Service Catalog and Service Design
d. The RFS specifications of those network slice subnets to be deployed at Spain facility site (NSS-A and NSS-B) are designed in "Madrid-Openslice". These specifications include "Service Frontend Spec (RFS): NSS-A" and "Service Backend Spec (RFS): NSS-B".	 openslice Services Marketplace Manage Services Manage Entities Monitoring Service Specification Designer Edit Design of ZSM_NS_SRV_GR Service Specification CustomerFacingServiceSpecification Main Properties Service Specification Relationships Resource Specification Relationships Related Parties Service Specification Characteristics Logo Attachments Create New Characteristic All Name Value Type Default Values Configurable Actions Service Specification Designer ResourceFacingServiceSpecification
e. The RFS specification of the network slice subnet to be deployed at Greece facility site (NSS-C) is designed in "Patras-Openslice". This specification corresponds to "Service Frontend Spec (RFS): NSS-C".	
f. The "Service Frontend Spec (RFS): NSS-C" needs to be available public in the "Patras-Openslice" service catalog, so that it can be exposed to the "Madrid-Openslice" service catalog. To that end, the RFS specification is turned into a CFS specification.	
g. The CFS specification of the PoC network slice is designed in "Madrid-Openslice" according to this bundle: "Service Frontend Spec (RFS): NSS-A" + "Service Backend Spec (RFS): NSS-B" + "Service Backend Spec (CFS): NSS-C".	 Service Specification Designer Edit Design of ZSM PoC Service Specification CustomerFacingServiceSpecification Main Properties Service Specification Relationships Resource Specification Relationships Related Parties Service Specification Characteristics Logo Attachments All Who we are Connect with us

2.1.4.2 Scenario 2: Service deployment

<table>
<tr><td><b>Precondition</b></td><td colspan="2">The CFS/RFS specifications and NSD/VNFDs are onboarded to Openslice and OSM at both facility sites.</td></tr>
<tr><td><b>Verification</b></td><td colspan="2">The network slice instance is running. Metadata info (records) of deployed network slice subnet instances are stored in the service inventories of both facility sites. Action rules for service policy management are created.</td></tr>
<tr><td colspan="3"><b>Sequence</b></td></tr>
<tr><td colspan="2"><b>a.</b> The customer requests the allocation of a dedicated network slice. To that end, it issues a service order based on Service PoC bundle (CFS).</td><td rowspan="2"></td></tr>
<tr><td colspan="2"><b>b.</b> The service order is captured in “Madrid-Openslice” OSOM.</td></tr>
<tr><td colspan="2"><b>c.</b> Following the diagram tree for the PoC slice specification, the network services (and VNFs) corresponding to individual network slice subnets are deployed on every facility site. Network service instances based on NSD_F and NSD_{SRV} are deployed in Spain facility site (via “Madrid-OSM”), while a network service instance based on NSD_{SRV} is deployed in Greece facility site (via “Patras-OSM”).</td><td rowspan="2">
</td></tr>
<tr><td colspan="2"><b>d.</b> Day-0 + day-1 configuration of individual VNFs is performed via Juju charms. After this, the service order is successfully completed. The components building up the network slice instance are running.</td></tr>
</table>

Service Orders

View and manage service orders

Filter Order User

Orders from (datetime): 25/12/2020, 11:37

Orders to (datetime): 25/03/2021, 11:37

Apply Date Filter

Order ID	Placed By	Order Date (Local Time)	State	Requested Start Date (Local Time)	Requested Completion Date (Local Time)	Actions
c085c502-1e3f-45ad-8498-4166228538f5	admin (REQUESTER)	24 Mar 2021, 5:02 pm	COMPLETED	24 Mar 2021, 5:02 pm	25 Mar 2021, 5:02 pm	
a1174dfc-c09d-4edd-b761-def57d2f6a0b	admin (REQUESTER)	24 Mar 2021, 12:46 pm	COMPLETED	24 Mar 2021, 12:46 pm	26 Mar 2021, 12:46 pm	

NS Instances

init ● running / configured ● failed

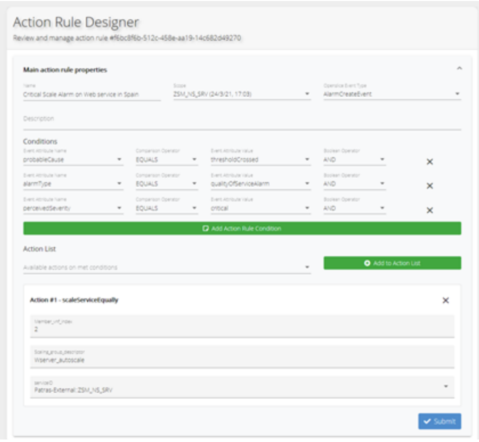
Name	Identifier	Nsd name	Operational Status	Config Status	Detailed Status	Actions
Service_Order_cec92888-3f86-4317-86aa-ac87dd2d6b89	ec1ed2eb-298b-4afc-bd2c-3df8adf22ccc	ZSM_NS_SRV	scaling	✓		Actio

Supporting Services allocated with Service

active ZSM_NS_F ResourceFacingServiceSpecification	RFS	StartMode: **AUTOMATICALLY_MANAGED**, StartDate: **4 Mar 2021, 10:54 am (Local Time)**
active ZSM_NS_SRV_GR ResourceFacingServiceSpecification	RFS	StartMode: **AUTOMATICALLY_MANAGED**, StartDate: **4 Mar 2021, 10:54 am (Local Time)**
active ZSMPoC CustomerFacingServiceSpecification	CFS	StartMode: **AUTOMATICALLY_MANAGED**, StartDate: **4 Mar 2021, 10:54 am (Local Time)**
active ZSM_NS_SRV ResourceFacingServiceSpecification	RFS	StartMode: **AUTOMATICALLY_MANAGED**, StartDate: **4 Mar 2021, 10:54 am (Local Time)**

e. An action rule is created on the scope of the running network slice. This action rule assists Openslice to perform service auto-scaling. The created alarm is as follows:

SCOPE affectedService="ZSM_NS_SRV"
ON AlarmCreateEvent
IF (probableCause = thresholdCrossed) & (severity = critical) & (alarmType = qualityOfServiceAlarm)
THEN actions = scaleServiceEqually(Patras-External::ZSM_NS_SRV, VNFIndex=2)



Action Rule Designer

Review and manage action rule #f6bc8f6b-512c-458e-aa19-14c682d49270

Main action rule properties

Name: Critical Scale Alarm on Web service in Spain
Scope: ZSM_NS_SRV (24/3/21, 17:03)
Openslice Event Type: AlarmCreateEvent
Description:

Conditions

Event Attribute Name	Comparison Operator	Event Attribute Value	Boolean Operator
probableCause	EQUALS	thresholdCrossed	AND
alarmType	EQUALS	qualityOfServiceAlarm	AND
perceivedSeverity	EQUALS	critical	AND

Action List

Available actions on met conditions

Action #1 - scaleServiceEqually

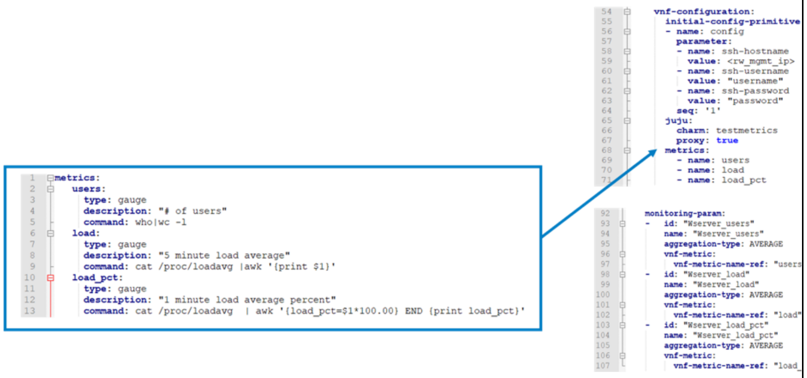
Member_vnf_index: 2
Scaling_group_descriptor: Wserver_autoscale
serviceID: Patras-External::ZSM_NS_SRV

2.1.4.3 Scenario 3a: Service auto-scaling (OSM)

Precondition	After scenario 2, the slice instance is completely deployed and configured across both facility sites.
Verification	The OSM component included in the orchestration stack of the Madrid facility site monitors the service performance offered by both subnets deployed in that facility site, and automatically executes the reactive scaling out operations in case of detecting a service performance degradation. NSS-A and NSS-B are successfully scaled out.

Sequence

a. "OSM-Madrid" starts monitoring the performance offered by both subnets deployed in this facility site. For this purpose, the VNFDs include the metrics that are intended to be collected by the OSM monitoring framework, as well as the frequency for their collection.



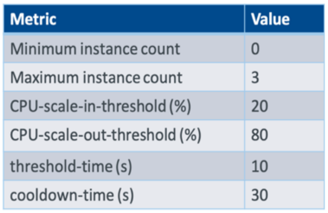
```
metrics:
    users:
      type: gauge
      description: "# of users"
      command: who|wc -l
    load:
      type: gauge
      description: "5 minute load average"
      command: cat /proc/loadavg |awk '{print $1}'
    load_pct:
      type: gauge
      description: "1 minute load average percent"
      command: cat /proc/loadavg  | awk '{load_pct=$1*100.00} END {print load_pct}'
```

```
      vnf-configuration:
        initial-config-primitive
        - name: config
          parameter:
          - name: ssh-hostname
            value: <rw_mgmt_ip>
          - name: ssh-username
            value: "username"
          - name: ssh-password
            value: "password"
          seq: '1'
        juju:
          charm: testmetrics
          proxy: true
        metrics:
          - name: users
          - name: load
          - name: load_pct
```

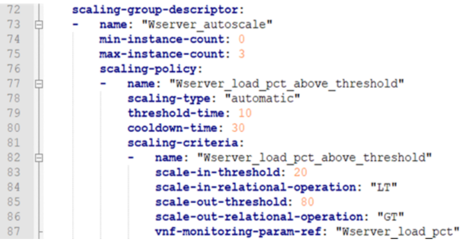
```
    monitoring-param:
    -   id: "Wserver_users"
        name: "Wserver_users"
        aggregation-type: AVERAGE
        vnf-metric:
          vnf-metric-name-ref: "users
    -   id: "Wserver_load"
        name: "Wserver_load"
        aggregation-type: AVERAGE
        vnf-metric:
          vnf-metric-name-ref: "load"
    -   id: "Wserver_load_pct"
        name: "Wserver_load_pct"
        aggregation-type: AVERAGE
        vnf-metric:
          vnf-metric-name-ref: "load_
```

b. Due to the high demand of user requests (cf. user story, step 1), the Web Server collapses in terms of CPU usage (cf. user story, step 2). "Madrid-OSM" detects a performance degradation on NSS-A, leveraging OSM performance management framework (with OSM's POL and MON modules involved), and decides that a corrective action needs to be taken on this web server. To that end, the POL module checks the rules defined in the VNFD: trigger scaling out operation when CPU usage exceeds 80%.

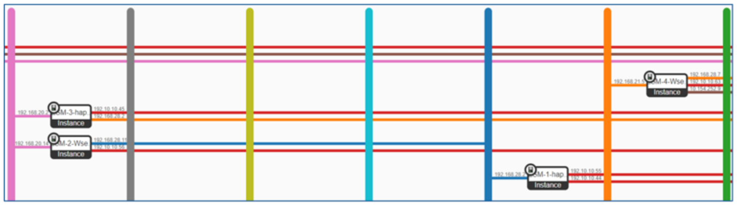
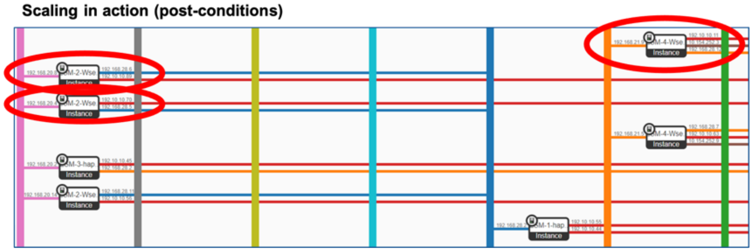
c. "Madrid-OSM" proceeds with the scaling operation on web server VNF.



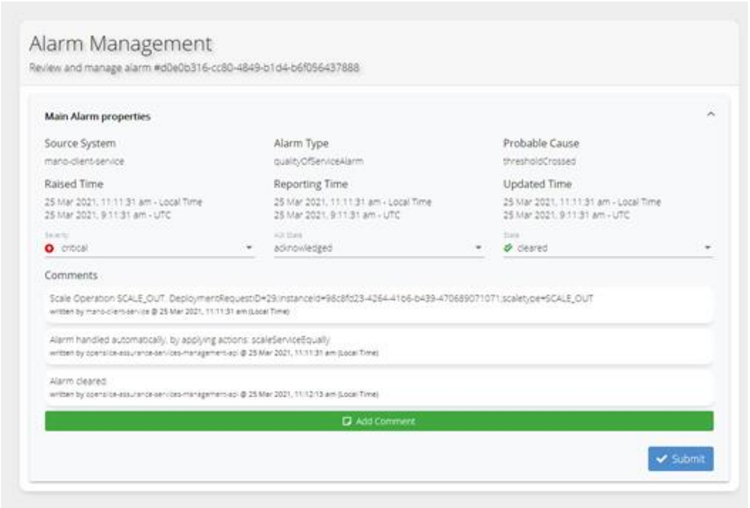
Metric	Value
Minimum instance count	0
Maximum instance count	3
CPU-scale-in-threshold (%)	20
CPU-scale-out-threshold (%)	80
threshold-time (s)	10
cooldown-time (s)	30

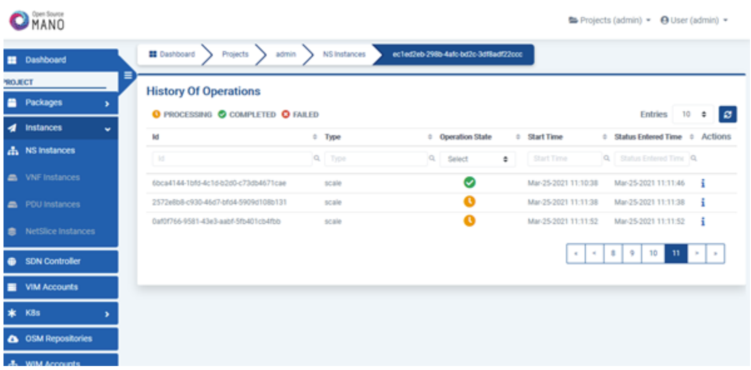


```
    scaling-group-descriptor:
    -   name: "Wserver_autoscale"
        min-instance-count: 0
        max-instance-count: 3
        scaling-policy:
        -   name: "Wserver_load_pct_above_threshold"
            scaling-type: "automatic"
            threshold-time: 10
            cooldown-time: 30
            scaling-criteria:
            -   name: "Wserver_load_pct_above_threshold"
                scale-in-threshold: 20
                scale-in-relational-operation: "LT"
                scale-out-threshold: 80
                scale-out-relational-operation: "GT"
                vnf-monitoring-param-ref: "Wserver_load_pct"
```

d. Once web server VNF has been scaled out, the rest of NSS-A components need also to be resized accordingly, by creating additional instances of backend API brokering service VNF, following the same procedure as steps 2 and steps 3.	Scaling in action (pre-conditions)  Scaling in action (post-conditions) 
e. The NSS-A components, including existing and newly created VNF instances, are configured accordingly (cf. user story, step 3). This allows capturing the results of scaling operation in the semantics of individual VNFs.	
f. Due to the high demand of user requests (cf. user story, step 1), the NSS-B VNFs collapse (cf. user story, step 4). "Madrid-OSM" detects a performance degradation on NSS-B leveraging OSM performance management framework, and decides that a corrective action needs to be taken on the "Repository Catalog service".	
g. The NSS-B is scaled out (cf. user story, step 5). To that end, steps c, d and e are similarly applied on NSS-B VNFs.	

2.1.4.4 Scenario 3b: Service auto-scaling (Openslice)

Precondition	NSS-A and NSS-B have been successfully scaled out at the Spain facility site.
Verification	NSS-C is scaled at Patras, following up the event captured at Madrid. "Madrid-Openslice" is notified about the successful NSS-C scaling out operation.
Sequence	
a. Upon NSS-A and NSS-B scaling out operation, "Madrid-OSM" sends a notification to "Madrid-Openslice" (cf. use story, step 6)	 Alarm Management Review and manage alarm #d0e0b316-cc80-4849-b1d4-b6f056437888 Main Alarm properties Source System: mano-client-service Alarm Type: qualityOfServiceAlarm Probable Cause: thresholdCrossed Raised Time: 25 Mar 2021, 11:11:31 am - Local Time; 25 Mar 2021, 9:11:31 am - UTC Reporting Time: 25 Mar 2021, 11:11:31 am - Local Time; 25 Mar 2021, 9:11:31 am - UTC Updated Time: 25 Mar 2021, 11:11:31 am - Local Time; 25 Mar 2021, 9:11:31 am - UTC Severity: critical Ack State: acknowledged State: cleared Comments Scale Operation SCALE_OUT. DeploymentRequestID=29;instanceId=98c8fd23-4264-4106-b439-470689071071;scaletype=SCALE_OUT written by mano-client-service @ 25 Mar 2021, 11:11:31 am (Local Time) Alarm handled automatically, by applying actions: scaleServiceEqually written by openslice-assurance-services-management-api @ 25 Mar 2021, 11:11:31 am (Local Time) Alarm cleared written by openslice-assurance-services-management-api @ 25 Mar 2021, 11:12:13 am (Local Time) Add Comment ✓ Submit
b. "Madrid-Openslice" acknowledges the receipt of this notification by creating an alarm. The alarm matches the action rule originally designed in scenario 2 (service deployment), and therefore "Madrid-Openslice" handles it (cf. user story, step 7). **SCOPE** affectedService="ZSM_NS_SRV" **ON** AlarmCreateEvent **IF** (probableCause = thresholdCrossed) & (severity = critical) & (alarmType = qualityOfServiceAlarm) **THEN** actions = scaleServiceEqually(Patras-External::ZSM_NS_SRV, VNFIndex=2)	

c. Following up the directives from the action rule, **“**Madrid-Openslice” requests “Patras-Openslice” to scale NSS-C out, using TMF OpenAPIs (cf. user story, step 8).	
d. NSS-C is scaled at Patras (cf. user story, step 9), following the step g from scenario 3a.	
e. Upon receiving notification from “Patras-OSM”, the **“**Patras-Openslice” notifies the “Madrid-Openslice” (cf. user story, steps 10 and 11).	

History Of Operations

● PROCESSING ✓ COMPLETED ✕ FAILED

Entries 10

Id	Type	Operation State	Start Time	Status Entered Time	Actions
6bca4144-1bfd-4c1d-b2d0-c73db4671cae	scale	✓	Mar-25-2021 11:10:38	Mar-25-2021 11:11:46	i
2572e8b8-c930-46d7-bfd4-5909d108b131	scale	●	Mar-25-2021 11:11:38	Mar-25-2021 11:11:38	i
0af0f766-9581-43e3-aabf-5fb401cb4fbb	scale	●	Mar-25-2021 11:11:52	Mar-25-2021 11:11:52	i

2.2 PoC Contribution to ZSM ISG

Use table B.1 to list any contributions to the ZSM ISG resulting from this PoC Project.

Table B.1

Contribution	WI/Document Ref	Comments	Meeting
ZSM(21)000162 “ZSM004 Add Openslice to Section 6”	ETSI GR ZSM 004 [3]	This contribution aims to include Openslice in the landscape of ZSM related open-source communities (ZSM 004, Section 6)	ZSM-14m Tech Call
ZSM(21)000163 “ZSM004 Openslice in ZSM architecture”	ETSI GR ZSM 004 [3]	This contribution is a proposal on how Openslice framework fits with the ZSM reference architecture, illustrating how Openslice components map with the ZSM grouping of management and data services.	ZSM-14m Tech Call

2.3 Gaps identified in ZSM standardization

Table B.2

Gap Identified	Forum (ZSM ISG, Other)	Affected WG/EG	WI/Document Ref	Gap details and Status
Policy-driven E2E service assurance	ZSM		ETSI GS ZSM 008 [4]	The PoC has demonstrated that automated scaling on a E2E service requires the definition of policies (action rules) in the service assurance set-up operation. However, no guidance on how a policy should be specified for this operation has been captured in ZSM 008 thus far. The PoC team recommends the ZSM 008 rapporteur (and contributors) to take action on this, providing some guidance for CSPs/vendors, so that they do not need to develop ad-hoc solutions every time they want to define a policy for a E2E service.
ZSM framework consumer	ZSM		ETSI GS ZSM 008 [4]	The PoC has demonstrated up to three different actors for the ZSM framework consumer: a ZSM management domain, a NFV developer and a vertical customer. The on-boarding, fulfilment and assurance operations detailed in ZSM 008 represents ZSM framework consumer in a generic, abstract manner, which are not always applicable to the different actors playing the role of ZSM framework consumer. The PoC team recommends the ZSM 008 rapporteur (and contributors) to take action on this, making it clear that not all the operation defined therein are applicable to every ZSM framework consumer. Examples captured in an informative annex could be valuable for outside readers.

2.4 PoC Suggested Action Items

The PoC#2 has leveraged the 5G-VINNI results and environment to demonstrate automation in multi-domain environments, with a focus on network slice lifecycle management, covering on-boarding, fulfilment and assurance phases [4]. The PoC team has showcased how ZSM architectural framework is a key asset to achieve a zero-touch slice operation beyond the boundaries of one network operator (thanks to the definition of a SBMA that facilitate collaborative interactions among different stakeholder), bridging the gaps between a variety of standards with different focus (e.g., TM Forum, ETSI NFV) as well.

The PoC#2 exemplifies a complete technology evolution path, based on the triplet {research + experimentation + standardization} and with open-source communities (OSM and Openslice) along the entire path.

The PoC#2 sets the ground for future experimentation in the future, with

- Further integration of additional NFVO solutions. For future work, PoC team is exploring the use of both open-source and vendor-specific NFVOs, to assess the interworking of YANG and TOSCA models, in on-boarding and fulfilment phases. To achieve the required interoperability, it is important that selected NFVOs provide SOL005 capabilities through their NBI.
- Scenarios focused on ETSI GS ZSM 009 (Closed-Loop Automation) and ETSI GS ZSM 012 (AI enablers).

2.5 Additional messages to ZSM

The PoC topic #2 only includes ZSM 001 and ZSM 003 as concerned WIs. However, there are other recent WIs, such as ZSM 004 ("Landscape", revision active) and ZSM 008 ("Cross-domain E2E service lifecycle management", now active after a long period of inactivity), that despite being related to the scope of PoC topic #2, they are not explicitly mentioned in the current PoC topic #2 description (see https://zsmwiki.etsi.org/index.php?title=Topic2_-_Automation_in_Multi-Stakeholder_Ecosystems).

The PoC team recommends the PoC Management Team (PMT) to update the current PoC topic #2 description to include ZSM 004 and ZSM 008 as in-scope WIs.

2.6 Additional messages to Network Operators and Service Providers

None

References

[1] ZSM PoC#2 Report 1, "PoC#2 user story", Feb 2021. Available: https://zsmwiki.etsi.org/images/f/ff/ZSM_POC_2_User_Story.pdf

[2] Nogales, B., Gonzalez, L. F., Vidal, I., Valera, F., Garcia-Reinoso, J., Lopez, D. R., Rodríguez, J., Gonzalez, N., Berberana, I., Azcorra, A. Integration of 5G Experimentation Infrastructures into a Multi-Site NFV Ecosystem. *J. Vis. Exp.* (168), e61946, doi:10.3791/61946 (2021).

[3] ETSI GR ZSM 004, "Zero-touch network and Service Management (ZSM); Landscape", v1.6.0, March 2021

[4] ETSI GR ZSM 008, "Zero-touch network and Service Management (ZSM); Cross-domain E2E Service Lifecycle Management", v0.6.0, March 2021.