ETSI GS ZSM 002 V1.1.1 (2019-08)

Zero-touch network and Service Management (ZSM); Reference Architecture

Disclaimer

The present document has been produced and approved by the Zero touch network and Service Management (ZSM) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/ZSM-002ed111_Arch

Keywords

architecture, management, network, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Zero touch network and Service Management (ZSM).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document defines and describes the reference architecture for the end-to-end Zero-touch network and Service Management (ZSM) framework based on a set of user scenarios and requirements documented in ETSI GS ZSM 001 [i.9].

The reference architecture employs a set of architectural principles, described further in the present document, and a service-centric architectural model to define at a high level a set of management services for zero-touch network and service management. It also defines means of management service integration, communication, interoperation, and organization. Procedures and detailed information models are beyond the scope of the present document.

The reference architecture also defines normative provisions for externally visible management services, defined as part of the reference architecture, as well as recommendations for their organization. It is assumed that the architectural patterns introduced in the present document can be used not only for the ZSM framework, but also for architecture and design of individual management services.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR ZSM 005: "Zero-touch network and Service Management (ZSM); Means of Automation".

[i.2] Boyd, J.R.: "The Essence of Winning and Losing", June 1995.

[i.3] Kephart, J. and D. Chess: "The Vision of Autonomic Computing", IEEE Computer, vol. 36, no. 1, pp. 41-50, DOI 10.1109/MC.2003.1160055, January 2003.

[i.4] Miller, D.E.: "A new approach to model reference adaptive control", IEEE Transactions on Automatic Control, Volume: 48, Issue: 5, May 2003.

[i.5] EU General Data Protection Regulation (GDPR).

NOTE: Available from https://eugdpr.org/.

[i.6] Telemanagement Forum Open Digital Architecture Project.

NOTE: Available from https://www.tmforum.org/collaboration/open-digital-architecture-oda-project/.

[i.7] ETSI TS 128 533: "5G; Management and orchestration;Architecture framework (3GPP TS 28.533)".

NOTE: Available at https://www.etsi.org/deliver/etsi_ts/128500_128599/128533/.

[i.8] ETSI GS ZSM 007: "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

[i.9] ETSI GS ZSM 001: "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios".

3 Definition of terms, symbols, abbreviations and conventions

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS ZSM 007 [i.8] and the following apply:

NOTE: If the same term is defined in both ETSI GS ZSM 007 [i.8] and in the present document, the definition in the present document takes precedence.

cross-domain data services: services that allow to share data with authorized consumers across management domains

external visibility: property of a ZSM service that indicates whether the scope of the service consumption spans outside the management domain

NOTE: Conventions for external visibility are defined in clause 3.4.

integration fabric: management function that plays both the roles of service consumer and service producer and which facilitates the interoperation and communication between management functions

key performance indicator: measurement of a specific aspect of the performance of a service that can be used in a service level objective

managed entity: managed resource or managed service

NOTE: Examples of managed entities are infrastructure resources, such as virtual network functions (VNF), physical network functions (PNF), and services such as cloud services, NFV network services, CFSs, RFSs.

managed resource: resource that is managed by one or more ZSM services

managed service: service that is managed by one or more ZSM services

management domain: scope of management that federates together management services, that enables their exposure towards external service consumers and that is delineated by a business, administrative, technological or other boundary

management function: logical entity playing the roles of service consumer and/or service producer

NOTE: The implementation details of a management function are not covered in the present document.

management service: See "ZSM service".

service capability: specific part of a ZSM service

NOTE: Examples of service capabilities are defined in the sub-clauses "Provided management services" of clauses 6.3, 6.4, 6.5 and 6.6 of the present document.

service consumer: role of an entity consuming one or more ZSM services

service end-point: interface through which service capabilities are offered and consumed

service level agreement: part of a business agreement between a service provider and a customer, specifying the committed service quality and quantity in terms of service level specifications, and the associated consequences in case the service level objectives are not met

service level objective: element in a service level specification that is defined in terms of parameters, and related metrics, thresholds and tolerances associated with the parameters

service level specification: specification of the minimum acceptable standard of service

service producer: role of an entity offering one or more ZSM services

ZSM framework consumer: entity outside the ZSM framework that uses one or several of the management capabilities offered by the ZSM framework

NOTE 1: ZSM framework consumers may be non-human entities (e.g. digital store fronts, web portals, BSS components, other ZSM framework instances) or human users.

NOTE 2: ZSM services offer machine-consumable interfaces. They may also allow interfacing with human users using e.g. a GUI, web portal or application.

ZSM service: set of offered management capabilities

NOTE: In the present document, the terms "ZSM service" and "management service" are used interchangeably.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ZSM 007 [i.8] and the following apply:

NOTE: If the same abbreviation is defined in both ETSI GS ZSM 007 [i.8] and in the present document, the definition in the present document takes precedence.

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
BSS	Business Support System
CDS	Cross-domain Data Services
CFS	Customer Facing Service
CPU	Central Processing Unit
CRUD	Create-Read-Update-Delete
CRUDL	Create-Read-Update-Delete-List
E2E	End-to-End
EP	End-Point
ETSI	European Telecommunications Standards Institute
FM	Fault Management
GDPR	General Data Protection Regulation
GR	Group Report
GS	Group Specification
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
IF	Integration Fabric
IP	Internet Protocol
IPR	Intellectual Property Right
ISG	Industry Specification Group
KPI	Key Performance Indicator
LI	Lawful Intercept
MANO	MANagement and Orchestration
MAPE-K	Monitor-Analyse-Plan-Execute plus Knowledge

MD	Management Domain
ML	Machine Learning
MRACL	Model-Reference Adaptive Control Loop
NBI	North Bound Interface
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
OODA	Observe, Orient, Decide, Act
PM	Performance Management
PNF	Physical Network Function
RFS	Resource Facing Service
SBI	South Bound Interface
SDN	Software-Defined Network
SLA	Service Level Agreement
SLO	Service Level Objective
SLS	Service Level Specification
SON	Self-Organizing Networks
TS	Technical Specification
VIM	Virtualized Infrastructure Manager
VLAN	Virtualized Local Area Network
VNF	Virtualized Network Function
XaaS	X-as-a-Service
ZSM	Zero-touch network and Service Management

3.4 Conventions

The present document defines ZSM services in a table that provides the name of the service, information about the visibility of that service outside the management domain where the service producer is located, information on the capabilities of that service and whether or not the capabilities are mandatory to provide.

The table format is reproduced below.

Table 3.4-1: Service definition template

Service name		Name of the service
External visibility		MANDATORY/CONDITIONAL (define condition)/OPTIONAL
Service capabilities		
	First capability (M/C/O)	Capability description.
	Next capability2 (M/C/O)	…
NOTE: (if needed, e.g. to define conditions.)		

The external visibility (or "ExtVis" in short) defines whether the service:

- shall always (i.e. without condition) be visible to consumers that are external to the management domain in which the producer resides (external visibility set to MANDATORY);
- shall be visible to external consumers if certain conditions are met and may be visible to external consumers otherwise (external visibility set to CONDITIONAL); or
- may be visible to external consumers (external visibility set to OPTIONAL).

If the external visibility is defined as CONDITIONAL, a condition is defined either in the "External visibility" row or in the "NOTE" row. ZSM services that are defined with optional external visibility are not required to be supported in ZSM.

The external visibility of data services and integration fabric services is documented separately as it depends on the scope. Hence, the "external visibility" row is not contained in tables that define a data service or an integration fabric service.

The capabilities offered by the service are defined under "Service capabilities". A capability can be mandatory (M) which means it shall be offered if the service is offered, conditional (C) which means it shall be offered under certain conditions if the service is offered or optional (O) which means it may be offered if the service is offered. For a conditional capability, the condition is defined in the description of the capability, or in the "NOTE" row. The description can contain normative statements to provide a finer-granular definition of the level of support for parts of a capability.

EXAMPLE 1: A capability to manage models could include items such as "create", "read", "update", "delete" and "list", where "create", "read" and "delete" are mandatory and "list" and "update" are optional. This can be documented as follows: "Manage models (M) -- Manage (create, read, update, delete, list) models. Create, read and delete shall be supported whereas update and list may be supported". In this case, the capability to manage models is mandatory to support, which implies that create, read and delete are mandatory and update and list are optional.

EXAMPLE 2: This example assumes that the "Manage models" capability is optional: "Manage models (O) -- Manage (create, read, update, delete, list) models. Create, read and delete shall be supported whereas update and list may be supported". In this case, the normative statements only apply if the "Manage models" capability is offered. In other words, if the "Manage models" capability is offered, create, read and delete are mandatory and update and list are optional.

4 Architecture principles

4.1 Introduction

The overarching design goal of ZSM is to enable zero-touch automated network and service management in a multi-vendor environment.

This clause introduces a number of architecture principles applicable to the ZSM framework reference architecture. These principles guide the way of designing the ZSM architecture to achieve the design goal stated above in order to allow fully automated network and service management.

4.2 The principles

4.2.1 Principle 01: Modularity

A modular architecture avoids monoliths and tight coupling, and consists of self-contained, loosely-coupled services, each with a confined scope which interact over well-defined interfaces.

4.2.2 Principle 02: Extensibility

An extensible architecture allows addition of new services, service capabilities and service end-points without breaking backward-compatibility and requiring changes to existing service designs, implementations and interactions.

4.2.3 Principle 03: Scalability

A scalable architecture allows deployments that can be adapted to satisfy the increasing or decreasing demand of the managed entities, and/or to various scales of the geographic distribution of these entities. Based on the principle of modularity (Principle 01), modules can be independently deployed and scaled.

4.2.4 Principle 04: Model-driven, open interfaces

An architecture that is based on model-driven approach performs the management of services and resources through the use of information models that capture the definition of managed entities in terms of attributes and supported operations. The models are defined independent from the implementation of the managed entities in order to facilitate portability, reusability and to allow vendor-neutral management of resources and services.

4.2.5 Principle 05: Closed-loop management automation

Closed-loop management automation is a feedback-driven process. It seeks to reach and preserve a set of objectives without any intervention external to the specific loop.

NOTE: Closed loops (e.g. using the stages Observe, Orient, Decide, Act) allow e.g. self-optimization, improvement of network and resource utilization, and automated service assurance and fulfilment.

4.2.6 Principle 06: Support for stateless management functions

The architecture supports inclusion of management functions that separate processing from data storage.

4.2.7 Principle 07: Resilience

Management services are designed to, as far as possible, provide and maintain configurable levels of their offered functionalities in face of degradation of the infrastructure and other management services. They also have the ability to return to normal operation when the degradation has been resolved.

4.2.8 Principle 08: Separation of concerns in management

In the ZSM framework, two different management concerns are distinguished: domain management and end-to-end service management across management domains. In practice, there can be a hierarchy of management domains.

Inside a management domain, resources and services based on these resources are managed. The complexity of domain resources can be abstracted from service consumers outside of the management domain.

The end-to-end cross-domain service management manages end-to-end services that span multiple management domains, and coordinates between management domains using orchestration. In this context, end-to-end services may span multiple management domains provided by different administrative entities (e.g. different network service providers or external partners).

Decoupling of management domains and end-to-end service management across domains avoids monolithic systems, allows to reduce the complexity of the overall service, and enables independent evolution of each management domain and of end-to-end management.

4.2.9 Principle 09: Service composability

Management services exposed by the management domains can be combined to create new management services.

4.2.10 Principle 10: Intent-based interfaces

Intent-based interfaces aim to hide complexity, technology- and vendor-specific details from the user by exposing high-level abstractions.

Intent-based interfaces express the consumer request(s) in a declarative form. A declarative form assumes the ability of e.g. the target system and its service producers to understand the request(s).

4.2.11 Principle 11: Functional abstraction

Functional abstraction is defined as the ability to generalize the behaviour of related entities, allowing to encapsulate details of multiple variants of those entities into a single one. Functional abstraction supports several other principles, such as replicability, scalability and composability.

4.2.12 Principle 12: Simplicity

The architecture has minimal complexity while still meeting the functional and non-functional requirements.

4.2.13 Principle 13: Designed for automation

The ZSM framework components and functionalities support the automation of network and service management and the integration of technology evolutions.

5 Architecture requirements

5.1 Introduction

Clause 5 defines architecture requirements applicable to the ZSM framework reference architecture. Architecture requirements are derived from the scenarios and requirements described in ETSI GS ZSM 001 [i.9] and define non-functional as well as functional needs to be satisfied by the architecture.

5.2 Non-functional requirements

5.2.1 General non-functional requirements

[NFunc-Gen-01] The ZSM framework reference architecture shall support the capability to achieve a specified level of availability of the ZSM framework.

[NFunc-Gen-02] The ZSM framework reference architecture shall enable management actions to comply with appropriate regulatory requirements.

[NFunc-Gen-03] The ZSM framework reference architecture shall enable energy efficiency where applicable.

[NFunc-Gen-04] The ZSM framework reference architecture shall be vendor, operator and service provider agnostic.

5.2.2 Non-functional requirements for cross-domain data services

[NFunc-CDS-01] The ZSM framework reference architecture shall support handling of different data services QoS requirements.

NOTE 1: QoS refers to for example the performance of data services in terms of throughput and delay.

[NFunc-CDS-02] The ZSM framework reference architecture shall enable interoperability of data services across different management domains.

[NFunc-CDS-03] The ZSM framework reference architecture shall enable interoperability of data services provided by the ZSM framework with data services outside of the ZSM framework.

[NFunc-CDS-04] The ZSM framework reference architecture shall support capabilities to process data within the pre-defined processing time.

NOTE 2: The term "pre-defined processing time" is strongly related to use cases and their criticality.

NOTE 3: Processing includes collection, aggregation, and correlation of data.

[NFunc-CDS-05] The ZSM framework reference architecture shall support capabilities to execute management tasks within the pre-defined processing time.

NOTE 4: The term "pre-defined processing time" is strongly related to use cases and their criticality.

[NFunc-CDS-06] The ZSM framework reference architecture shall support the capability to achieve high data availability.

5.2.3 Non-functional requirements for cross-domain service integration

[NFunc-Int-01] The ZSM framework reference architecture shall support integration of both new and legacy management functions.

[NFunc-Int-02] Integration of management services into the ZSM framework should not require changes to the management functions.

[NFunc-Int-03] The ZSM framework reference architecture shall support on-demand addition or removal of management services.

[NFunc-Int-04] The ZSM framework reference architecture shall support coexistence of different management service versions at the same time.

5.3 Functional requirements

5.3.1 General functional requirements

[Func-Gen-01] The ZSM framework reference architecture shall provide means to manage the resources and services (including RFS and CFS) exposed from management domains and CFS across multiple management domains.

NOTE 1: Resources include programmable networks including multi-layer networks, cloud-native and traditional virtualized network functions, and physical network functions.

[Func-Gen-02] The ZSM framework reference architecture shall support the cross-domain management of end-to-end services.

[Func-Gen-03] The ZSM framework reference architecture shall support adaptive closed-loop management.

NOTE 2: It is possible that closed-loops span multiple management domains.

[Func-Gen-04] The ZSM framework reference architecture shall support bounding the automated decision-making mechanisms by rules and policies set by the operator.

[Func-Gen-05] The ZSM framework reference architecture shall support hiding the management complexity of management domains and end-to-end services.

[Func-Gen-06] The ZSM framework reference architecture shall support all technology domains necessary to realize an E2E service.

NOTE 3: The typical examples of technology domains are but not limited to access network, transport network, core network and cloud.

[Func-Gen-07] Management services provided by the ZSM management domains shall support automation of operational lifecycle management functions as applicable to the resources and services (including RFS/CFS).

[Func-Gen-08] The ZSM framework reference architecture shall define standard interfaces within the management domains so that their management can be fully automated.

[Func-Gen-09] The ZSM framework reference architecture shall support access control to services exposed by the management domains.

[Func-Gen-10] The ZSM framework reference architecture shall support open interfaces.

[Func-Gen-11] The ZSM framework reference architecture shall support management of end-to-end services that cross boundaries between different domains.

5.3.2 Functional requirements for data collection

[Func-DColl-01] The ZSM framework reference architecture shall support functionality that enables collecting up-to-date data.

NOTE 1: The term "up-to-date" refers to the data collection period(s).

NOTE 2: Collected data include, but are not limited to:

- telemetry data related to infrastructure resources and services;
- logs from system, infrastructure and application software entities;
- labelled training data for machine learning.

[Func-DColl-02] The ZSM framework reference architecture shall support functionality that enables storing collected data (or to steer their appropriate storage).

[Func-DColl-03] The ZSM framework reference architecture shall support functionality that enables the common access to the collected up-to-date data across management domains.

[Func-DColl-04] While providing common access to the collected data, the ZSM framework reference architecture shall support the capability of enforcing data governance.

[Func-DColl-05] The ZSM framework reference architecture shall support functionality that enables aggregating the collected data cross-domain, and (pre-) processing/filtering the collected data.

[Func-DColl-06] The ZSM framework reference architecture shall support different degrees of cadence, velocity and volume of data collection.

[Func-DColl-07] The ZSM framework reference architecture shall support different degrees of cadence, velocity and volume of data sharing.

EXAMPLE: While data may be consumed locally inside a management domain with a high sampling frequency, entities in other management domains may just need aggregate data, or a data stream with a lower sampling frequency.

[Func-DColl-08] The ZSM framework reference architecture shall support the capability to manage the distribution of collected data and keep distributed data consistent.

[Func-DColl-09] The ZSM framework reference architecture shall support functionality to provide data to the data consumer according to the data consumer's requirements (e.g. relevant data, relevant time, relevant form).

[Func-DColl-10] The ZSM framework reference architecture shall support attaching metadata to collected data.

NOTE 3: This enables closed-loop machine interpretation of the collected data.

5.3.3 Functional requirements for cross-domain data services

[Func-CDS-01] The ZSM framework reference architecture shall support cross-domain data services.

[Func-CDS-02] The ZSM framework reference architecture shall support functionality that enables the separation of data storage and data processing.

[Func-CDS-03] The ZSM framework reference architecture shall support functionality that enables the sharing of data within the ZSM framework reference architecture.

[Func-CDS-04] The ZSM framework reference architecture shall support functionality that enables data recovery in an automated manner.

[Func-CDS-05] The ZSM framework reference architecture shall support functionality that enables to manage the consistency of redundantly-stored data in an automated manner.

[Func-CDS-07] The ZSM framework reference architecture shall support functionality that enables data service failover in an automated manner.

[Func-CDS-08] The ZSM framework reference architecture shall support functionality that enables automated overload handling of data services.

[Func-CDS-09] The ZSM framework reference architecture shall support capabilities that allow logically centralized storage and processing of data, as well as the automatic provisioning of these capabilities.

[Func-CDS-10] The ZSM framework reference architecture shall support functionality that enables automated policy-based processing of data.

[Func-CDS-11] The ZSM framework reference architecture shall support functionality that enables the processing of several data services with different data types (e.g. structured and unstructured data) in an automated manner.

5.3.4 Functional requirements for cross-domain service integration and access

[Func-SrvIA-01] The ZSM framework reference architecture shall support functionality that enables the registration of the management services provided.

[Func-SrvIA-02] The ZSM framework reference architecture shall support functionality that enables the discovery of the management services provided.

[Func-SrvIA-03] The ZSM framework reference architecture shall support functionality that provides information about the means to access a discovered service.

[Func-SrvIA-04] The ZSM framework reference architecture shall support functionality that facilitates synchronous and asynchronous communication between service producers and service consumers.

[Func-SrvIA-05] The ZSM framework reference architecture shall support functionality that facilitates the indirect invocation of the management services.

[Func-SrvIA-06] The ZSM framework reference architecture shall not prevent the direct invocation of discovered management services by the service consumer.

5.3.5 Functional requirements for lawful intercept

[Func-LI-01] The ZSM framework reference architecture shall support Lawful Intercept (LI) undetectability.

[Func-LI-02] The ZSM framework reference architecture shall support the capability to prevent a lawful interception from being disrupted, i.e. lawful intercept needs to continue despite any service or network adjustments performed by the ZSM framework.

5.4 Security requirements

This clause defines security requirements. Management data, as well as data related to management functions such as logs are covered under the general term "data" used in these requirements.

[Sec-01] The ZSM framework reference architecture shall support functionality that enables security of data at rest, in transit and in use, infrastructure resources, managed services and management functions.

[Sec-02] The ZSM framework reference architecture shall support confidentiality of management data at rest, in transit and in use.

[Sec-03] The ZSM framework reference architecture shall support integrity of data at rest, in transit and in use.

[Sec-04] The ZSM framework reference architecture shall support integrity of managed services and management functions.

[Sec-05] The ZSM framework reference architecture shall support the capability to ensure availability of data, infrastructure resources, managed services and management functions, in so far as security measures to handle availability threats are concerned.

[Sec-06] The ZSM framework reference architecture shall support functionality that enables privacy of personal data, including privacy-by-design and privacy-by-default mechanisms.

[Sec-07] The building blocks of the ZSM framework reference architecture shall include the necessary safeguards and features to ensure security of operation as well as data protection appropriate to mitigate the risks.

[Sec-08] The ZSM framework reference architecture shall allow authorization of service access by authenticated service consumers.

[Sec-09] The ZSM framework reference architecture shall support the capabilities to automatically apply appropriate security policies according to the compliance status of individual management services concerning the security requirements (expressed as certification by corresponding authorities).

[Sec-10] The ZSM framework reference architecture shall support capabilities for automated attack/incident detection, identification, prevention, and mitigation.

[Sec-11] The ZSM framework reference architecture shall support capabilities to audit/supervise AI/ML decisions against security and privacy criteria to prevent the proliferation of vulnerabilities and attacks.

6 Reference architecture

6.1 General architecture overview

6.1.1 Introduction

The ZSM framework reference architecture follows the industry trend to move away from tightly coupled management systems to more flexible sets of management services, for instance defined by TM Forum as part of the Open Digital Architecture [i.6] or by 3GPP in their service-based management architecture [i.7].

The ZSM framework reference architecture defines a set of architectural building blocks that collectively enable construction of more complex management services and management functions using a consistent set of composition and interoperation patterns.

Logically, the ZSM framework is composed of distributed management and data services, organized into management domains and integrated via an integration fabric. The integration fabric is also used to enable management service consumption, communication, and integration with 3rd party management systems. The cross-domain data service allows data sharing across domains. All management services provide a set of capabilities for their consumption.

The ZSM framework reference architecture provides means to build and compose loosely-coupled management functions that offer management services and collectively deliver end-to-end and domain-specific capabilities for zero-touch management of network services and infrastructure. To offer their services, management functions provide management service end-points used for management service invocation and communication.

6.1.2 Architectural building blocks

6.1.2.1 Management services

A "management service" is the most fundamental building block, used as part of the ZSM framework reference architecture.

Management services offer capabilities for consumption by service consumers via standardized management service end-points.

Capabilities of a given management service collectively define its function with respect to entities being managed by it. Service capabilities may be offered for consumption by multiple service consumers. One or more service capabilities can be mapped to one or more service end-points.

All management services offer a consistent set of capabilities for invocation and communication purposes. This enables a high degree of automation and continuity, when it comes to interactions between management domains.

Offered management services can be combined into new management services. In the composition hierarchy, each higher layer supports management services with a higher abstraction and a broader scope.

In order to provide their capabilities, management service producers may be required to interact with infrastructure resources: directly, via their management interfaces, or indirectly, by consuming other management services via their service end-points.

6.1.2.2 Management functions

Management functions are entities that produce and/or consume management services. A management function is said to be a "service producer" if it produces (offers) certain capabilities of one or more management services. A management function is said to be a "service consumer" if it consumes certain capabilities of one or more management services.

A given management function can either be a management "service producer", a management "service consumer", or both at the same time.

6.1.2.3 Management domains

Management domains are used to partition administrative responsibilities and to create "separation of concerns" within a given ZSM deployment, based on various deployment, functional, operational and governance constraints. Typically, such constraints reflect the need for management consistency across a grouping of related resource facing services and/or resources contained within the management domain based on similarities or relationships such as services using the same set of infrastructure resources, types of infrastructure resources, technology or ownership.

Management domains federate together management services with capabilities needed to manage resource-facing services or resources within a given domain. A management domain may be further split into multiple "subordinate" management domains, if additional separation of concern is needed. Optionally, management domains may also provide means of lifecycle management for management services they contain.

Some management services can be restricted to be consumed by authorized consumers inside the management domain only (internal services, i.e. their external visibility is optional which implies their support in the domain is also optional), whereas others are required to always be available for consumption by authorized consumers inside and outside the management domain (exposed services, i.e. external visibility is mandatory). External visibility can also be mandatory only under certain conditions, and optional otherwise (conditional services).

Each management domain manages one or more entities, such as infrastructure resources and/or resource-facing services associated with the management domain. Infrastructure resources can be physical (e.g. physical network functions (PNFs)), virtual (e.g. virtualized network functions (VNFs) or software-based services) and/or cloud based (e.g. "X-as-a-service" (XaaS) resources).

Each management domain provides one or more service capabilities, by exposing or consuming service end-points.

A resource-facing or customer-facing service managed by a management domain can consume further resource-facing or customer-facing services managed by other management domains, as needed (*managed* services). In that case, the management domain which manages the consuming service also consumes *management* services from the management domains that manage the consumed resource-facing or customer-facing services. Management services are in the scope of the present document, whereas managed services are not.

Clause 6.5 specifies the management domain and the related management services in detail.

6.1.2.4 The end-to-end (E2E) service management domain

The E2E service management domain is a special management domain that provides end-to-end management of customer-facing services, composed from the customer-facing or resource-facing services provided by one or more management domains. The E2E service management domain does not directly manage infrastructure resources.

Clause 6.6 specifies the end-to-end service management domain and the related management services in detail.

6.1.2.5 Integration fabric

The integration fabric enables interoperation and communication between management functions within and across management domains, including the registration, discovery and invocation of management services and the communication between management functions. It is a special management function that both offers a set of management service integration, interoperation and communication capabilities, and consumes capabilities provided by management services within and across management domains.

Clause 6.3 specifies the integration fabric in detail. The service consumption patterns illustrated in annex B are supported by the integration fabric.

6.1.2.6 Data services

Data services enable consistent means of shared management data access and persistence by authorized consumers across management services within or across management domains. They also eliminate the need for management functions to handle their own data persistence, thereby allowing to separate data persistence from data processing.

Clause 6.4 specifies the data services in detail.

6.2 Architecture diagram

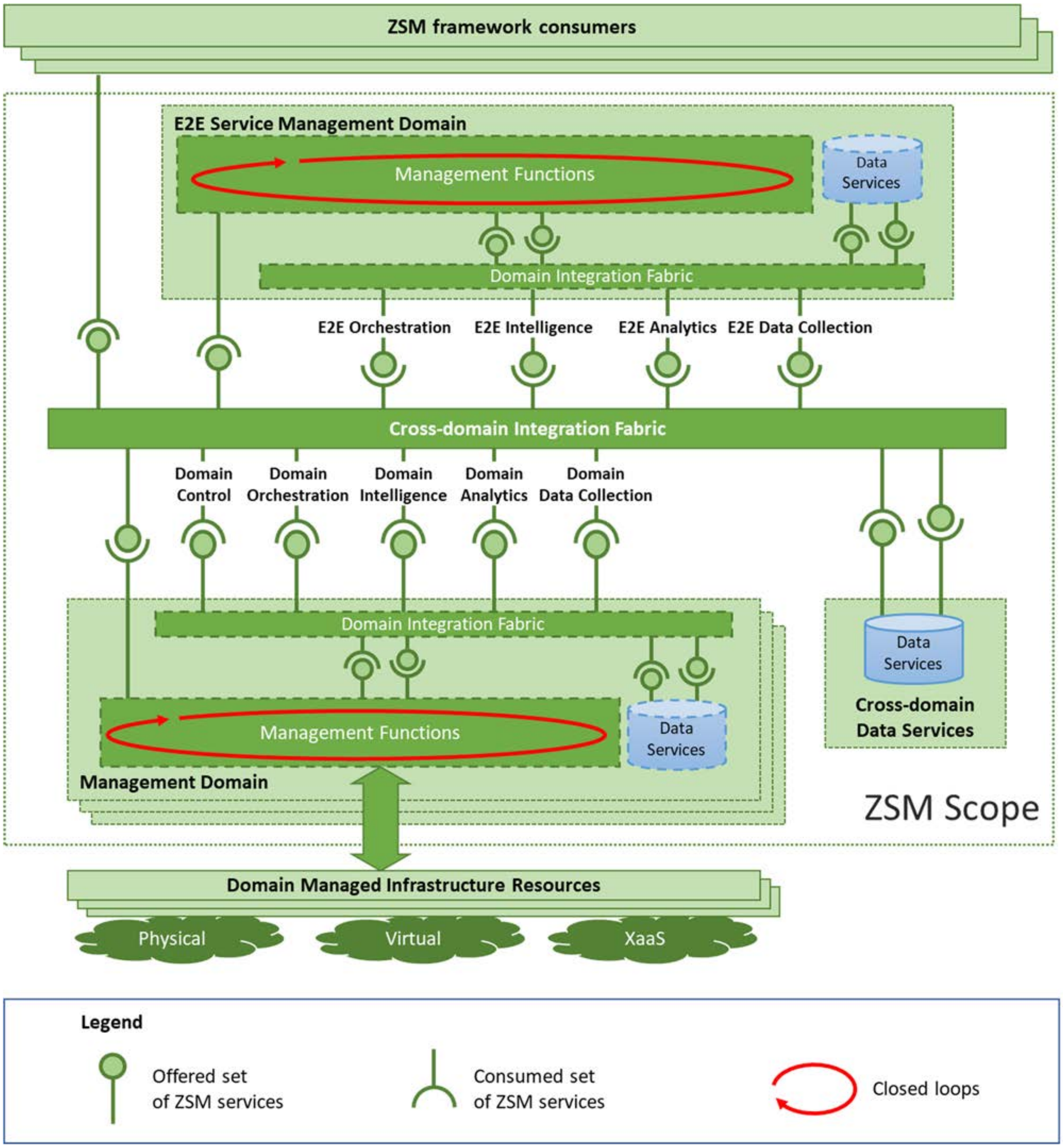


Figure 6.2-1: ZSM framework reference architecture

Figure 6.2-1 depicts the ZSM framework reference architecture. Every management domain, as well as the E2E service management domain, provides a set of ZSM service capabilities by management functions that expose and/or consume a set of service end-points. The cross-domain integration fabric facilitates providing capabilities and accessing end-points cross-domain. Some services are only provided and consumed locally inside the management domain. Each of the logical groups of management services contains services with related functionality. The grouping does not imply a particular implementation.

Whereas ETSI ZSM normatively defines the set of ZSM services visible outside a management domain, it only provides options for the management domain's internal composition. More details are defined in clauses 6.5.1 and 6.6.1.

The domain integration fabric is a logical entity which represents one or more management functions responsible for controlling exposure of services beyond domain boundaries and for controlling access to the management services exposed by the domain. The domain integration fabric may also provide further integration services to the management functions inside the management domain.

NOTE: "Logical entity" means that the ZSM specification defines the optional and mandatory services provided by a management domain, however, it does not prescribe how these services are structured into management functions.

In addition to providing access to ZSM services, a management domain and the E2E service management domain can also consume ZSM services provided by other management domains. ZSM framework consumers (such as digital store fronts that provide automation of consumer and business management, BSS applications, web portals, another ZSM framework instance, or even human users via additional user interfaces) can consume ZSM services provided by the E2E service management domain and the management domains.

Data services may be provided and consumed inside a management domain including the E2E service management domain. In addition, the ZSM framework reference architecture shall provide cross-domain data services that can be consumed by the management domains, the E2E service management domain and the ZSM framework consumers. Also, the cross-domain data services can consume services provided by the management domains and the E2E service management domain.

When managing infrastructure resources, a management domain interfaces with these resources by management interfaces provided by the resources. Those interfaces are out of scope of the ZSM framework reference architecture.

6.3 Integration fabric

6.3.1 Overview

The integration fabric provides a set of ZSM services that facilitate the communication and interoperation of management functions with respect to the offered and consumed management services. The services of the integration fabric include the following:

- registration/de-registration of management services;
- discovery of the registered management services and the means to access them;
- means of supporting the invocation of management services;
- means of supporting synchronous and asynchronous communication.

The integration fabric can be realized as one or more management functions that collectively provide the services and capabilities as described below.

Providing and consuming services use particular patterns. In the scope of the present document, the request-response pattern and the publish/subscribe pattern are supported. See annex B for an illustration.

6.3.2 Provided management services

6.3.2.1 Management services registration service

This service handles the addition and removal of management services and management functions to and from the set that can be discovered using the management services discovery service. For each management service, the list of supported capabilities is included as part of the registration.

The service is further defined in table 6.3.2.1-1.

Table 6.3.2.1-1: Service definition

Service name		Management services registration service.
Service capabilities		
	Manage service registrations (M)	Manage (create, read, update, delete, list) registrations of management services and their supported capabilities. Create, read, list, delete shall be supported whereas update may be supported.

6.3.2.2 Management services discovery service

This management service enables the consumer to discover the available management services and their supported capabilities. In the cross-domain integration fabric, this is used to discover services available from ZSM management domains. This service provides information that allows service consumers to directly invoke discovered services.

The service is further defined in table 6.3.2.2-1.

Table 6.3.2.2-1: Service definition

Service name		Management services discovery service.
Service capabilities		
	Query service list (M)	Enable authorized consumers to query the list of currently available management services.
	Get service info (M)	Get the supported capabilities and specific service related information, e.g. APIs for the service. Filtering criteria may be specified.
	Provide notifications about service list changes (M)	Notify authorized consumers about the changes in the list of currently available management services and their supported capabilities.

6.3.2.3 Management communication service

This service is provided by the integration fabric. It enables communication between two or more management functions using a set of communication channels. The content of the communication includes event notifications, streams and data objects that are generated by the service producer asynchronously and can be provided synchronously (pull) or asynchronously (push) to the service consumer. The exact delivery mode and mechanism is left for the future stages of specification.

Service producers can select one of the existing channels or create new channels for communication. When creating new channels, the service producer can specify channel properties such as QoS, content type, restrictions, access control, policies, acknowledgement, and available communication styles. Service consumers can subscribe to one or more communication channels. A channel facilitates the transfer of content from all producers that publish content in the channel to all consumers that have subscribed to that channel. As part of the subscription, service consumers can specify what communication content they are interested in (filtering criteria) and how it is delivered to them (e.g. synchronous (pull) or asynchronous (push)).

The management communication service provides a set of capabilities (subscription management, channel management and delivery of management data) to a service consumer.

Service producers offer the capability to provide content which is consumed by the integration fabric as part of providing the communication service. The integration fabric basically re-exposes that consumed capability towards the consuming management function, using one of the defined communication channels. Based on this service model, the actual communication pattern (such as push, pull) of how the data are consumed from the producers and delivered via the communication channels are subject to later, more detailed stages of specification.

A channel shall exist before content can be published and subscriptions can be made to the channel.

The service is further defined in table 6.3.2.3-1.

Table 6.3.2.3-1: Service definition

Service name		Management communication service.
Service capabilities		
	Manage channels (M)	Manage (create, read, update, delete, list) the communication channels. "create", "read", "delete" and "list" shall be supported, and "update" may be supported. "create" and "update" allow to manage parameters associated with the channel, such as QoS, content type, event category, communication pattern (such as push, pull), acknowledgements, restrictions, access control, delivery guarantees and subscription policies.
	Manage subscriptions (M)	Manage (create, read, update, delete, list) the consumer's subscriptions. Filters may be specified.
	Provide data (M)	Forwards received data (such as event notifications, streams) to subscribers via a communication channel.
	Receive data (M)	Accept data for forwarding to subscribers via a communication channel.

6.3.2.4 Management service invocation routing service

This service enables indirect invocation of management services by authorized service consumers via the integration fabric with optional delegation of service discovery. It also manages invocation rules (e.g. service call routing rules, service version rules, etc.). During indirect invocations, the integration fabric is responsible for optionally determining service/management function existence, obtaining service producer location information, invoking the service, and delivering any invocation results to the service consumer.

The service is further defined in table 6.3.2.4-1.

Table 6.3.2.4-1: Service definition

Service name		Management service invocation routing service.
Service capabilities		
	Manage routing rules (M)	Manage (create, read, update, delete, list) communication rules between service consumers and service producers based on e.g. service type, affinity policies, load balancing, failover, etc.
	Discover and invoke service (O)	Enable service consumer to invoke via the integration fabric a management service where the service producer is discovered by the integration fabric. Results of the service invocation are delivered by the integration fabric to the service consumer. See note 1.
	Invoke service (M)	Enable service consumer to invoke via the integration fabric a management service where the actual service end-point to access is selected by the integration fabric. Results of the service invocation are delivered by the integration fabric to the service consumer. See note 2.
NOTE 1: This means that service discovery and service invocation are combined. When consuming this capability, the consumer has to provide information needed to discover the service and information needed to invoke the service. The integration fabric discovers the service producer, the end-point and further interface details. It adapts the service invocation accordingly and routes the invocation to the selected end-point. NOTE 2: This means that service invocation is separate from service discovery. When consuming this capability, the consumer has to provide information needed to invoke the service. The integration fabric selects the end-point to access and routes the service invocation there.		

6.3.2.5 Management capability exposure configuration service

The management capability exposure configuration service is used for the configurations of entitlements of service consumers to ZSM services, capabilities or end-points externally visible from a management domain or the E2E service management domain.

Based on the entitlements configured by this service, the domain integration fabric of the respective management domain or the E2E service management domain provides access to service consumer specific sets of management services exposed by the domain.

The service is further defined in table 6.3.2.5-1.

The entitlements to exposed ZSM services, capabilities, end-points and data provided by management function can change from time to time. The exposure service may also have a capability to allow consumers external to the domain to request changes in the entitlements.

Table 6.3.2.5-1: Service Capabilities

Service name		Management capability exposure configuration service.
Service capabilities		
	Provide notification of changes in entitlements (O)	Provide notification if there are changes in the entitlements for a specific consumer to access exposed ZSM services, capabilities, end-points or data provided by management function (see note).
	Configure entitlements to exposed services (M)	Configure entitlements for a specific consumer to access exposed ZSM services, capabilities, end-points or data provided by management function. This capability shall be supported but need not be externally visible.
	Process external requests for change in entitlements (O)	Enable an external authorized consumer to request modification in entitlements for a specific consumer to access ZSM services, capabilities, end-points or data provided by management function (see note).
NOTE: The external visibility of this capability is mandatory if the capability is supported.		

6.3.3 Cross-domain integration fabric

Any ZSM deployment shall contain management functions that provide in a cross-domain fashion management services as defined in table 6.3.3-1, indicating for each service whether its support by the cross-domain integration fabric is OPTIONAL or MANDATORY.

Table 6.3.3-1: Support of services offered by the cross-domain integration fabric

Service name	Clause	Support
Management services registration service	6.3.2.1	MANDATORY
Management services discovery service	6.3.2.2	MANDATORY
Management communication service	6.3.2.3	MANDATORY
Management service invocation routing service	6.3.2.4	MANDATORY
Management capability exposure configuration service	6.3.2.5	OPTIONAL

6.3.4 Domain integration fabric

A management domain including the E2E service management domain shall contain management functions that control access to the management services exposed by the domain, and that further provide management services as defined in table 6.3.4-1, indicating for each service whether its visibility outside the domain is OPTIONAL or MANDATORY. Services not externally visible need not be supported.

Table 6.3.4-1: Support and external visibility of services offered by the domain integration fabric

Service name	Clause	External visibility
Management services registration service	6.3.2.1	OPTIONAL
Management services discovery service	6.3.2.2	OPTIONAL
Management communication service	6.3.2.3	OPTIONAL
Management service invocation routing service	6.3.2.4	OPTIONAL
Management capability exposure configuration service	6.3.2.5	MANDATORY

6.4 Data services

6.4.1 Overview

Data services provide means of data persistence and enable data sharing with authorized consumers within and across management domains, subject to information security and data governance regulations. Data services also enable abstraction of data persistence and data processing actions from the management functions. This enables stateless management functions and eliminates the need to handle data persistence and processing on per-function basis.

The data services support different types of storage mechanisms and database technologies for different purposes and allow the explicit or automatic selection of a suitable storage mechanism/database type for each data store.

Automation needs seamless and timely access to consistent and current management data, within a domain as well as across domains. Collected data should be handled within the domain where it was produced or by a designated entity. Data should be made available to authorized consumers, within the originating domain and to services in other domains, subject to access control and information security policies. A service that offers data to multiple consumers is responsible for providing the level of data consistency needed by each consumer. The architecture does not mandate how or where data is stored.

Management data types stored in the data services may include, but are not limited to:

- managed entities' performance monitoring data (e.g. performance counters);
- managed entities' assurance data (e.g. performance/fault alarm events);
- managed entities' trace data (e.g. packet capture data);
- managed entities' configuration data;
- managed entities' miscellaneous log data;
- network/service topology data;
- network/service inventory data.

6.4.2 Provided management services

6.4.2.1 Data store management service

The data store management service allows to discover the available data persistence services, to create and delete data stores, to define metadata and to enforce data governance by means of authorization and access control.

The service is further defined in table 6.4.2.1-1.

Table 6.4.2.1-1: Service definition

Service name		Data store management service.
Service capabilities		
	Enumerate data store types (O)	Enumerate the available data store types supported by the data persistence services, e.g. different database technologies or storage techniques.
	Manage data stores (M)	Manage (create, read, update, delete, list) data stores. The type of the data store created may be explicitly requested based on a discovered data store type or may be chosen by the service based on policies and metadata.
	Manage data access and authorization rights (M)	Manage (create, read, update, delete, list) access and authorization rights for data stores or parts thereof.
	Authorize data access (M)	Provide authorization to service consumers to access a data store or parts thereof.
	Manage metadata (M)	Manage (create, read, update, delete, list) metadata for a data store.
	Define data mapping policies (O)	Define policies that allow to select the data store for a data item to be stored based on meta data and characteristics of the data.
	Manage data confidentiality and integrity (M)	Manage the mechanisms and configurations needed to ensure data confidentiality (optional) and integrity (mandatory), including support for authentication. Manage keys and credentials and their storage.

6.4.2.2 Data persistence services

Data persistence services support persistent storage of data and events, possibly using a range of different database technologies (e.g. NoSQL databases, time series databases and graph/topology databases). Streaming data typically generate huge data volumes and hence benefit from highly optimized Big Data storage solutions. The stored data can be exposed to authorized consumers, including consumers outside the management domain in which the data services reside, respecting the applicable data protection and privacy measures.

The service is further defined in table 6.4.2.2-1.

Table 6.4.2.2-1: Service definition

Service name		Data persistence services (see note).
Service capabilities		
	Store data (M)	Allows to store (write) data to a data store. This includes creation and update of different kinds of data. The data persistence services are also able to capture and store data that are streamed. Data store selection may be explicit as part of the request or may be left to the system based on mapping policies and characteristics of the data.
	Query data (M)	Query (read) data from a data store.
	Delete data (M)	Remove stored data from a data store.
	Provide notifications about data changes (O)	Provide notifications about changes in stored data.
NOTE: There may be different types of data stores for different characteristics/types of stored data. The available types can be enumerated using the data store management service.		

6.4.2.3 Data processing service

The data processing service provides a generic execution environment (workflow and task management) for processing of data. It allows performing data analysis and data processing based on provided processing instructions.

EXAMPLE: Possible use case: analysis of very large data sets such as "Big Data".

The service is further defined in table 6.4.2.3-1.

Table 6.4.2.3-1: Service definition

Service name		Data processing service.
Service capabilities		
	Analyse data (M)	Analyse stored data and make the result of the analysis available. The analysis is based on processing instructions that can be pre-stored or provided by the service consumer when consuming the service.
	Manage processing instructions (O)	Manage (create, read, update, delete, list) processing instructions.

6.4.3 Cross-domain data services

The ZSM framework reference architecture includes data services that enable sharing of management data across multiple management domains. Any ZSM deployment shall contain such cross-domain data services, i.e. a management function or set of management functions that provide in a cross-domain fashion the management services defined in clause 6.4.2.

The cross-domain data services receive management data from the management domains including the E2E service management domain in the ZSM framework. The data is stored in a logically centralized place (actual data placement is implementation-specific). Various authorized consumers can request data from the cross-domain data services e.g. to access data originating from another management domain as well as to achieve E2E global optimization. Also, data processing tasks can be run directly on the stored data, requested by service consumers e.g. those in domain intelligence. That means, the cross-domain data services support the separation of data storage and data processing and allow sharing of data within the ZSM framework reference architecture. Data in the cross-domain data services is generally used to achieve different aspects of automated E2E optimization (e.g. routing optimization in the managed domains, different levels of resource optimization for each managed network service, etc.) as well as automation of management and operation of the whole ZSM framework.

Any ZSM deployment shall contain management functions that provide in a cross-domain fashion management services as defined in table 6.4.3-1, indicating for each service whether its support by the cross-domain integration fabric is OPTIONAL or MANDATORY.

Table 6.4.3-1: Support of services offered by the cross-domain data services

Service name	Clause	Support
Data store management service	6.4.2.1	MANDATORY
Data persistence services	6.4.2.2	MANDATORY
Data processing service	6.4.2.3	MANDATORY

6.4.4 Domain data services

A management domain including the E2E service management domain may contain management functions that provide management services as defined in table 6.4.4-1, indicating for each service whether its visibility outside the domain is OPTIONAL or MANDATORY. Services not externally visible need not be supported.

Table 6.4.4-1: Support and external visibility of services offered by the domain data services

Service name	Clause	External visibility
Data store management service	6.4.2.1	OPTIONAL
Data persistence services	6.4.2.2	OPTIONAL
Data processing service	6.4.2.3	OPTIONAL

6.5 Management domain

6.5.1 Overview

Within each management domain, management services are provided. Each service is provided via a set of end-points by a service producer.

Some management services can be restricted to be consumed by authorized consumers inside the management domain only (internal services), whereas others are available for consumption by authorized consumers inside and outside the management domain (exposed services). See clause 6.1.2.3 for a more detailed description.

6.5.2 Domain data collection

6.5.2.1 Description

The domain data collection services monitor the managed entities and consumed managed services and provide e.g. live performance and fault data to support closed-loop automation, which needs to be able to verify how the network reacts to changes (such as optimization).

As part of the closed loops at management domain level, domain data collection services interact with domain analytics and domain intelligence services, but also with domain orchestration services and domain control services as needed to trigger actions or changes to the managed entities of the management domain.

If a service managed by the current management domain contains (by way of composition) services managed by another management domain, service producers in the current management domain that provide domain data collection services can also consume domain data collection services from the other management domain that manages the contained service. If the current management domain manages services that are consumed by services managed by another management domain including the E2E service management domain, the domain data collection services provided by the current management domain can be consumed by that other management domain.

Domain data collection services include services that process incoming events, data objects and other inputs related to faults, performance and security from the underlying managed entities and consumed managed services and provide related data and notifications. They can also aggregate the information and derive e.g. key performance indicators.

6.5.2.2 Provided management services

6.5.2.2.1 Event notification services

Various event notification services can generate discrete asynchronous event notifications to report information about state changes and issues in the managed services and resources in a timely manner. The event notifications are provided to subscribed consumers using the management communication service of the integration fabric.

The standard capabilities of such event notification services are further defined in table 6.5.2.2.1-1 as a generic event notification service.

Table 6.5.2.2.1-1: Capabilities of a generic event notification service

Service name		Generic event notification service.
External visibility		CONDITIONAL (see note).
Service capabilities		
	Configure monitoring (O)	Configure what information is provided.
	Provide notifications (M)	Provide event notifications.
NOTE: It depends on the actual event notification service whether the external visibility of this service is MANDATORY or OPTIONAL.		

Actual specific event notification services have the same set of capabilities as the generic event notification service but differ in the type of event notifications they generate and the actual configuration. Table 6.5.2.2.1-2 lists specific event notification services defined by the ZSM framework. This set of services is extensible.

Table 6.5.2.2.1-2: Specific event notification services defined by the ZSM framework

Service name	ExtVis	Service description	Events reported
Fault events service	M	The fault events service provides notifications about abnormal system states (fault events) originating from the infrastructure resources and consumed services.	Fault events
Security events service	M	The security events service provides notifications about security-related events.	Security events
Performance events service	M	The performance events service provides notifications about events related to monitored performance conditions (e.g. if a threshold was crossed) and allows to configure the performance conditions to monitor.	Events related to monitored performance conditions

NOTE: Besides specific event notification services that can be derived from the generic event notification service as they have the same set of capabilities, additional event notification services that have different capabilities than the generic service can be defined separately.

6.5.2.2.2 Performance measurements streaming service

The performance measurements streaming service provides time series of performance measurements originating from the infrastructure resources and network services in a streaming fashion (i.e. once one or more measurements have been taken, provide a message related to the measurement(s)), using the management communication service of the integration fabric. The performance measurements streaming service also allows to configure control information (e.g. subscription, data to be measured including filters and how to provide the collected performance data). In addition, the performance measurement streaming service offers information about the available measurements (types of available measurements, including KPIs).

The service is further defined in table 6.5.2.2.2-1.

Table 6.5.2.2.2-1: Service definition

Service name		Performance measurements streaming service.
External visibility		CONDITIONAL (see note).
Service capabilities		
	Provide streaming measurements (M)	Provide streams of measured data.
	Configure measurements (O)	Configure the measurements to be taken.
	Get measurements list (M)	Obtain the list of measurements (e.g. including KPIs) supported by the management domain.
	Manage subscriptions to measurement changes (C)	Manage (create, read, update, delete, list) subscriptions to any changes of measurement list. Only available if "Provide notifications" is supported.
	Provide notifications (O)	Provide notifications about changes of the measurement list.
NOTE: At least one of Performance measurements streaming service and performance measurements collection service shall be provided by the management domain.		

6.5.2.2.3 Performance measurements collection service

The performance measurements collection service provides time series of performance measurements originating from the infrastructure resources and network services in a batch fashion. During time intervals of configurable length, the measurements collection service collects data originating from the infrastructure resources and provides these data in batches to authorized consumers (such as producers of other management services in the management domains including the E2E service management domain and to the cross-domain data services). The performance measurements collection service also allows listing the supported measurements. The performance measurements collection service also allows to configure control information (e.g. subscription, data to be reported including filters and how to collect and provide the performance data).

The service is further defined in table 6.5.2.2.3-1.

Table 6.5.2.2.3-1: Service definition

Service name		Performance measurements collection service.
External visibility		CONDITIONAL (see note).
Service capabilities		
	Get batch measurements (M)	Obtain batches of collected measurements.
	Provide batch availability notifications (O)	Provide notifications that a collected batch is available.
	Configure batch measurements (O)	Configure the measurements to be taken
	Get measurements list (M)	Obtain the list of measurements supported by the MD for collection (e.g. including KPIs).
	Manage subscriptions to measurement list changes (C)	Manage (create, read, update, delete, list) subscriptions to any changes of measurement list. Only available if "Provide notifications" is supported.
	Provide measurements list notifications (O)	Provide notifications about changes of the measurement list.
NOTE: At least one of Performance measurements streaming service and performance measurements collection service shall be provided by the management domain.		

6.5.2.2.4 Log collection service

Logs from managed resources and services contain information about system running, operation and security events. This information can be analysed e.g. for troubleshooting, anomaly detection, or for other decision making in network and service management automation. The information collected by the log collection service enables health, security and performance monitoring of software entities that do not produce traditional performance measurements or alarms. As the log formats can vary widely, the data optimization service offers capabilities for pre-processing of the logs to provide clean, structured and aggregated data.

The log collection service provides logs originating from the managed entities in a streaming fashion (i.e. once one or more log lines have been produced, the log lines are provided), using the management communication service of the integration fabric. The information provided includes at least information about the managed entity producing the log, the timestamp of producing the log and the content of the log.

The service is further defined in table 6.5.2.2.4-1.

Table 6.5.2.2.4-1: Service definition

Service name		Log collection service.
External visibility		OPTIONAL.
Service capabilities		
	Provide log information (M)	Provide log data, i.e. a block of one or more log lines.
	Configure log collection (O)	Configure log collection rules.
	Query logs (M)	Enable a consumer to query existing logs.
	Manage subscriptions to log information (O)	Manage (create, read, update, delete, list) subscriptions to log information.

6.5.3 Domain analytics

6.5.3.1 Description

The domain analytics services provide domain-specific insights and generate domain-specific predictions based on data collected by domain data collection services and other data (e.g. data collected by other domains or stored in data services).

6.5.3.2 Provided management services

6.5.3.2.1 Analytics services

Various analytics services can generate aggregated data and derive insights from the collected data, possibly considering additional information such as topology.

The standard capabilities of analytics services are further defined in table 6.5.3.2.1-1 as a generic analytics service.

Table 6.5.3.2.1-1: Capabilities of a generic analytics service

Service name		Generic analytics service.
External visibility		CONDITIONAL (see note 1).
Service capabilities		
	Manage subscriptions (O)	Manage (create, read, update, delete, list) subscriptions to analysis results generated by this particular analytics service. Filters may be specified.
	Configure analytics (O)	Configure how analysis results are derived.
	Provide analysis results (C)	Provide notifications with analysis results. This capability is applicable to services which generate analysis results asynchronously (see note 2).
	Request analysis result (C)	Trigger an analytics process and obtain the result. This capability is applicable to services that need an explicit trigger to start (see note 2).
NOTE 1: It depends on the actual analytics service whether the external visibility of this service is MANDATORY or OPTIONAL. NOTE 2: At least one of these capabilities shall be supported.		

Actual specific analytics services have the same set of capabilities as the generic analytics service but differ in the type of analysis result they generate, the analysis they perform and the actual configuration. Table 6.5.3.2.1-2 lists specific analytics services that are defined by the ZSM framework. This set of services is extensible.

Table 6.5.3.2.1-2: Specific analytics services defined by the ZSM framework

Service name	ExtVis	Analysis performed	Analysis result
Anomaly detection service	O	The anomaly detection service provides capabilities to detect anomalous conditions using the collected fault, performance, usage and configuration data about the managed entity. Such conditions might be, for example, security violations/anomalies, localized/short term fault conditions or localized/short term service capacity degradations that can occur despite the service KPIs indicate that the service is working properly, and that can indicate the need for healing or resource scaling. If any anomalies are detected, the results can trigger domain intelligence to make appropriate decisions or to make the data available to other analytics for further analysis.	Notifications related to detected anomalies.
Deployed AI model performance evaluation service	O	The deployed AI model performance evaluation service allows determining the level of performance of deployed AI models and detecting e.g. performance degradation (AI models are probabilistic systems that may suffer performance degradation over time and need to be retrained), sudden performance drop, irregular performance, etc. The deployed AI model performance evaluation service can be used for instance by the deployed AI model assessment service to decide on the most appropriate actions to perform on the deployed AI models.	Notifications related to performance evaluation of deployed AI models.
Proactive incident analysis service	O	Collection and classification of data, insights and input from other services, e.g. anomaly detection service, for the purpose of taking proactive measures. Analysis of incident patterns and root cause analysis to produce insights.	Publication of available data and insights, allowing consumers to subscribe to tailored reports.
Reactive incident analysis service	O	Collection and classification of data, insights and input from other services for the purpose of performing corrective actions. Analysis of incident patterns and root cause analysis to perform corrective actions.	Publication of available data and insights, allowing consumers to subscribe to tailored reports.

Service name	ExtVis	Analysis performed	Analysis result
Proactive network optimization service	O	Collection of insights from other services and relevant performance metrics from the network. Analysis of the network structure, insights and performance metrics to optimize network performance.	Publication of suggested network optimizations.

NOTE: Besides specific analytics services that can be derived from the generic analytics service as they have the same set of capabilities, additional analytics services that have different capabilities than the generic service can be defined separately.

6.5.3.2.2 Domain condition detection service

This management service receives a set of conditions to be monitored and can decompose them into other typically domain specific conditions and monitor them. In case the status of the tracked conditions changes it provides a notification. The condition can be defined on a case by case basis. This service can be used by the producers of other services, e.g. to track the fulfilment or violation of certain conditions.

The service is further defined in table 6.5.3.2.2-1.

Table 6.5.3.2.2-1: Service definition

Service name		Domain condition detection service.
External visibility		MANDATORY.
Service capabilities		
	Manage conditions (M)	Manage (create, read, update, delete, list) conditions associated with a *domain service model*.
	Activate/deactivate conditions (M)	Activate/deactivate detection of conditions. The activation or deactivation of detection of conditions is specific to the network service instance and can be done per condition.
	Manage subscriptions (M)	Manage (create, read, update, delete, list) subscriptions to condition state change notifications for a network service.
	Provide condition state change notifications (M)	Provide notifications if the state of the set conditions changes (from not met to met or vice versa).

6.5.3.2.3 Data optimization services

The data optimization services can be used to pre-process data, to provide data ready to be used to the data analytics applications, and to provide alternative views of data, and to remove redundancy and/or irrelevance which reduces the workload of analysis and localization.

Different data optimization services are foreseen as the optimization algorithms typically require data set specific knowledge.

The standard capabilities of data optimization services are further defined in table 6.5.3.2.3-1 as a generic data optimization service.

Table 6.5.3.2.3-1: Capabilities of a generic data optimization service

Service name		Generic data optimization service.
External visibility		OPTIONAL.
Service capabilities		
	Optimize data (M)	Perform data optimization that is specific to the service and related to the characteristics of the data set.
	Configure data optimization (O)	Allow users to configure the data optimization.

Actual specific data optimization services have the same set of capabilities as the generic data optimization service but differ in the optimization they perform, the data sets for which they are suitable and the applicable data optimization configuration. Table 6.5.3.2.3-2 lists specific data optimization services that are defined by the ZSM framework. This set of services is extensible.

Table 6.5.3.2.3-2: Specific data optimization services defined by the ZSM framework

Service name	ExtVis	Optimization performed
Redundancy removal services	O	Removing redundant data according to the relationships of resources and services.
Irrelevancy removal services	O	Removing irrelevant data to decrease the data volume while keeping the data that are relevant for the data consumers.
Data aggregation services	O	Aggregating data as group according different dimensions based on the locations, time-period, topology, and so on.

NOTE: Besides specific data optimization services that can be derived from the generic data optimization service as they have the same set of capabilities, additional data optimization services that have different capabilities than the generic service can be defined separately.

6.5.4 Domain intelligence

6.5.4.1 Description

Domain intelligence services are responsible for driving intelligent closed-loop automation in a domain by supporting variable degrees of automated decision-making and human oversight with fully autonomous management being the final stage.

Intelligence services can be categorized as follows:

1) Decision support.

2) Decision making.

3) Action planning.

Decision support services enable decision making via technologies such as artificial intelligence, machine learning and knowledge management and are defined in clause 6.5.4.2.

Service and network management decision making is based on information provided by ZSM services defined as part of domain data collection (see clause 6.5.2), domain analytics (see clause 6.5.3), domain data services (see clause 6.4.4) and applicable other sources. Subsequent action planning defines orchestration/control actions to be executed by ZSM services defined as part of domain orchestration (see clause 6.5.5) and domain control (see clause 6.5.6). Services pertaining to decision making and action planning are left for future specification.

6.5.4.2 Provided management services

6.5.4.2.1 AI model management service

The AI model management service enables to manage AI models. An AI model can be updated on the basis of new input data periodically or at any time.

The service is further defined in table 6.5.4.2.1-1.

Table 6.5.4.2.1-1: Service definition

Service name		AI model management service
External visibility		OPTIONAL
Service capabilities		
	Manage AI models (M)	Manage (create, read, update, delete, list) the AI models

6.5.4.2.2 Deployed AI model assessment service

The performance of deployed AI models can degrade over time due to a change of reality, which results in the model not matching the reality accurately enough and can require model update or replacement. The deployed AI model assessment service allows determining the most appropriate action to execute on the AI models deployed and used by management functions based on available information regarding the performance of the model. For that purpose, the deployed AI model assessment service may use the output of the deployed AI model performance evaluation service defined in clause 6.5.3.2.1.

The assessment derived from the deployed AI model assessment service is used to decide on the most appropriate actions to perform on the deployed AI model such as retrain, reconfigure, upgrade, replace, pause, terminate.

The service is further defined in table 6.5.4.2.2-1.

Table 6.5.4.2.2-1: Service definition

Service name		Deployed AI model assessment service
External visibility		OPTIONAL
Service capabilities		
	Provide decision result (C)	Provide the result of the assessment process
	Request decision result (C)	Trigger the deployed AI model assessment service to generate a decision result
NOTE: At least one of the two capabilities shall be offered.		

6.5.4.2.3 AI training data management service

The AI training data management service enables to manage training data that is required to train or re-train the AI models. The training data may be labelled data that include the input features/attributes and the ground-truth output of classification, prediction or other machine learning problems. The training data may refer to a specific AI model whose training depends on the data or may be accumulating training data independently of existing AI models to enable future AI model development.

The service is further defined in table 6.5.4.2.3-1.

Table 6.5.4.2.3-1: Service definition

Service name		AI Training data management service
External visibility		OPTIONAL
Service capabilities		
	Manage AI training data (M)	Manage (create, read, update, delete, list) the AI training data sets. Create, read, delete and list are mandatory, update is optional

6.5.4.2.4 Knowledge base service

The purpose of the service is to create and maintain a machine-readable knowledge base where known problem cause descriptions, in combination with corresponding resolutions, are collected and analysed. The objective is to replace the present use of manuals.

The knowledge base shall contain problem causes derived from historical, operational (e.g. FM, PM) and configurational data, as well as conclusions drawn from analysis of combinations of problem causes.

The service is further defined in table 6.5.4.2.4-1.

Table 6.5.4.2.4-1: Service definition

Service name		Knowledge base service.
Visibility		OPTIONAL.
Service capabilities		
	Create knowledge base (M)	Create a machine-readable knowledge base for known problem causes and corresponding resolutions.
	Add new data-set/schema (M)	Add a new data set or schema in an existing knowledge base.
	Collect data (M)	Collect problem causes and corresponding resolutions.
	Produce derived knowledge (O)	Derive new sets of problem causes and resolutions based on analysis of collected data.
	Query knowledge (M)	Responds to queries from other services.

6.5.4.2.5 Health issue reporting service

Even in an automated system, not all service health issues can be repaired automatically. For certain issues, reporting to a higher-order entity (E2E service management domain or ZSM framework consumer) is needed. This service allows to manage such issue reports.

The health issue reporting service provides information about abnormal service health states (e.g. due to faults, security issues, etc.). It also allows to track and update the status of the health issues and their severity and to configure what information is provided.

The service is further defined in table 6.5.4.2.5-1.

Table 6.5.4.2.5-1: Service definition

Service name		Health issue reporting service.
External visibility		OPTIONAL.
Service capabilities		
	Provide health issue notifications (M)	Provide notifications about health issues. This includes information about the occurrence of new issues, but also about status changes of known issues.
	Query health issues (M)	Query information about service health status and active health issues. The response can include information about the probable root cause, related resource issues, related health issues of consumed managed services, unsuccessful repair actions that were tried automatically, etc.
	Update health issue status (M)	Update the status of a health issue, e.g. to indicate that the issue has been dealt with by an entity that is responsible for handling an escalation.
	Configure service (O)	Configure the service.

6.5.5 Domain orchestration

6.5.5.1 Description

Domain orchestration provides management services that allow automating workflows and processes inside a management domain to handle lifecycle management of the managed customer and/or resource-facing services. Domain orchestration services maintain the inventory of network services and virtualized resources managed by the management domain and an up-to-date view of the related topology, by using discovery, inventory and topology management services. Domain orchestration is controlled by policies and other additional relevant information sources, e.g. SLSs.

NOTE 1: The inventory of hardware resources is not managed by domain orchestration, as hardware resources installation/de-installation is not part of orchestration.

Domain orchestration services in the current management domain can be consumed by service requests from another management domain which manages services that consume services managed by the current management domain. They can also be consumed by service consumers that provide E2E service orchestration, or by the ZSM framework consumers.

NOTE 2: In some cases, the services provided by a management domain can be directly consumed by the ZSM framework consumers, e.g. if it is only a single managed service that is provided to the customers. The standard way however is that the ZSM framework consumers consume services from the E2E service management domain.

As part of the closed loops at management domain level, domain orchestration services can also be consumed by management functions that provide domain intelligence services, which can e.g. lead to the execution of a pre-configured workflow.

The management functions providing domain orchestration services consume domain control services to control the state of the managed entities of the management domain. If the current management domain manages services that contain (by way of composition) resource-facing services managed by another management domain, the management functions providing domain orchestration services can also consume services, including domain orchestration or domain control services, provided by that other management domain.

6.5.5.2 Provided management services

6.5.5.2.1 Domain orchestration service

The domain orchestration service allows authorized consumers to instantiate and maintain domain-level network services, including creation, modification and termination of the services, and allows the automation of corresponding workflows. An explicit domain service model may provide a complete description of all necessary infrastructure resources and consumed services, their topology, their configuration, their policies and their location in the network, etc. Further, it contains the orchestration workflows that can be executed for this service. Some aspects of the service models may be intent-based and need resolution of the intent. Service model aspects (e.g. a latency target or an affinity rule) need to be mapped to one or more orchestration actions (e.g. VNF placement or PNF selection). Others can be parameterized when performing operations that manage the lifecycle of the services. Orchestration execution includes consuming domain control services to configure or modify the infrastructure resources or consumed services, issuing requests to manage the connectivity of the managed entities (e.g. by VIMs), and consuming domain orchestration services of other management domains, such as managing connectivity services between PNFs using an SDN domain. The domain service model is maintained in the managed services catalogue of the domain.

The domain orchestration service is further defined in table 6.5.5.2.1-1.

Table 6.5.5.2.1-1: Service definition

Service name		Domain orchestration service.
External visibility		MANDATORY.
Service capabilities		
	Manage service lifecycle (M)	Manage the lifecycle of the services that are managed by the domain (see note), as defined by the domain service model to be applied. This capability also allows to execute service-specific lifecycle management operations that are defined in the domain service model. Supported lifecycle management operations shall include operations instantiation, termination and configuration management of the services and may include further operations such as scaling, healing, etc. of the services, based on the domain service model.
	Execute workflow (M)	Execute a workflow that is defined in the domain service model. Some workflows may be triggered by entities outside the management domain, others may be visible only domain-internally to be used e.g. in closed loops.
	Query domain service info (M)	Query the domain service information (e.g. operational service state).
	Provide notifications about lifecycle changes (M)	Notify subscribed consumers about lifecycle changes of the services managed by the management domain.
	Manage subscription to lifecycle changes (O)	Manage (create, read, update, delete, list) subscription to notifications about lifecycle changes.
NOTE: An NFV MANO domain and a 3GPP Management domain are examples of the domains for which services are managed.		

6.5.5.2.2 Feasibility check service

Feasibility check service is used to check if a particular parameterized managed service is deployable in the current management domain at the proposed service level.

Further details are described in table 6.5.5.2.2-1.

Table 6.5.5.2.2-1: Service definition

Service name		Feasibility check service.
External visibility		MANDATORY.
Service capabilities		
	Check deployment feasibility (M)	Check whether the service requirements the respective management domain is responsible for can be satisfied by the management domain. The result of the feasibility check may include an indication of the confidence that the requirements can be satisfied; in addition, the request may indicate the desired confidence.
	Check and reserve (O)	Check whether the service requirements the respective management domain is responsible for can be satisfied by the management domain, and, if yes, create a reservation for a given time.

6.5.5.2.3 Managed services catalogue management service

The managed services catalogue management service is responsible for managing a catalogue of service models representing the services managed by the management domain and exposing this catalogue to other management domains including the end-to-end service management domain. The service models may include supporting information, such as supported coverage areas, supported SLS levels, service templates and so on, and may be grouped in service categories. Service models typically have a lifecycle which means that every entry in the catalogue has a state that represents the stage of the lifecycle of the related service model. These managed services may be combined at the E2E service management domain level to create E2E services.

The service is further defined in table 6.5.5.2.3-1.

Table 6.5.5.2.3-1: Service definition

Service name		Managed services catalogue management service.
External visibility		MANDATORY.
Service capabilities		
	Manage service models (M)	Manage (create, read, update, delete, list) the service models that are part of the managed services catalogue. Read and list operations are mandatory while the rest are optional. "Update" allows to modify properties of the service model, including its state (lifecycle stage). Filtering mechanisms may be used to select the information returned when listing the content of the catalogue.
	Manage service categories (O)	Manage (create, read, update, delete, list) the service categories used in the catalogue.
	Provide catalogue change notifications (O)	Provides notifications about catalogue changes.

6.5.5.2.4 Testing service

The testing service enables the execution of tests based on information such as policies, configuration data, and performance data before activation and/or within production/live networks to ensure that the infrastructure resources are working correctly.

Tests are executed based on a test specification (which is designed outside and lifecycle-managed). Tests can be triggered as needed e.g. by the E2E service management domain or as part of automated procedures. The service also allows to query previous and ongoing tests, their status and results.

The service is further defined in table 6.5.5.2.4-1.

Table 6.5.5.2.4-1: Service definition

Service name		Testing service.
External visibility		OPTIONAL.
Service capabilities		
	Manage test specifications (M)	Manage (create, read, update, delete, list) test specifications.
	Test resources (M)	Check if the infrastructure resources are working correctly. For example, the configuration is set as requested, state normality and CPU/memory utilization. The test is executed based on a test specification.
	Query tests (M)	Query ongoing tests (including their status) and finished tests (including their results).
	Provide test notifications (O)	Provide event notifications about changes of the status of a test.

6.5.5.2.5 Domain inventory information service

The domain inventory information service allows to query information about available infrastructure resources as well as available (instantiated and active) managed services managed by the management domain e.g. for the purpose of end-to-end service management. The information can be provided at different abstraction levels to support different use cases: Information used for end-to-end management is abstract while information used for the domain specific management is more detailed.

The service is further detailed in table 6.5.5.2.5-1.

Table 6.5.5.2.5-1: Service definition

Service name		Domain inventory service.
External visibility		CONDITIONAL (see note).
Service capabilities		
	Query inventory of available resources (M)	Query information about available infrastructure resources and available (instantiated and active) managed services.
NOTE: This service is MANDATORY if the management domain is able to produce inventory information.		

6.5.5.2.6 Domain inventory management service

The domain inventory management service collects information on available infrastructure resources as well as available (instantiated and active) managed services in the management domain. This service is provided only to consumers inside the domain.

Each change to the inventory is triggered as a side effect of a control or orchestration service invocation on the managed entities of the domain.

The service is further detailed in table 6.5.5.2.6-1.

Table 6.5.5.2.6-1: Service definition

Service name		Domain inventory management service.
External visibility		OPTIONAL.
Service capabilities		
	Manage inventory (M)	Manage (create, read, update, delete) inventory information.

6.5.5.2.7 Domain topology information service

This service provides information about the topology of the infrastructure resources and services managed by the management domain at different abstraction levels.

The information is made available via the cross-domain data services.

The service is further detailed in table 6.5.5.2.7-1.

Table 6.5.5.2.7-1: Service definition

Service name		Domain topology information service.
External visibility		OPTIONAL.
Service capabilities		
	Configure service (O)	Configure the service, such as setting the abstraction policy to control the degree of detail of the provided topology information.
	Query topology information (M)	Allow to query information about the topology of the infrastructure. This may include resources (and their utilization level), services, physical/virtualized nodes, physical and/or virtual links/network connections. The reported information is supplied at an abstraction level that matches the needs of the consumer and that fulfils the policy to control the degree of detail of the provided information.

6.5.6 Domain control

6.5.6.1 Description

Domain control services allow to individually steer the state of each managed entity. The service producers which provide domain control services consume for example the configuration management interfaces provided by the managed entities and abstract from their service consumers the details of configuration changes. As an example, the domain control services can be consumed by management functions that offer services in the domain orchestration group to change the state or configuration of a managed entity and consumed service. The domain control group may also contain services that are needed to control virtualized resources.

As part of the closed loops at domain level, domain control services are consumed by management functions in the domain orchestration and domain intelligence groups to control the state (including configuration, lifecycle) of managed entities and consumed services.

6.5.6.2 Provided management services

6.5.6.2.1 Resource configuration management service

This service allows to manage the configuration the resources managed by the management domain.

The service is further defined in table 6.5.6.2.1-1.

Table 6.5.6.2.1-1: Service definition

Service name		Resource configuration management service.
External visibility		OPTIONAL.
Service capabilities		
	Manage resource configuration (O)	Manage the configuration of the managed resources of the domain, including the software and the configuration parameters of the resources.

6.5.6.2.2 Resource lifecycle management services

Various services can manage the lifecycle of resources in the domain.

The set of operations for managing the lifecycle of resources in the domain depends on the type of resources. A VNF is an example of a resource type that needs lifecycle management.

The lifecycle management can include operations such as instantiation, update, scaling, healing and termination.

This service can be consumed by management functions providing the domain orchestration service (see clause 6.5.5.2).

The standard capabilities of resource lifecycle management services are further defined in table 6.5.6.2.2-1 as a generic resource lifecycle management service.

Table 6.5.6.2.2-1: Capabilities of a generic resource lifecycle management

Service name		Generic resource lifecycle management service.
External Visibility		OPTIONAL.
Service capabilities		
	Manage resource lifecycle (M)	Manage the lifecycle of the resources in the domain. The set of applicable lifecycle management operations depends on the resource type, but typically includes the instantiation and termination of the resources.
	Provide notifications of lifecycle changes (M)	Notify subscribed consumers about executed lifecycle operations and the changes they make to the resources.
	Manage subscriptions to lifecycle changes (O)	Manage (create, read, update, delete, list) subscriptions to notifications of lifecycle changes.

Actual specific resource lifecycle management services have the same set of capabilities as the generic resource lifecycle management service but differ in the type of resource they manage and in the set of lifecycle operations they support. Table 6.5.6.2.2-2 lists specific resource lifecycle management services that are defined by the ZSM framework. This set of services is extensible.

Table 6.5.6.2.2-2: Specific resource lifecycle management services defined by the ZSM framework

Service name	ExtVis	Resource lifecycle management performed	Operations
Virtualized resource lifecycle management service	O	Virtualized resources, e.g. VNF, virtual link, etc, can be based on a deployment template/model, which captures the deployment and operational behaviour requirements, including the supported lifecycle management operations, in an abstract manner.	Instantiation, termination, optionally scaling, healing, update, and further resource specific operations.

NOTE: Besides specific resource lifecycle management services that can be derived from the generic resource lifecycle management service as they have the same set of capabilities, additional resource lifecycle management services that have different capabilities than the generic service can be defined separately.

6.5.6.2.3 Configuration data generation service

The configuration data generation service generates the configuration data (e.g. IP address, VLAN) automatically.

The service is further defined in table 6.5.6.2.3-1.

Table 6.5.6.2.3-1: Service definition

Service name		Configuration data generation service.
External visibility		OPTIONAL.
Service capabilities		
	Generate configuration data (M)	Generate configuration data e.g. by consuming domain assurance services or domain intelligence services.

6.5.7 Supporting services

6.5.7.1 Description

The following services provide support functionalities for the management domain.

6.5.7.2 Provided management services

6.5.7.2.1 Policy management service

Policy and Artificial Intelligence (AI)/Machine Learning (ML) are used in the decision and recommendations. This service focuses on the policy management, including the policy lifecycle management, and policy conflict detection. Once a policy has been created, the ZSM framework needs to check that the newly created policy does not conflict with other existing policies that are currently running in the management domain. The ZSM framework should avoid policy conflicts with other activities within the management domain.

Examples of policy conflicts:

- An event triggers multiple policy-actions that cannot occur together or contradict each other.
- Different events trigger one policy-action each, while these actions contradict each other.

The service is further defined in table 6.5.7.2.1-1.

Table 6.5.7.2.1-1: Service definition

Service name		Policy management service.
External visibility		OPTIONAL (see note).
Service capabilities		
	Manage policies (M)	Manage (create, read, update, delete, list) the policies.
	Activate/deactivate policy (M)	Activate/deactivate created policies.
	Detect policy conflict (O)	Detect the potential conflicts that can exist in the policies.
	Provide notifications about policy conflicts (O)	Provide notifications policy about conflicts when a conflict has been detected.
NOTE: Some management domains may not support the external consumption of the policy management service.		

6.6 E2E service management domain

6.6.1 Overview

The E2E service management domain manages customer-facing E2E services composed from services managed by the various management domains. Within the E2E service management domain, the following groups of management services are provided:

- E2E service orchestration - responsible for the coordination of the provisioning, configuration and lifecycle management of the various services across management domains in the end-to-end network that make up a customer facing E2E service.
- E2E service intelligence - responsible for driving intelligent closed-loop automation in the E2E service management domain, supporting variable degrees of automated decision-making and human oversight. This enables various tasks such as troubleshooting and fixing of issues across management domains in the end-to-end network that cause E2E service disruption.
- E2E service analytics - responsible for deriving end-to-end service insights, and for managing the end-to-end service-related KPIs.
- E2E service data collection - responsible for the collection of end-to-end service-related data, e.g. fault or performance data.

As in the individual management domains, each E2E management service capability is offered via one or more end-points.

Some management services can be restricted to be consumed by authorized consumers inside the E2E service management domain only (internal services), whereas others are available for consumption by authorized consumers inside and outside the E2E service management domain (exposed services). See clause 6.1.2.3 for a more detailed description.

Message exchange between the management functions may be accomplished via the domain integration fabric, using the service end-points. Depending on the nature of the service capabilities offered, the service interfaces may be based on, e.g. publish/subscribe or request-response models.

Communication between the management domains and the E2E service management domain as well as between the E2E service management domain and the ZSM framework consumers is handled via the cross-domain integration fabric.

6.6.2 E2E service data collection

6.6.2.1 Description

The E2E service data collection services are responsible for monitoring the quality and availability of customer-facing services. This necessitates monitoring the actual E2E service quality and verifying the end user experience, based on up-to-date data which are typically provided by data collection services of the management domains that manage the services of which the E2E service is composed.

6.6.2.2 Provided management services

6.6.2.2.1 E2E performance data reporting service

The E2E performance data reporting service collects the performance data of services managed by the management domain(s) and provides the performance data (e.g. KPIs) of E2E services to corresponding authorized customers.

The service is further defined in table 6.6.2.2.1-1.

Table 6.6.2.2.1-1: Service definition

Service name		E2E performance data reporting service.
External visibility		MANDATORY.
Service capabilities		
	Provide performance data (M)	Report performance data (e.g. KPIs) of E2E services.
	Manage subscriptions (O)	Manage (create, read, update, delete, list) subscriptions to performance data reports of a given E2E service.

6.6.3 E2E service analytics

6.6.3.1 Description

The E2E service analytics services are responsible for handling E2E service impact analysis and root cause analysis and generate service-specific predictions. Also, the verification of Service Level Specifications (SLSs) and monitoring of KPIs is included in E2E service analytics.

6.6.3.2 Provided management services

6.6.3.2.1 Analytics services

Various analytics services process incoming events and other information related to faults and performance from the underlying management domains and other inputs, aggregate and analyse the information and derive e.g. end-to-end service and user level key performance indicators and other insights. Analytics services can also have capabilities to keep track of end-to-end service KPIs and user experience (such as video freezing or frame-dropping) that are specific to the service provided. This works based on service-specific observation mechanisms or probes in the underlying management domains. Analytics services can also be configured to customize how and when analysis results are provided. For instance, the way the insights are created and the algorithms that are used can all be configured.

The standard capabilities of analytics services are further defined in table 6.6.3.2.1-1 as a generic analytics service.

Table 6.6.3.2.1-1: Capabilities of a generic analytics service

Service name		Analytics services.
External visibility		CONDITIONAL (see note 1).
Service capabilities		
	Manage subscriptions (O)	Manage (create, read, update, delete, list) subscriptions to analysis results generated by this particular analytics service. Filters may be specified.
	Configure analytics (O)	Configure how analysis results are derived for a given E2E Service. E.g. by configuring analytics event calculation method, insights derived by multiple analytics, input data, recommendation algorithm used, and so on.
	Provide analysis results (C)	Provide notifications with analysis results. This capability is applicable to services which generate analysis results asynchronously (see note 2).
	Request analysis result (C)	Trigger an analytics process and obtain the result. This capability is applicable to services that need an explicit trigger to start (see note 2).
NOTE 1: It depends on the actual analytics service whether the external visibility of the service is MANDATORY or OPTIONAL. NOTE 2: At least one of these capabilities shall be supported.		

Actual specific analytics services have the same set of capabilities as the generic analytics service but differ in the type of analysis result they generate, the analysis they perform and the actual configuration. Table 6.6.3.2.1-2 lists specific analytics services defined by the ZSM framework. This set of services is extensible.

Table 6.6.3.2.1-2: Specific analytics services defined by the ZSM framework

Service name	ExtVis	Analysis performed	Analysis result
E2E anomaly detection service	O	The anomaly detection service provides capabilities to detect anomalous conditions related to the E2E service using information provided by the domain data collection services from the underlying management domains. Such conditions might be, for example, security violations/anomalies, fault conditions that lead to localized or short-term unavailability of the E2E service or inconsistencies in the service even though no SLS violation might be detected. If any anomalies or abnormal behaviour are detected, the results can trigger E2E service intelligence services producers to make appropriate decisions, e.g. find a resolution or a workaround, or to make the data available to other analytics services for further analysis, or it may expose the information to the ZSM framework consumers via the cross-domain integration fabric.	Notifications related to detected anomalies.
Deployed AI model performance evaluation service	O	The deployed AI model performance evaluation service allows determining the level of performance of deployed AI models and detecting e.g. performance degradation (AI models are probabilistic systems that may suffer performance degradation over time and need to be retrained), sudden performance drop, irregular performance, etc. The deployed AI model performance evaluation service can be used for instance by the deployed AI model assessment service to decide on the most appropriate actions to perform on the deployed AI models.	Notifications related to performance evaluation of deployed AI models.
Root cause analysis service	O	Determining the root cause of a problem by correlating information about multiple faults, identifying dependencies and using additional insights or knowledge.	Information about root cause.
Impact analysis service	O	Determining the impact of a fault or other problem (e.g. performance issue) on the actual managed service performance or availability.	Information about impact.
Performance analysis service	O	Processing data collected by the data collection services of the underlying management domains to obtain high-level service performance insights, e.g. KPIs and information related to service degradations such as congestion and overload situations.	Information about performance issues.
Security analytics service	O	Processing security events to identify specific attack patterns, threats and suspicious behaviour that can have security implications.	Information about security issues.

NOTE: Besides specific analytics services that can be derived from the generic analytics service as they have the same set of capabilities, additional analytics services that have different capabilities than the generic service can be defined separately.

6.6.3.2.2 E2E service quality management service

The E2E service quality management service allows authorized consumers to manage the service level objectives (SLO) and service level specifications (SLS) of the E2E services, and to track their violations.

SLSs and SLOs are related to service level agreements (SLAs). SLSs are composed of SLOs and provide the technical parameters that define the service quality that is committed in the SLA to be delivered. An SLA is a legally binding contract between a service provider and a customer, which includes for example the consequences in case of not meeting the required service quality, and further business-related aspects. The definition and management of SLAs is outside the scope of the present document as these are business agreements.

The service is further defined in table 6.6.3.2.2-1.

Table 6.6.3.2.2-1: Service definition

Service name		E2E service quality management service.
External visibility		MANDATORY.
Service capabilities		
	Manage E2E service SLSs (M)	Manage (create, read, update, delete, list) SLSs. Any of these can be associated to a given E2E service model or E2E service instance.
	Manage E2E service SLOs (M)	Manage (create, read, update, delete, list) SLOs associated to SLSs.
	Provide violation notifications (M)	Provide event notifications about violations of SLSs and/or SLOs. This allows to trigger corrective actions (see note).
	Manage subscriptions (O)	Manage (create, read, update, delete, list) subscriptions to event notifications about SLS and/or SLO violations.
	Query violations (O)	Query/read information about violations of SLSs and/or SLOs.
NOTE: Violation of SLSs and/or SLOs can also lead to consequences as defined by a service level agreement (SLA) associated with the violated SLS and/or SLO, depending on how the SLA is defined related to the SLS(s)/SLO(s). The content of SLAs is outside the scope of the present document.		

6.6.3.2.3 E2E service condition detection service

This service enables the decomposition of a condition (example: SLS) related to the E2E services to other conditions (example: KPIs to be met) that are supported by individual management domains. It then tracks these conditions to check if they are met and provides a notification if the status of a condition changes. The condition can be defined on a case by case basis. This service can be used by the producers of other services, e.g. to track SLS violations.

The service is further defined in table 6.6.3.2.3-1.

Table 6.6.3.2.3-1: Service definition

Service name		E2E service condition detection service.
External visibility		MANDATORY.
Service capabilities		
	Manage conditions (M)	Manage (create, read, update, delete, list) conditions associated with an E2E service model. This is based on the conditions that can be supported by the composing management domains. Created conditions can be activated/deactivated. The activated conditions are specific to the E2E service instance.
	Activate/deactivate conditions (M)	Activate/deactivate detection of conditions. The activation and deactivation of detection of conditions is specific to the E2E service instance and can be done per condition.
	Manage subscriptions (M)	Manage (create, read, update, delete, list) subscriptions to condition state change notifications for an E2E service.
	Provide condition state change notifications (M)	Provide a notification if the state of the set conditions changes (from met to not met or vice versa).

6.6.4 E2E service intelligence

6.6.4.1 Description

E2E service intelligence services are responsible for driving intelligent closed-loop automation in the E2E service management domain by supporting variable degrees of automated decision-making and human oversight with fully autonomous management being the final stage.

Intelligence services can be categorized as follows:

1) Decision support.

2) Decision making.

3) Action planning.

Decision support services enable decision making via technologies such as artificial intelligence, machine learning and knowledge management and are defined in clause 6.6.4.2.

E2E service management decision making is based on information provided by ZSM services defined as part of E2E service data collection (see clause 6.6.2), E2E service analytics (see clause 6.6.3), domain data services in the E2E service management domain (see clause 6.4.4), cross-domain data services (see clause 6.4.3) and applicable other sources. Subsequent action planning defines orchestration/control actions to be executed by ZSM services defined as part of E2E service orchestration (see clause 6.6.5). Services pertaining to decision making and action planning are left for future specification.

6.6.4.2 Provided management services

6.6.4.2.1 AI model management service

The AI model management service enables to manage AI models. An AI model can be updated on the basis of new input data periodically or at any time.

The service is further defined in table 6.6.4.2.1-1.

Table 6.6.4.2.1-1: Service definition

Service name		AI model management service.
External visibility		OPTIONAL.
Service capabilities		
	Manage AI models (M)	Manage (create, read, update, delete, list) the AI models.

6.6.4.2.2 Deployed AI model assessment service

The performance of deployed AI models can degrade over time due to a change of reality, which results in the model not matching the reality accurately enough and can require model update or replacement. The deployed AI model assessment service allows determining the most appropriate action to execute on the AI models deployed and used by management functions based on available information regarding the performance of the model. For that purpose, the deployed AI assessment service may use the output of the deployed AI model performance evaluation service defined in clause 6.6.3.2.1.

The assessment derived from the deployed AI model assessment service is used to decide on the most appropriate actions to perform on the deployed AI model such as retrain, reconfigure, upgrade, replace, pause, terminate.

The service is further defined in table 6.6.4.2.2-1.

Table 6.6.4.2.2-1: Service definition

Service name		Deployed AI model assessment service.
External visibility		OPTIONAL.
Service capabilities		
	Provide decision result (C)	Provide the result of the assessment process.
	Request decision result (C)	Trigger the deployed AI model assessment service to generate a decision result.
NOTE: At least one of the two capabilities shall be offered.		

6.6.4.2.3 AI training data management service

The AI training data management service enables to manage training data that is needed to train or re-train the AI models. The training data may be labelled data that include the input features/attributes and the ground-truth output of classification, prediction or other machine learning problems. The training data may refer to a specific AI model whose training depends on the data or may be accumulating training data independently of existing AI models to enable future AI model development.

The service is further defined in table 6.6.4.2.3-1.

Table 6.6.4.2.3-1: Service definition

Service name		AI Training data management service.
External visibility		OPTIONAL.
Service capabilities		
	Manage AI training data (M)	Manage (create, read, update, delete, list) the AI training data sets. Create, read, delete and list are mandatory, update is optional.

6.6.4.2.4 E2E service health issue reporting service

Even in an automated system, not all service health issues can be repaired automatically. For certain issues, reporting to a higher-order entity (such as ZSM framework consumer) is needed. This service allows to manage such issue reports.

The E2E service health issue reporting service provides information about abnormal service health states (e.g. due to faults, security issues, etc.) and allows to correlate them with issues in the underlying management domain if that information is available. It also allows to track and update the status of the health issues and their severity and to configure what information is provided.

The service is further defined in table 6.6.4.2.4-1.

Table 6.6.4.2.4-1: Service definition

Service name	E2E service health issue reporting service.	
External visibility	MANDATORY.	
Service capabilities		
	Provide health issue notifications (M)	Provide notifications about health issues. This includes information about the occurrence of new issues, but also about status changes of known issues.
	Query health issues (M)	Query information about service health status and active health issues. The response can include information about the probable root cause, related health issues in the services managed by the management domains that contribute to the E2E service, unsuccessful repair actions that were tried automatically, etc.
	Update health issue status (M)	Request the update of the status of a health issue, e.g. to indicate that the issue has been dealt with by an external entity that is responsible for handling an escalation.
	Configure service (O)	Configure the service.

6.6.5 E2E service orchestration

6.6.5.1 Description

The services in E2E service orchestration are responsible for the catalogue-driven E2E orchestration of multiple management domains to create/modify/delete cross-domain customer-facing services. A service model defines how the various pieces of a service are linked together and map to management domains.

6.6.5.2 Provided management services

6.6.5.2.1 E2E service orchestration service

The E2E service orchestration service allows authorized consumers to instantiate and maintain E2E services (e.g. network slice), including creation, modification and termination of the E2E service, and allows the automation of corresponding workflows. This service applies to the E2E service model which is managed by the managed services catalogue management service in the E2E service management domain (see clause 6.6.5.2.3). The E2E service model describes the entire E2E service including references to descriptions of service parts provided by the management domains and their inter-connections. The E2E service orchestration service can be consumed by the ZSM framework consumers to deploy the E2E services.

The service is further defined in table 6.6.5.2.1-1.

Table 6.6.5.2.1-1: Service definition

Service name		E2E service orchestration service.
External visibility		MANDATORY.
Service capabilities		
	Manage service lifecycle (M)	Manage the lifecycle of the E2E services (see note) provided by the E2E service management domain, as defined by the E2E service model to be applied. This capability also allows to execute E2E service-specific lifecycle management operations that are defined in the E2E service model. Supported lifecycle management operations shall include instantiation, termination and configuration management of the services and may include further operations such as modification, scaling and healing of E2E services based on E2E service and workflow models, if available.
	Execute workflow (M)	Execute a workflow that is defined in the E2E service model. Some workflows may be triggered by entities outside the E2E service management domain, others may be visible only domain-internally to be used e.g. in closed loops.
	Get mapping info (O)	Returns the information on how an E2E service is or will be mapped across the management domains. The information of this mapping is returned at the level of abstraction the consumer of this service is authorized to view.
	Query service info (M)	Query the E2E service information (e.g. service state).
	Provide notifications about lifecycle changes (M)	Notify its consumers about the lifecycle changes of E2E services.
	Manage subscriptions to lifecycle changes (O)	Manage (create, read, update, delete, list) subscriptions to notifications about lifecycle changes.
NOTE: Network slices can be an example of E2E services managed with this capability.		

6.6.5.2.2 Feasibility check service

Feasibility check service is used to check if a particular parameterized E2E service (e.g. network slice) is deployable at the proposed service level.

Different kinds of checks can provide different trade-offs of resource requirements vs. accuracy. Examples of checks are:

- simple checks of selected sets of fundamental domain capabilities to determine if a managed service is offered (e.g. in a particular location) that have low effort but also low accuracy;
- the collection of complete and current information about idle (i.e. available) resources that needs more effort but is more accurate; and
- the full assignment of all aspects of a service and the reservation of the resources to provide the service that is most accurate but needs the highest effort.

In certain scenarios, when low effort of the check is prioritized over accuracy, resource availability might be uncertain for selected management domains, which implies that the check results include a confidence indicator in case of uncertainty in resource availability.

Further details are described in table 6.6.5.2.2-1.

Table 6.6.5.2.2-1: Service definition

Service name		Feasibility Check Service.
External visibility		MANDATORY.
Service capabilities		
	Check deployment feasibility (M)	Check whether the E2E service requirements can be satisfied by the E2E service management domain. This invokes feasibility checks for parts of the E2E service provided by the respective management domain. The result of the feasibility check may include an indication of the confidence that the requirements can be satisfied; in addition, the request may indicate the desired confidence.
	Check and reserve (O)	Check whether the E2E service requirements can be satisfied by the E2E service management domain and, if yes, create a reservation for a given time.

6.6.5.2.3 Managed services catalogue management service

The managed services catalogue management service is responsible for managing a catalogue of service models representing the available E2E services managed by the E2E service management domain and exposing this catalogue to ZSM framework consumers. The E2E service models may include supporting information, such as supported coverage areas, associated SLSs, service templates and so on, and may be grouped in service categories. Service models typically have a lifecycle which means that every entry in the catalogue has a state that represents the stage of the lifecycle of the related service model.

The service is further defined in table 6.6.5.2.3-1.

Table 6.6.5.2.3-1: Service definition

Service name		Managed services catalogue management service.
External visibility		MANDATORY.
Service capabilities		
	Manage service models (M)	Manage (create, read, update, delete, list) the E2E service models that are a part of the managed services catalogue. Read and list operations are mandatory while the rest are optional. "Update" allows to modify properties of the service model, including its state (lifecycle stage). Filtering mechanisms may be used to select the information returned when listing the content of the catalogue.
	Manage service categories (O)	Manage (create, read, update, delete, list) the service categories used in the catalogue.
	Provide catalogue change notifications (O)	Provides notifications about catalogue changes.

6.6.5.2.4 E2E testing service

The E2E testing service enables the execution of active or passive tests of end-to-end services and/or parts of them to find out the failure location(s), without any impact on other unrelated network services.

Tests are executed based on a test specification (which is designed outside and lifecycle-managed). Tests can be triggered as needed e.g. by a ZSM framework consumer or as part of automated procedures. The service also allows to query previous and ongoing tests, their status and results.

The service is further defined in table 6.6.5.2.4-1.

Table 6.6.5.2.4-1: Service definition

Service name		E2E testing service.
External visibility		OPTIONAL.
Service capabilities		
	Manage test specifications (M)	Manage (create, read, update, delete, list) test specifications.
	Test services (M)	Check if an end-to-end service and/or parts of it works correctly and find out the failure location(s) if the test fails (see note). The test is executed based on a test specification.
	Query tests (M)	Query ongoing tests (including their status) and finished tests (including their results).
	Provide test notifications (O)	Provide event notifications about changes of the status of a test.
NOTE: An example of passive test is an audit of orchestration.		

6.6.5.2.5 E2E services inventory information service

The E2E services inventory information service allows to query information about available (instantiated and active) E2E services. This information is are based on aggregating inventory information provided by the involved management domains.

The service is further detailed in table 6.6.5.2.5-1.

Table 6.6.5.2.5-1: Service definition

Service name		E2E services inventory information service.
External visibility		MANDATORY.
Service capabilities		
	Query inventory of available services (M)	Query information about available (instantiated and active) E2E services.

6.6.5.2.6 E2E services inventory management service

The E2E services inventory service collects information about available (instantiated and active) E2E services. This service is provided only to consumers inside the E2E service management domain.

Each change to the inventory is triggered as a side effect of an orchestration service invocation on the managed services of the E2E service management domain, or by changes to the RFSs/CFSs of which the E2E service is composed.

The service is further detailed in table 6.6.5.2.6-1.

Table 6.6.5.2.6-1: Service definition

Service name		E2E services inventory management service.
External visibility		OPTIONAL.
Service capabilities		
	Manage inventory (M)	Manage (create, read, update, delete) inventory information.

6.6.5.2.7 E2E services topology information service

This service provides information on the topology of the infrastructure from the perspective of E2E services at different abstraction levels.

The service is further defined in table 6.6.5.2.7-1.

Table 6.6.5.2.7-1: Service definition

Service name		E2E service topology information service.
External visibility		OPTIONAL.
Service capabilities		
	Configure service (O)	Configure the service, such as setting the abstraction policy to control the degree of detail of the provided topology information.
	Query topology information (M)	Allow to query information about the topology of the infrastructure from the perspective of E2E services. This may include resources (and their utilization level), services, physical/virtualized nodes, physical and/or virtual links/network connections. The reported information is supplied at an abstraction level that matches the needs of the consumer and that fulfils the policy to control the degree of detail of the provided information.

6.6.6 Supporting services

6.6.6.1 Description

The following services provide support functionalities for the E2E service management domain.

6.6.6.2 Provided management services

6.6.6.2.1 E2E policy management service

Policy and Artificial Intelligence (AI)/Machine Learning (ML) are used in the decisions and recommendations. This service focuses on the policy management, including the policy lifecycle management, and policy conflict detection. The E2E level policies are associated with the policies composing network facing services in the respective individual management domains. The ZSM framework also verifies that the newly created policy does not conflict with other existing policies that are currently running in the management domain. The ZSM framework should avoid policy conflicts with other activities within the E2E service management domain.

Examples of policy conflicts:

- An event triggers multiple policy-actions that cannot occur together or contradict each other.
- Different events trigger one policy-action each, while these actions contradict each other.

The service is further defined in table 6.6.6.2.1-1.

Table 6.6.6.2.1-1: Service definition

Service name		E2E policy management service.
External visibility		MANDATORY.
Service capabilities		
	Manage policies (M)	Manage (create, read, update, delete, list) the policies.
	Activate/deactivate policy (M)	Activate/deactivate created policies.
	Detect policy conflict (O)	Detect the potential conflicts that can exist in the policies.
	Provide policy conflict notifications (O)	Provide a notification if a conflict has been detected.

7 Operational considerations (informative)

7.1 Support for closed-loop operation

Closed-loop operation enables automation of management tasks, continuous optimization, and adaptation of the behaviour of the managed entities in response to changes in internal or external conditions.

Closed loops are composed of the building blocks defined in clause 6.1.2. The management functions contribute with their respective management services capabilities to achieve the different steps of the closed loops. Closed-loop operation can happen at the management domain level, at the end-to-end service management domain level and can span across multiple management domains (including or not the end-to-end service management domain). Multiple closed loops can run simultaneously and use various subsets of the management services and management functions to realize their purpose.

Closed-loop operation can happen in the managed resources. The ZSM management framework interacts with managed resources via the producers of management services defined in "Control" and "Data collection". The specification of managed resources closed loops is out of scope of the present version of the present document.

Closed-loop operation is bounded by operational policies. The operational policies allow determining operation conditions under which autonomous operation is allowed i.e. levels of human oversight, of reporting, and conditions for escalation, delegation and coordination.

NOTE: How closed loops coordinate with each other is out of scope of the present version of the present document.

An example of closed-loop operations is described in Annex E.4. Illustrations of closed loop support are provided in Annex C.

8 Security considerations

8.1 General

Security has an end-to-end scope. It encompasses two main aspects: one is the security and privacy of data being transmitted/processed/stored within the ZSM framework and the other is the security of the ZSM framework components themselves, the so called "system security" aspect.

Providing security as a service is not within the scope of the present document.

8.2 Data security

Data could be any type of input/output that is being handled by management functions in the ZSM framework, including operational data, payloads, identity information and credentials.

Security features need to be built into management functions that handle data, for data at rest, data in transit and data in use. Protection of data in transit would preferably be handled by the integration fabric, protection of data at rest is appropriately placed in the data services. Management domains, including the end-to-end service management domain, are responsible for the protection of data in use and the end-to-end protection of data.

Features of data security:

- Management of credentials, including identities and digital certificates.
- Protection of confidentiality and integrity of data at rest, data in transit, data in use and meta data from unauthorized access and modification.
- Mutual authentication of the end-points for data in transit.
- Use of state-of-the-art cryptography:
    - NIST and industry standard cryptographic algorithms and standard modes of operations are used for cryptography, as far as possible. Using other cryptography algorithms as needed.
    - Ability to migrate to newer versions of cryptographic algorithms and protocols, with minimal impact and without disruption on running services.

8.3 Data privacy

The ZSM framework shall protect the privacy of personal data related to end users of the managed services as identified by applicable data protection and privacy regulatory laws. Additionally (see clause 5.4), the ZSM framework needs to support privacy-by-design and privacy-by-default requirements, i.e. only collecting, processing and storing the minimum amount of data needed for any function and taking necessary measures not to expose it by default (for example, as per article 25 of GDPR [i.5]).

8.4 System security

Any management function inside a management domain needs to be trustworthy. Current mechanisms to ensure this trust include access control, non-repudiation and attribution. Any ZSM management function needs to be verified initially against security-related criteria, monitored continuously and audited periodically. If the function does not meet the specified criteria, it is not allowed to be executed in the domain. If it fails subsequently in monitoring or audits, it is quarantined to mitigate the risk.

If, within a ZSM framework instance, a domain or set of domains can be trusted by default due to organizational assumptions, the aforementioned security checks can be omitted (concept of a trust boundary or "trusted domain").

Functionality needed:

- Verify security compliance.
- Monitor/Audit function.
- Allow/disallow function based on the outcome of security compliance verification, monitoring or auditing.
- Provide notifications about allow/disallow decisions.

Annex A (informative): Architecture options

A.1 Integration with legacy management systems

A.1.1 Overview

To support the end-to-end communication service, the ZSM framework potentially needs to coordinate with legacy management systems to host the legacy parts of the service. The ZSM framework should support the following options to interact with legacy management domains:

1) Integration with the domain control services at domain level.

2) Integration with cross-domain integration fabric.

A.1.2 Option 1: Legacy management domain integration using domain control services at management domain level

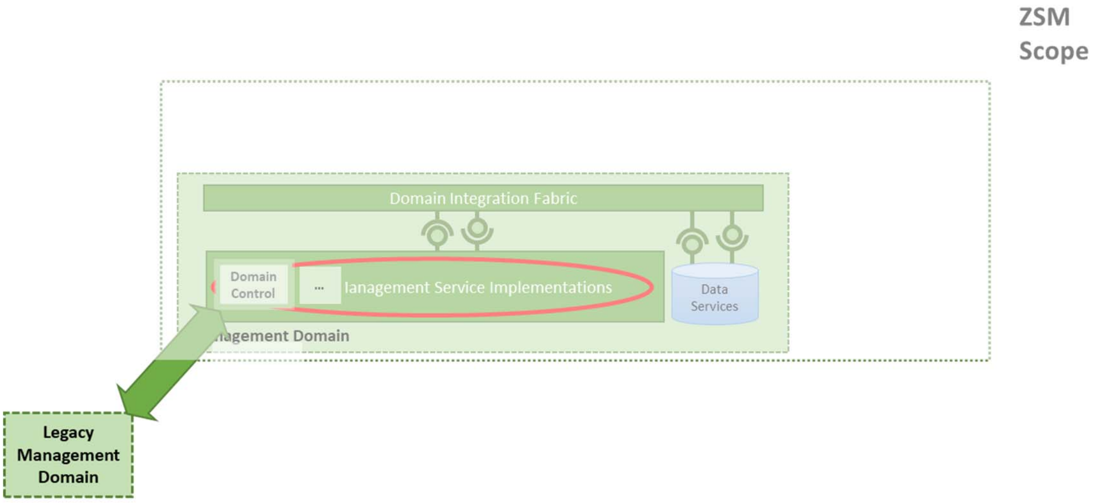


Figure A.1.2-1: Legacy management systems integration at MD - option 1

Figure A.1.2-1 depicts the first option of the high-level architecture of legacy management system integration at management domain level. In this option, the integration is inside the management domain by interacting with the domain control services of the ZSM management domain using the ZSM interfaces provided by the legacy management domain.

A.1.3 Option 2: Legacy management domain integration using a ZSM adapter

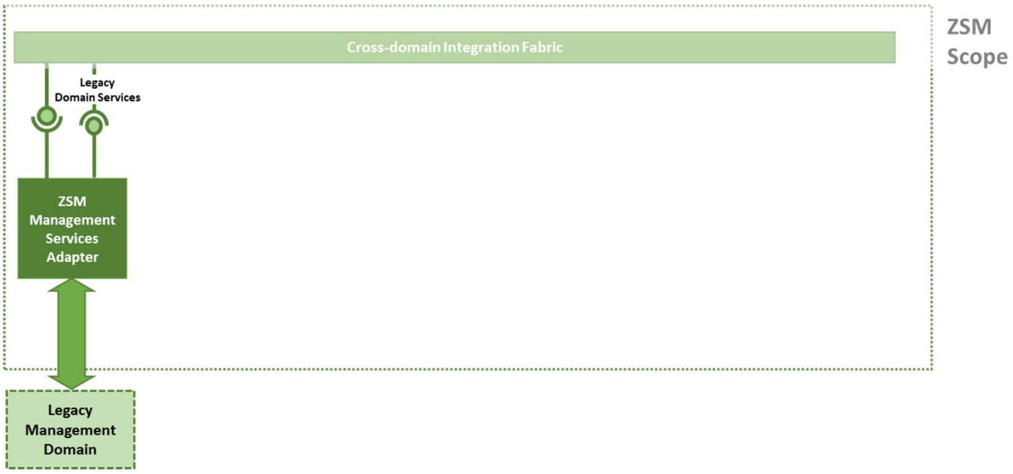

Cross-domain Integration Fabric
ZSM Scope
Legacy Domain Services
ZSM Management Services Adapter
Legacy Management Domain

Figure A.1.3-1: Legacy management systems integration - option 2

Figure A.1.3-1 depicts the second option of legacy management systems integration with the cross-domain integration fabric. In this option, the legacy management domain is considered as one of the ZSM management domains assuming that the legacy management system is able to interact via an interface adapter (i.e. legacy domain services) with the ZSM cross-domain integration fabric. The E2E service management domain manages the E2E management of the parts of service used by legacy management domains via the cross-domain integration fabric.

A.2 Examples of valid ZSM architecture deployments

A.2.1 Overview

The following clauses illustrate examples of valid deployments of the ZSM architecture.

NOTE: In the present version of the present document, only a single example is defined.

A.2.2 Example 1: Multiple recursive levels of domain hierarchies

The ZSM architecture may be configured to support multiple levels of domain hierarchies that are recursively organized.

Rationale: A management domain may be recursively composed of other management domains that still interact in accordance with the ZSM framework. Such a deployment option is enabled.

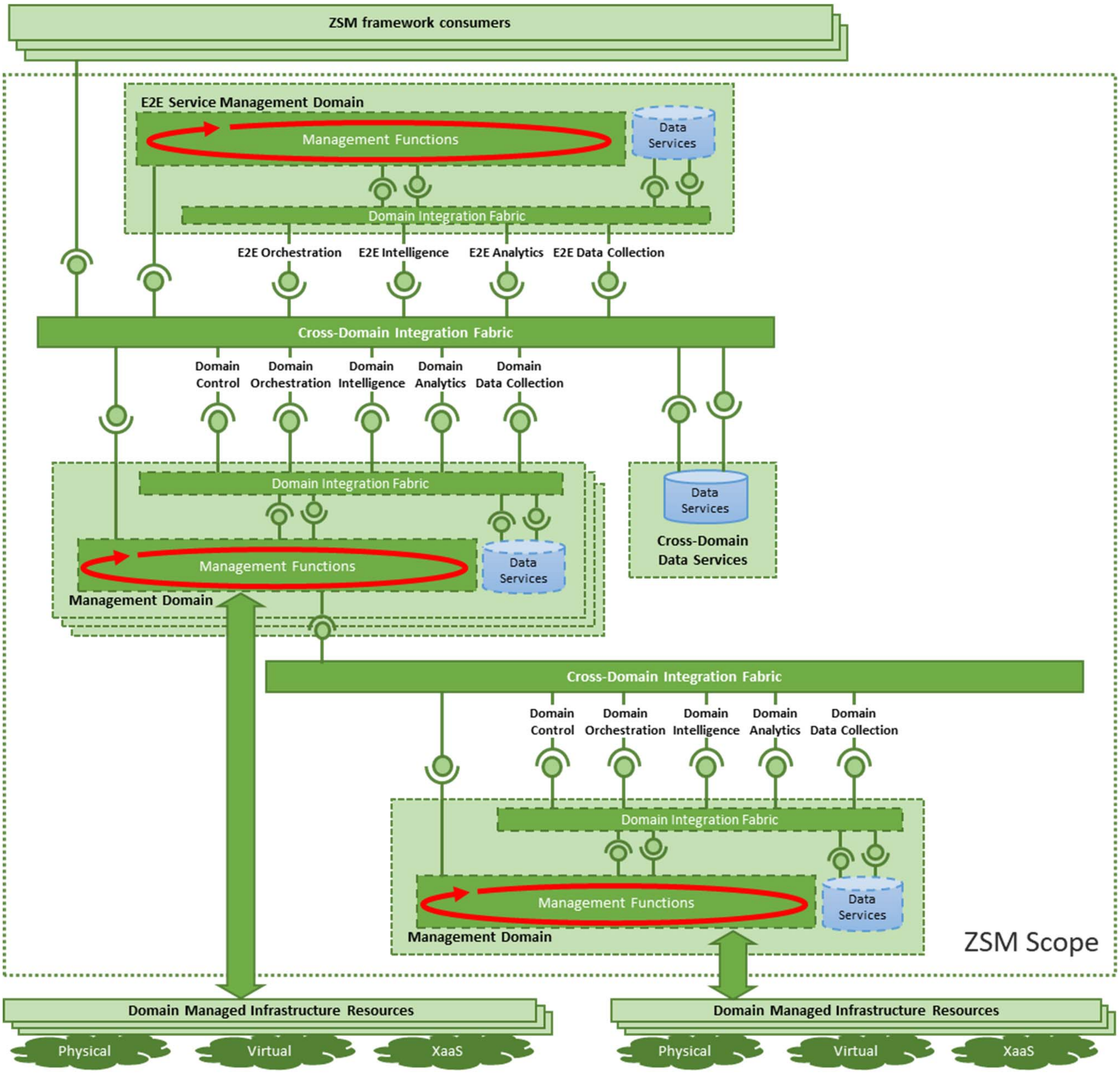


Figure A.2-1: The ZSM framework doesn't prevent management domains to be recursively stacked

As shown in figure A.2-1 the management domains in the ZSM architecture can be recursively stacked. This is also true for the E2E management domain.

Annex B (informative): Service consumption patterns

B.1 General

Providing and consuming services use particular patterns. In the scope of the present document, patterns for service registration/discovery, synchronous (request-response) interaction and asynchronous (publish-subscribe) communication are depicted in this clause.

B.2 Service registration and discovery

It is mandatory for the cross-domain integration fabric to support the registration and discovery of all management services. The integration fabric is the central registrar for management services and each service registers upon becoming active and de-registers upon deactivation. Clause E.2.2 illustrates an example of activating services in a new management domain. Management services exposed outside of a domain are registered with the cross-domain integration fabric.

A service consumer queries the integration fabric to discover the potential set of service producers available for consumption. The pattern is shown in figure B.2-1.

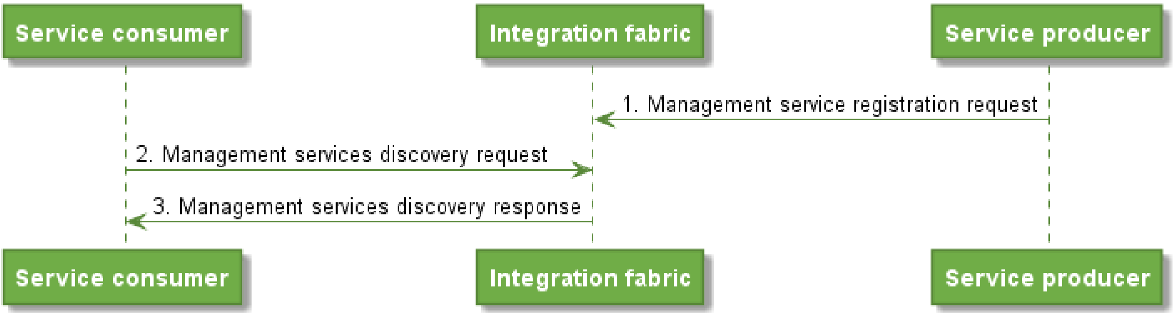

Service consumer
Integration fabric
Service producer
1. Management service registration request
2. Management services discovery request
3. Management services discovery response
Service consumer
Integration fabric
Service producer

Figure B.2-1: Registration and discovery pattern

B.3 Synchronous interactions (request-response)

It is mandatory for all exposed management service producers to be reachable to all service consumers within and across domains. After discovery and selection, a service consumer may directly access the service end-points exposed by a service producer. The pattern is shown in figure B.3-1.

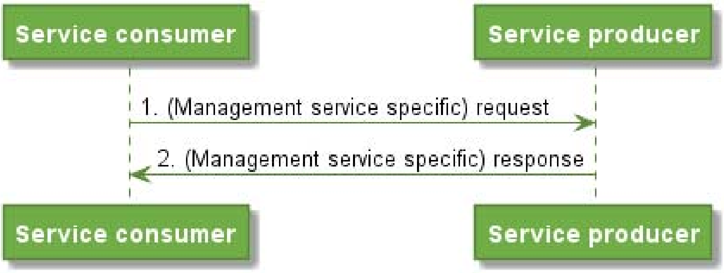

Service consumer
Service producer
1. (Management service specific) request
2. (Management service specific) response
Service consumer
Service producer

Figure B.3-1: Request-response pattern

As an alternative to direct service invocation by accessing the service end-points exposed by the service producer, the integration fabric has the capability to automatically route management service invocations and related results between service consumers and service producers while potentially taking into account load balancing, failover, security (e.g. access control), and routing rules. The management service invocation routing service is used to manage the routing rules and to invoke the service. Such indirect invocation can, in addition to routing, also include delegation of the discovery of the service itself. The pattern is shown in figure B.3-2.

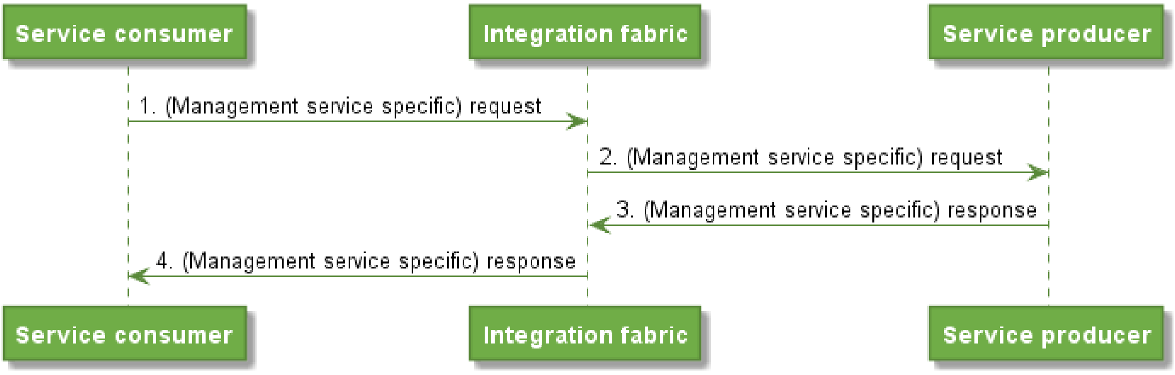

Service consumer
Integration fabric
Service producer
1. (Management service specific) request
2. (Management service specific) request
3. (Management service specific) response
4. (Management service specific) response
Service consumer
Integration fabric
Service producer

Figure B.3-2: Request-response using automatic invocation routing

B.4 Asynchronous communication (publish/subscribe) via the integration fabric

The integration fabric is a central logical entity that mediates communication between management functions (service producer and service consumer). For communication following the publish/subscribe pattern, the service producer is assumed to have the capability to provide asynchronous data (e.g. event notifications, streams) to the service consumer.

The service producer first creates one or more channels using the "manage channels" capability of the management service communication service produced by the integration fabric. Service consumers can subscribe to these channels by means of the "manage subscriptions" capability of the same service. When the service producer emits asynchronous data (such as event notifications, streams, etc.), these are consumed by the integration fabric and further provided to the subscribers which have previously registered with the management service communication service. There are two possibilities to map the capability to "provide data" to end points/message exchanges: "push" and "pull".

The "push" flow is illustrated in figure B.4-1.

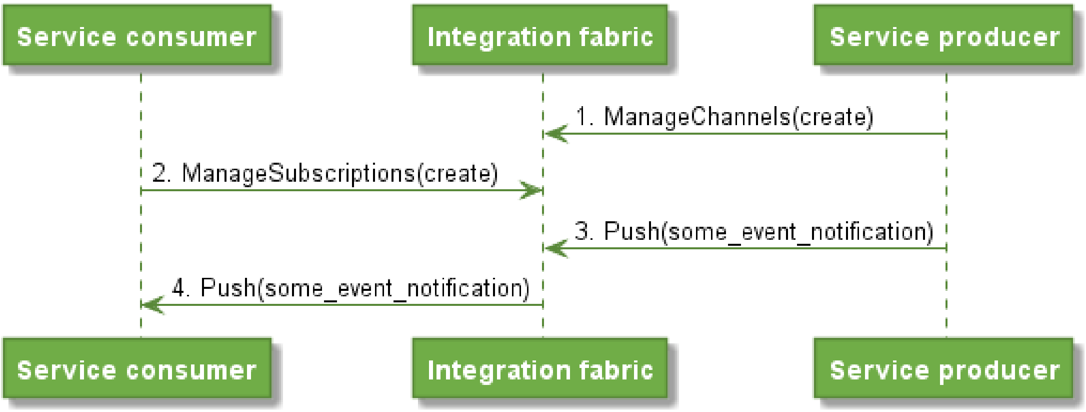

Service consumer
Integration fabric
Service producer
1. ManageChannels(create)
2. ManageSubscriptions(create)
3. Push(some_event_notification)
4. Push(some_event_notification)
Service consumer
Integration fabric
Service producer

Figure B.4-1: Publish/subscribe example via the integration fabric based on "push"

The "pull" flow is illustrated in figure B.4-2.

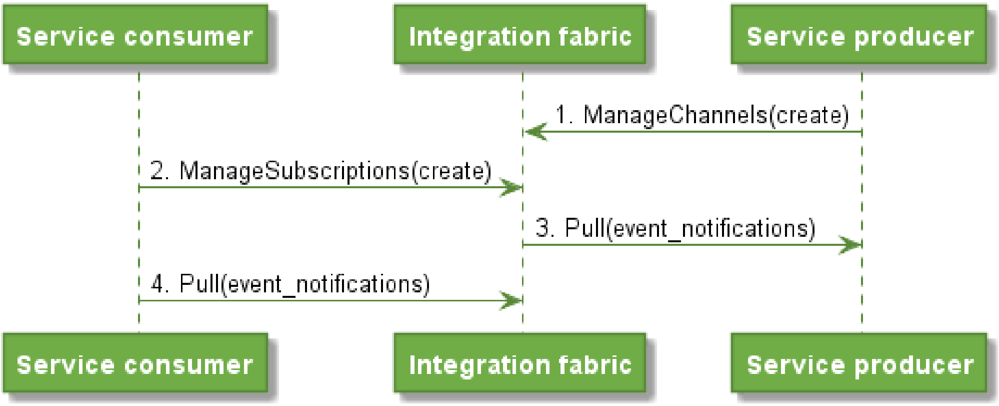

Service consumer
Integration fabric
Service producer
1. ManageChannels(create)
2. ManageSubscriptions(create)
3. Pull(event_notifications)
4. Pull(event_notifications)
Service consumer
Integration fabric
Service producer

Figure B.4-2: Publish/subscribe example via the integration fabric based on "pull"

It is also possible to mix these flows, e.g. using "push" between the service producer and the integration fabric and "pull" between the service consumer and the integration fabric.

B.5 Asynchronous communication (publish/subscribe) with subscription managed by the service producer

As an alternative to clause B.4, the capability to manage subscription can also be offered by the service producer itself. This is typically the case for management services produced by management functions that can operate in environments without an integration fabric.

In these cases, either the service consumer subscribes directly to the service producer after having discovered the service via the integration fabric (see figure B.5-1), or the integration fabric acts as mediation layer (see figure B.5-2).

The figures only illustrate "push" flows, however, "pull" flows or flows that mix both are also possible.

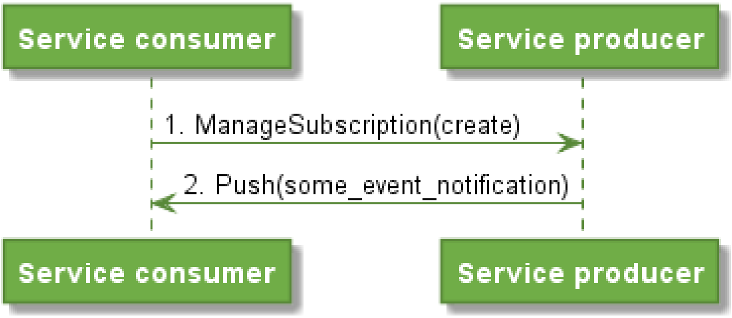


Figure B.5-1: Publish/subscribe example bypassing the integration fabric

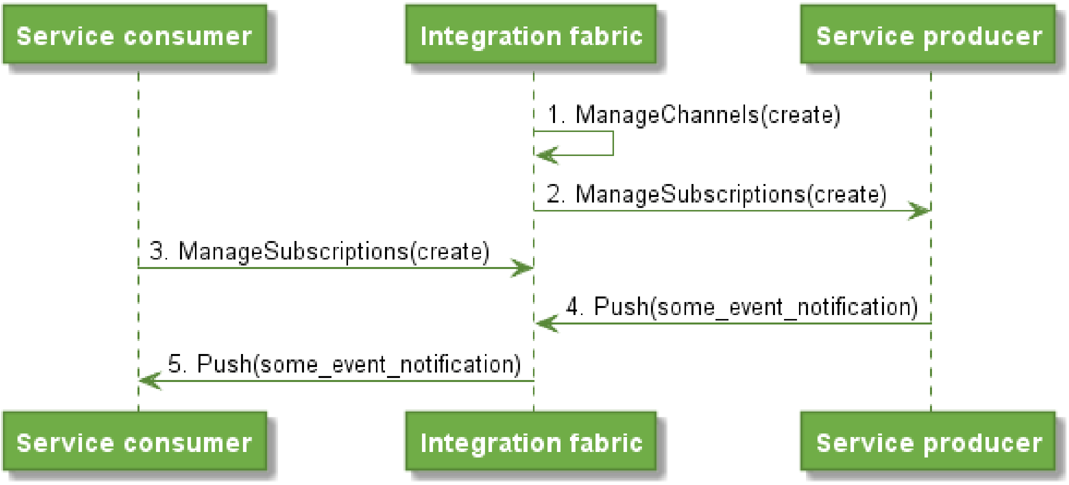

Service consumer
Integration fabric
Service producer
1. ManageChannels(create)
2. ManageSubscriptions(create)
3. ManageSubscriptions(create)
4. Push(some_event_notification)
5. Push(some_event_notification)
Service consumer
Integration fabric
Service producer

Figure B.5-2: Publish/subscribe example with subscriptions mediated by the integration fabric

NOTE: Steps 1 and 2 can be performed in any order.

Annex C (informative): Support for closed-loop operation

The end-to-end automation and zero-touch management of network services and infrastructures rely on the ability to close the management loop.

Closing the management loop implies the transfer of information, knowledge, functions and operations, such as domain knowledge, analysis, learning, reasoning, planning, or decision-making capabilities, typically owned or realized by humans to the management framework.

To achieve closed-loop operation, a management framework needs to provide means for the ordered invocation of the steps or phases of the closed loop (e.g. the Observe, Orient, Decide, Act steps of the OODA loop [i.2]), the composition of the necessary functionalities (i.e. composition of management services and functions) at each steps of the closed loop, and the transfer of/access to necessary information or commands between/by, the steps of the closed loop.

NOTE: Different closed-loop models than the OODA model exist and can be considered in support of closed-loop operation, such as e.g. MAPE-K (Monitor-Analyse -Plan-Execute plus Knowledge [i.3]) and MRACL (Model-Reference Adaptive Control Loop [i.4]).

The closed loops are composed of the building blocks defined in clause 6.1.2. The management functions contribute with their respective management services capabilities to achieve the functionality of the different steps of the closed loops as illustrated in figure C-1.

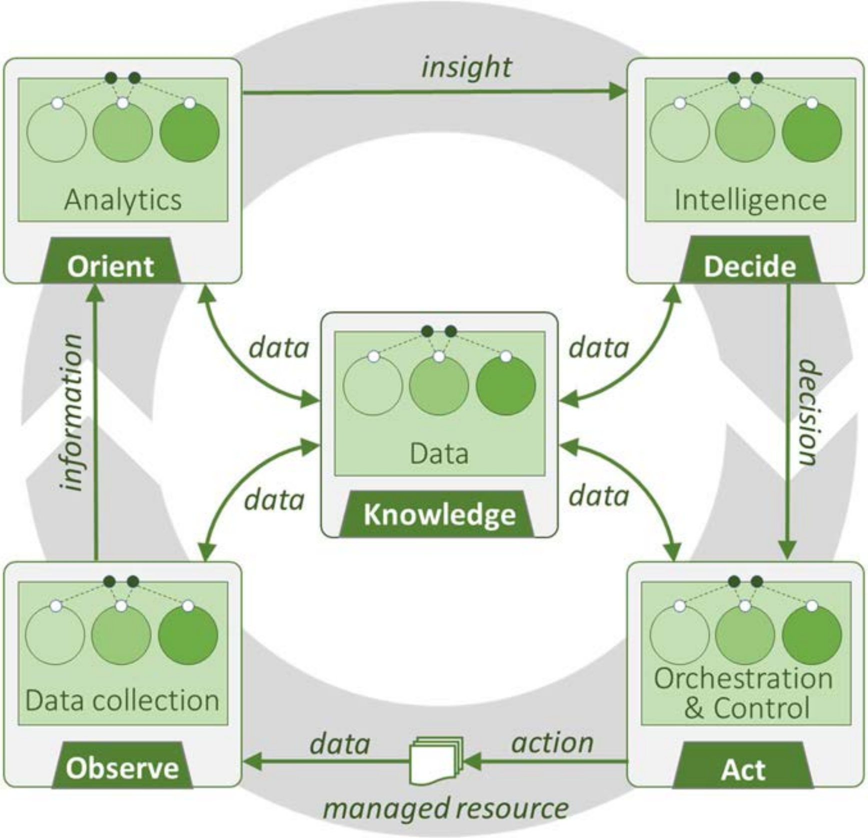
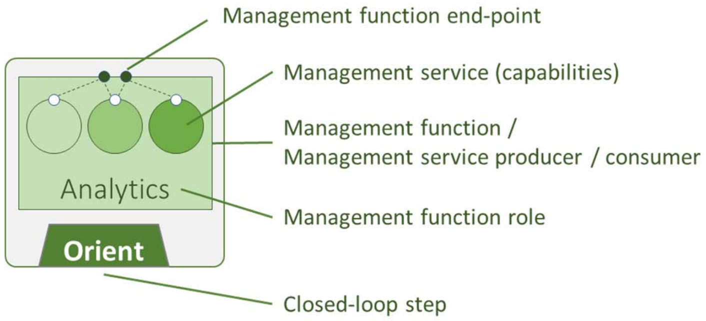


Figure C-1: Indicative mapping between architectural building blocks and closed-loop steps

Legend:


Management function end-point
Management service (capabilities)
Management function /
Management service producer / consumer
Analytics
Management function role
Orient
Closed-loop step

Different types of data can be written or read to/from the Knowledge step of the closed loop. E.g. collected data (PM), topology, insight / re-commendation, decisions, plans, workflows, etc…

The types of data depend on what the closed loop steps need to realize their function, and also what each step need to store as information indicating its activity (e.g. reports, list of actions taken, other metrics…)

NOTE: Number of end-points, services and their re-direction in figure C-1 are only illustrative.

Figure C-2: Legend for C-1

Closed-loop operation enables the management functions which are part of the loop to adapt the behaviour of the managed entities to respond to changes in user needs, business goals, internal or external conditions. Closed loops continuously observe and collect data on the managed entities, and their operating context. This enables the management functions in the loop to analyse those changes, to understand behaviour evolutions, to produce plans and decisions, and then to invoke actions to adapt the current observed state of the managed entities towards the target desired state or goal.

A closed loop performs the following functions as part of its operation:

- Observe and collect data from the managed entities, and other relevant data sources.
- Orient the processing of these data, so that their meaning and significance can be understood in the proper context.
- Analyse the collected data through filtering, correlation, and other mechanisms to define a model of past, current, and future states.
- Run machine learning algorithms to learn, recognizes patterns and make predictions on observed data.
- Plan different actions based on inferring trends, determining root causes and sequences, and similar processes.
- Decide which plan(s) to execute, and when to execute the plan(s).
- Detect and resolve conflicts between different goals.
- Collaborate with other control loops.

Closed-loop operation can happen at different granularities and scope: some closed-loop operations can happen in the managed resources such as in PNFs, VNFs or SON functions.

Managed resources closed-loop operations are acknowledged to exist; however, their specification is out of scope of the present version of the present document. The ZSM management framework interacts with managed resources via the producers of management services defined in "Control" and "Data collection".

Closed-loop operation can happen at the management domain level, at the end-to-end service management domain level and can span across multiple management domains (including or not the end-to-end service management domain level). Multiple closed loops can run simultaneously and use various subsets of the management services and management functions to realize their purpose.

Closed loops interact with managed resources through resource control services via "south bound interfaces" (SBI), with peer closed loops through "east-west" or "peer" interfaces, and with upper level closed loops through "North Bound Interfaces" (NBI). The structure of the interactions between closed loops can follow various distributivity and hierarchy models.

Closed-loop operation is defined and bounded by operational policies. Based on the capabilities exposed by the architectural building blocks, the operational policies allow determining operation conditions under which autonomous operation is allowed i.e. levels of human oversight, of reporting, and conditions for escalation and delegation. Operational conditions include specification of operational objectives, and other governance information, needed for proper service operation.

Under normal conditions, the closed loops operate within the boundaries defined by the operational policies.

Under exceptional conditions, the closed loops try to remediate to the exceptions with all possible means under their control, and within the boundaries of the operational policies. If despite having tried all possible and relevant remediation actions, the closed loop fails in solving the problem(s), it then generates an "escalation" as defined per the operational policies (target, relevant information, etc.). Beyond triggering an "upper" function or closed loop, the "escalation" action also allows conveying reporting information on remediation actions tried, augmenting the identified situation (exception) with contextual and historical information to further help the analysis by the receiving entity.

Annex D (informative): Automated discovery and consumption of management capabilities exposed from a management domain

Figure D-1 explains how the management capability exposure configuration service can be used for automated discovery and consumption of exposed management capabilities from a management domain. The logical entity in the management domains that provides this service is the domain integration fabric. The service is used to configure the entitlements of external consumers to exposed management services. It can receive this configuration from any (pre)-authorized consumer of this service (e.g. the E2E management domain or a ZSM framework consumer such as a digital store front), see figure D-1.

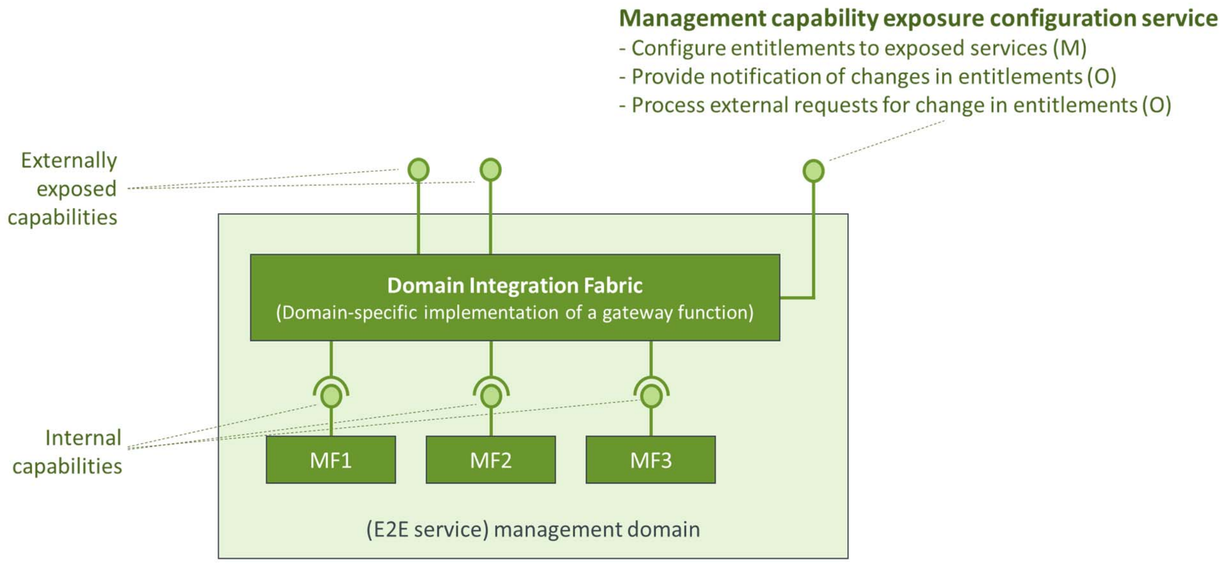

Management capability exposure configuration service
- Configure entitlements to exposed services (M)
- Provide notification of changes in entitlements (O)
- Process external requests for change in entitlements (O)
Externally exposed capabilities
Domain Integration Fabric
(Domain-specific implementation of a gateway function)
Internal capabilities
MF1
MF2
MF3
(E2E service) management domain

Figure D-1: Example of the management capability exposure configuration service

In an example deployment scenario when a new management domain is added to the network, its management capabilities (exposed ZSM services) are registered with the cross-domain integration fabric to enable cross-domain consumption. This happens as follows:

1) The set of exposed ZSM services/capabilities from the management domain are registered with the cross-domain integration fabric using the registration service therein.

2) Assume that a new E2E service is deployed with a part belonging to the respective management domain. For the part of the E2E service belonging to the management domains the E2E management domain can configure the entitlement rights to the management services, capabilities, end-points and management data.

3) A consumer can discover the exposed list of management services/capabilities offered by the management domain using the discovery service in the cross-domain integration fabric and can request the service from the management domain using the end-point information obtained during discovery.

4) Alternatively, the consumer can request access to a specific ZSM service/capability via the cross-domain integration fabric which redirects the request to the management domain.

5) The management domain's specific implementation of a gateway function (mapping to the logical component "domain integration fabric") allows the service consumer to consume the particular service capability as configured in step 2.

The entitlements of the consumer may be changed from time to time as in step 2.

Annex E (informative): Realization of selected scenarios in the ZSM framework reference architecture

E.1 Introduction

This annex illustrates how some of the use cases defined in ETSI GS ZSM 001 [i.9] can be realized in the ZSM framework reference architecture.

E.2 Example of services discovery with a new management domain

E.2.1 Objective

This clause examines how the scenario of adding a new management domain can be realized by an operator using the ZSM framework services. This scenario is related to the ZSM Scenario: "Automated detection of services offered by management domains" defined in ETSI GS ZSM 001 [i.9].

The goal of this scenario is:

1) that the management services of the new management domain are accessible over the cross-domain integration fabric to management functions in other management domains and to ZSM service consumers;

2) the management services from the other management domains are accessible to management functions in the new management domain.

E.2.2 Steps

In this scenario, the operator wants to add a new management domain (MD) to the deployed ZSM architecture instance. The following steps show an example of how the MD and its management and network services are automatically integrated into the ZSM framework:

1) The operator installs the MD with the configured address of the *end-point* for the *management services registration service* and the *management services discovery service*. This is the end of the manual steps for this scenario.

2) The MD uses the *management services registration service* to register its exposed services with the cross-domain integration fabric.

3) The MD uses the *management services discovery service* to query the available list of management services available.

Objective 2 is thereby achieved.

4) The management service consumers in other management domains that have subscribed to changes in the set of registered management services are notified by the *management services discovery service* of the newly registered management services from the new MD.

5) The other management service consumers that have not are not subscribed to change notifications of the *management services discovery service* may eventually query the *management services discovery service* to get the updated management services list.

Objective 1 is thereby achieved.

E.3 Example of a customer-facing service deployment

E.3.1 Objective

This clause demonstrates how a new customer-facing service can be deployed using the ZSM framework services. It is assumed that a digital store front is used as a ZSM framework consumer that interfaces with external customers. In addition, this scenario also demonstrates how SLS is decomposed into KPIs to be monitored in the resource level.

This is an example only (informative), and the purpose of this example is to illustrate the use of some of the ZSM management services in the present document to accomplish a customer-facing service deployment.

E.3.2 Steps

The steps of operation to deploy a customer-facing service are:

1) The operator on-boards a new E2E service in the *managed services catalogue management service*. The workflow definitions for the lifecycle of this service have been configured by the operator as part of the E2E service model creation.

2) The policies that concern this service are configured in the *policy management service* in the E2E domain.

3) Using the *managed services catalogue management service,* the new E2E service is automatically picked up by the digital store front where a product offering is created and is advertised to external customers.

4) The customer selects the product offering that will deploy the E2E service, provides the needed parameters, e.g. number of users to be supported, coverage area and so on. The manual steps regarding this scenario end here. Customer interactions in this step are out of scope of ZSM.

5) The deployment request is received by the digital store front which may choose to first perform a feasibility check whether the service can be deployed, using the *feasibility check service* in the E2E domain which may in turn delegate to *feasibility check service* in individual management domains to verify the availability and sufficient capacity of the managed resources to support the CFS.

6) If feasible, the *E2E service orchestration service* is used by the digital store front to request the deployment of the service. The *E2E service orchestration* service then delegates the deployment to the individual management domains' *domain orchestration service*. The *resource configuration management service* of the domain control may be used during the deployment process. The service is then deployed.

7) Decompose the SLSs to KPIs to be monitored using the *E2E service condition detection service*

8) The *E2E performance data reporting service* collects performance data from all the related management domains, creates an aggregated report with service-level performance information and provides it to authorized consumers (e.g. digital store front that has requested the service creation).

9) *Performance events service* and *performance measurements streaming service* from the management domain can be used by E2E service management domain to subscribe for performance measurement changes (e.g. performance degradation) in the individual resources based on the thresholds assigned for the resources.

10) The *E2E service condition detection* service sets KPI thresholds at the E2E level, and it may use the domain level performance events service to set performance events conditions (e.g. thresholds) to monitor.

11) Optionally, the digital store front may execute the *E2E testing service* to verify that the CFS deployment was successful.

E.4 Example of closed-loop operation in management domain

E.4.1 Objective

This clause examines how a closed loop can be realized in an operator's management domain using the ZSM framework services. This is an example only (informative), and the purpose of this example is to illustrate the use of some of the ZSM management services in the present document to accomplish closed-loop automation to maintain SLS assurance.

This example is modelled using some of the requirements listed in clause 4.2 in ETSI GS ZSM 001 [i.9]. The related requirements are summarized below:

- Capability to collect the performance and fault data of the network instance.
- Capability to monitor the network resources:
  - Network anomaly or undesired conditions.
  - Resource utilization (e.g. CPU, memory, etc.).
  - Performance (KPI) degradation.
- Capability to set policy conditions that need to be monitored.
- Capability of identifying root cause of a network issue.
- Capability of taking actions to mitigate network issue, including performance degradation.

In addition to the summarized requirements listed above, the "Closed-loop automation" scenario documented in ETSI GS ZSM 001 [i.9] (clause 5.2.3.9) applies.

Closed loops (observe, orient, decide, and act) allow e.g. self-optimization, improvement of network and resource utilization, and automated service assurance and fulfilment.

The goal of this example is to illustrate that the management services listed in the present document can function together to accomplish closed-loop operation:

1) Monitor the network resources (observe).
2) Upon detection of network issue, trigger analysis (orient).
3) Evaluate how to mitigate the issue and produce (re-)action plans (decide).
4) Perform the fix to solve the network issue (act).

The closed loop continues to try to fix the issue (i.e. network fault) while the anomaly persists. The closed loop may escalate to other management entities (e.g. operator intervention), in case no local solution can be found at the level of the current closed loop.

NOTE: Refer to ETSI GR ZSM 005 [i.1] for additional information regarding the principles of closed-loop automation.

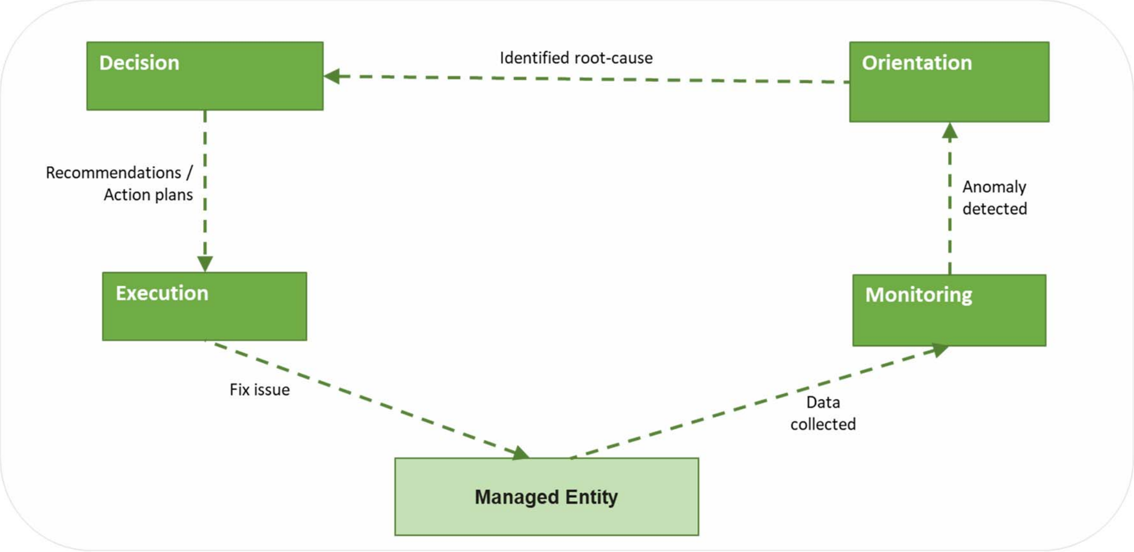


Figure E.4.1-1: High level closed-loop automation example

E.4.2 Steps

Preconditions:

- The intent is to guarantee SLS.

NOTE 1: The technology by which the intent is conveyed and the method by which the intent is decomposed into an instruction set are not defined in the present document and not described in this example.

- The setup of the "SLS assurance" closed loop consists in making sure that:
  - managed entities are monitored at real time;
  - violations of SLS metrics are detected;
  - causes of SLS metrics violations are identified and addressed automatically.

The initial setup is realized by several management service subscriptions. When triggered by events, the management services will operate together according to the operational policies.

- Domain analytics management functions subscribe to:
  - *Fault events service* - to consume information about abnormal system states originating from the infrastructure resources.
  - *Performance event service* - to consume information about events related to monitored performance conditions (e.g. if a threshold was crossed).
- (optionally) E2E Domain Analytics management functions subscribe to:
  - *Anomaly detection service* - to consume information about anomaly events from the management domain, to create a E2E closed-loop automation.

NOTE 2: This example illustrates a closed loop in the management domain level, and the E2E closed loop is not in scope of this example.

- Data services management functions subscribe to:
  - *Log collection service* - to store the log info in the data services store.
- Domain intelligence management functions subscribe to:
  - Notifications related to detected anomalies from the *anomaly detection service*.

- Domain intelligence management functions consume the *domain orchestration service ("Execute workflow"* capability*)*:
    - A domain intelligence management function makes the decision and instructs a domain orchestration management function that offers the "*Execute workflow*" capability to remediate the anomaly.

Objective 1 is thereby achieved.

Upon detection of an anomaly:

- The *reactive incident analytics service* is triggered to perform an analysis
    - As part of the analysis, other services may be invoked by the logic that performs the analysis, for example:
        - ▪ *Domain topology information service.*
        - ▪ *Data persistence services* (query) - e.g. to analyse log data.
        - ▪ *Data optimization services* - e.g. to aggregate data.
- The *reactive incident analysis service* then publishes the available data and insights.

Objective 2 is thereby achieved:

- *Domain intelligence* management functions receive the derived insights published by the *reactive incident analysis service* and make a decision and a plan of the next actions e.g. based on policy. In this example, the decision is to remediate the issue.
- A management function in *domain intelligence* consumes the *domain orchestration service (Execute workflow* capability*).* Based on the operational policy configured in the *policy management service*, the *domain orchestration service (Execute workflow)* executes a resolution workflow:
    - As part of the workflow, the following can be performed:
        - ▪ *Resource configuration management service (Configure resource).*
        - ▪ *Testing service (Test resource).*

Objectives 3 and 4 are thereby achieved.

Annex F (informative): Change history

Date	Version	Information about changes
26 Feb 2018	0.0.1	Skeleton (ZSM(18)000087r1_ZSM002_GS_Skeleton_proposal)
12 Apr 2018	0.1.0	Incorporated contributions - ZSM(18)000119r2_ZSM002_Addressing_EN_on_security_in_Architectural_Principles - ZSM(18)000120r1_ZSM002_Proposing_Architectural_Principles Editorials - Added draft disclaimer - Fixed case of headings
14 May 2018	0.2.0	Incorporated contributions - ZSM(18)000145r1_ZSM002_Arch_Principle__7_stateless_functional_components - ZSM(18)000127r3_ZSM002_Proposing_Architectural_Requirements Editorials - Fixed version indicator of 0.1.0 in history box
08 June 2018	0.3.0	Incorporated contributions - ZSM(18)000134r3_ZSM002_Proposal_for_general_architecture_requirements - ZSM(18)000146r4_ZSM002_Arch_Principles_Design_for_Failure - ZSM(18)000147r4_ZSM002_Arch_Principle__6_Separation_of_concerns_in_managemen - ZSM(18)000170r5_ZSM002_Architecture_requirements_related_to_telemetry - ZSM(18)000236r2_ZSM002_Proposal_on_the_overview_and_architecture_of_ZSM_fram Editorials - Removed empty annex A
16 July 2018	0.4.0	Incorporated contributions - ZSM(18)000253r2_ZSM002_principles_vs_requirements_removing_redundancy - ZSM(18)000254_ZSM002_add_reference_to_terminology_WI - ZSM(18)000259r1_ZSM002_domain_assurance_split_off_from_250 - ZSM(18)000276r2_ZSM002_Domain_Concept - ZSM(18)000301r4_ZSM002_Architectural_abstraction recursion - ZSM(18)000310r1_ZSM002_Additional_architectural_principle_about_intend-base - ZSM(18)000325r2_ZSM002 Proposed ZSM Architecture Diagram Changes v6 Editorials - Consistent terminology: changed "functional block" to "functional component".
31 July 2018	0.4.5	Incorporated contributions - ZSM(18)000333r2_ZSM002_Architecture_clause_restructuring Additional harmonization change by rapporteur: - Harmonized "Exposed management services" and "Provided management services" in the headings, both were used in CR 333r2, using now "Provided" consistently as not all "provided" services are also "exposed". Also, reflected this difference in the EN in 6.5.
03 Sept 2018	0.5.0	Incorporated contributions - ZSM(18)000340r4_ZSM002_integration_fabric_details - ZSM(18)000351_ZSM002_Management_service_template_update
05 Sept 2018	0.5.1	Changes - Updated history box - Fixed errors in the implementation of document 351 in the clean version of the GS

Date	Version	Information about changes
16 Sept 2018	0.6.0	Incorporated contributions - ZSM(18)000267r5_ZSM002_domain_assurance_more_details - ZSM(18)000269r5_ZSM002_domain_orchestration_more_details - ZSM(18)000270r3_ZSM002_domain_control_more_details - ZSM(18)000281r3_ZSM002_Common_Data_Services_description - ZSM(18)000357r1_ZSM002_rapporteur_s_clean-up - ZSM(18)000358r1_ZSM002_streaming_fixes - ZSM(18)000361r2_ZSM002_details_of_management_domain_provisioning - ZSM(18)000373r1_ZSM002_domain_intelligence_description - ZSM(18)000375r2_ZSM002_Anomaly_Detection_service_provided_by_Domain_Assuranc - ZSM(18)000377r1_ZSM002_Policy_administration_service_provided_by_Domain_Inte - ZSM(18)000380r2_ZSM002_Add_initial_list_of_External_Services_to_the_Manageme Editorials - Clause numbering fixes - Missing "the" - Added table references where missing. - Replaced leftovers of "EXTERNAL" by "EXPOSED"
02 Oct 2018	0.6.1	Incorporated contributions - ZSM(18)000354r1_ZSM002_E2E_Service_Mgmt_Domain_Overview - ZSM(18)000382r1_ZSM002_5_4_3_Functional_requirements_for_Common_Data_Service - ZSM(18)000383r1_ZSM_002_5_4_3_Functional_requirements_for_Common_Data_Servic
08 Oct 2018	0.6.2	Incorporated contributions - ZSM(18)000251r4_ZSM002_service_groups_in_E2E_service_domain - ZSM(18)000252r4_ZSM002_data_services
30 Oct 2018	0.7.0	Incorporated contributions - ZSM(18)000374r4_ZSM002_Conflict_resolution_service_provided_by_Domain_Intell - ZSM(18)000385r2_ZSM002_5_4_3_Functional_requirements_for_Common_Data_Service - ZSM(18)000386r1_ZSM002_5_4_3_Functional_requirements_for_Common_Data_Service - ZSM(18)000391r3_ZSM002_-_Considerations_on_an_abstraction_principle - ZSM(18)000399r1_ZSM002_PM_and_measurements_services_split_off_from_267r2 - ZSM(18)000402r2_ZSM002_Harmonization_of_managed_entities__resources_and_cons - ZSM(18)000410r1_ZSM002_Design_for_resilience_principle - ZSM(18)000418r1_ZSM002_data_processing_in_data_services_split_from_252r1 - ZSM(18)000423r1_ZSM002_Adapting_the_scope - ZSM(18)000429r3_ZSM002_Integration_Fabric_Pub_Sub_Services - ZSM(18)000432r3_ZSM002_Network_Capability_Inventory_Service - ZSM(18)000434r2_ZSM002_details_of_Configuration_data_generation_service - ZSM(18)000435r2_ZSM002_Testing_service - ZSM(18)000436r3_ZSM002_E2E_testing_service - ZSM(18)000437r6_ZSM002_Some_services_provided_by_E2E_service_intelligence - ZSM(18)000442r3_ZSM002_clarify_capability_of_domain_orchestration_and_some_c - ZSM(18)000445r2_ZSM002_Management_service_related_to_network_service_orchest - ZSM(18)000446r2_ZSM002_Management_service_related_to_service_performance_ass - ZSM(18)000452r2_ZSM002_Add_Feasibility_check - ZSM(18)000453r1_ZSM002_Catalog_Managment_Service - ZSM(18)000458r4_ZSM002_Data_abstraction_service_provided_by_Domain_Assurance - ZSM(18)000459_ZSM002_Add_the_abbreviations_of_AI_and_ML - ZSM(18)000465r2_ZSM002_5_3_1_Non-functional_requirements_for_Common_Data_Ser

Date	Version	Information about changes
		- ZSM(18)000467r1_ZSM002_5_3_2_Non-functional_requirements_for_Common_Data_Ser - ZSM(18)000468r1_ZSM002_5_3_2_Non-functional_requirements_for_Common_Data_Ser - ZSM(18)000471r2_ZSM002_5_5_Security_requirements - ZSM(18)000473r2_ZSM002_Principle_Security_changed_to_Requirements - ZSM(18)000476r3_ZSM002_E2E_Assurance_services - ZSM(18)000477r2_ZSM002_E2E_Intelligence - ZSM(18)000490r1_ZSM002_Structure_fix_for_Integration_fabric_and_Data_Service - ZSM(18)000499r1_ZSM002_merge_of_430_and_455__Integration_fabric_services - ZSM(18)000501r1_ZSM002_ZSM_Architecture_Diagram_Changes - ZSM(18)000502r1_ZSM002_part_of_ZSM_18_000415r1 - ZSM(18)000506_ZSM002_remove_provided_by Editorials
7 Nov 2018	0.7.1	Incorporated contributions - ZSM(18)000464r1_ZSM002_5_4_3_Functional_requirements_for_Common_Data_Service - ZSM(18)000469r1_ZSM002_5_3_1_General_non-functional_requirements - ZSM(18)000470r1_ZSM002_5_3_1_General_non-functional_requirements Fixing the allocation of the content from ZSM(18)000437r6 to the wrong clause (moved to 6.6.5.2.x from 6.5.5.2.x) Editorials and term alignments - network resource -> infrastructure resource - unsubscribe "from"
11 Dec 2018	0.8.0	Incorporated contributions - ZSM(18)000484r1_ZSM002_Leftover_changes_from_484 - ZSM(18)000520_ZSM002_Integration_Fabric_Text_Correction - ZSM(18)000538r2_ZSM002_Resolve_EN_6_6_6_2_2_Align_orchestration_services - ZSM(18)000541r2_ZSM002_Resolve_EN_6_2_Architecture_explanation - ZSM(18)000542_ZSM002_Resolve_EN_5_3_2_Non-functional_reqs_for_CDS - ZSM(18)000543r5_ZSM002_Normative_Aspects_Within_Clause_6 - ZSM(18)000556r1_ZSM002_Resolve_EN_6_5_4_Term__assurance - ZSM(18)000559r1_ZSM002_Changes_to_scope - ZSM(18)000560_Changes_to_references - ZSM(18)000561r3_ZSM002_Changes_to_principle_04 - ZSM(18)000563r1_ZSM002_Changes_to_principle_08 - ZSM(18)000576r2_ZSM002_AI_model_management_service_by_E2E_service_intelligen - ZSM(18)000593r1_ZSM002_Clean_up_Harmonize_CRUDL_or_Manage - ZSM(18)000595r1_ZSM002_Add_example_of_closed_loop_operation - ZSM(18)000596r2_ZSM002_Add_capabilities_to_Analytics_Service - ZSM(18)000597r2_ZSM002_Add_example_of_integrating_a_new_MD - ZSM(18)000600r2_ZSM002_Resolve_EN_6_5_Interaction_with_legacy - ZSM(18)000601r2_ZSM002_Add_E2E_SLA_Management - ZSM(18)000603r2_ZSM002_5_5_Security_requirements - ZSM(18)000607r3_ZSM002_rapporteur_s_simple_clean-up_changes_and_ENs_deletion Editorials - Corrected hanging paragraphs introduced by document 543r5. - Clause 6.2: Replaced one simple sentence introduced by document 541r1 ("Related end-points are logically grouped.") by its more detailed variant expressed in 543r5 ("Each of the logical groups of management service end-points contains end-points with related functionality.") to avoid redundancy. - Document 559: Replaced "this document" by "the present document". - Added missing captions - Added missing abbreviations: MD, CDS, CRUD, SLA, EP - Fixed references to ZSM001

Date	Version	Information about changes
08 Jan 2019	0.8.5	Incorporated contributions - ZSM(18)000562r2_ZSM002_Changes_to_principle_06_and_new_requirement - ZSM(18)000631r1_ZSM002_Remove_EN - ZSM(18)000639_ZSM002_deleting_internal_details_of_DSF
05 Feb 2019	0.9.0	Incorporated contributions - ZSM(18)000478r2_ZSM002_Domain_Intelligence_alignment_with_477r2 - ZSM(18)000539r4_ZSM002_Remove_functional_components - ZSM(18)000578r3_ZSM002_Add_MD_catalogue_management_service - ZSM(18)000602r3_ZSM002_Add_KPIs_list_into_Performance_measurements_streaming - ZSM(18)000610r7_ZSM002_Further_architecture_building_block_refinement_and_al - ZSM(18)000640r2_ZSM002_rapporteur_s_clean_up_after_ZSM_05 - ZSM(19)000019r1_ZSM002_Proposal_for_network_slice_lifecycle_management_servi - ZSM(19)000021r1_ZSM002__E2E_Policy_mgmt_service - ZSM(19)000036r1_ZSM002_definitions_from_539r2 - ZSM(19)000038r1_ZSM002_more_definitions Editorials - Added "void" to Symbols clause - Cleaned up empty table rows
11 Feb 2019	0.9.1	Incorporated contributions - ZSM(19)000051_ZSM002_Rapporteur_s_clean-up_after_v_0_9_0 - ZSM(19)000042r1_ZSM002_adding_a_conventions_clause
25 Feb 2019	0.9.2	Incorporated contributions - ZSM(19)000059_ZSM002_applying_external_visibility_convention_to_all_servic - ZSM(18)000564r1_ZSM002_Changes_to_event_category_configuration_service - ZSM(19)000022r2_ZSM002_Add_and_update_condition_managment_service On top of implementing the CR, rapporteur has aligned the use of external visibility in clause 6.5.5.2.3 with the convention, has aligned the description of the "Manage condition" operation in 6.6.5.2.4 with that in 6.5.5.2.3 and has aligned the description of the CRUD pattern with the other occurrences in the document.
20 Mar 2019	0.10.0	Incorporated contributions - ZSM(18)000511r2_ZSM002_E2E_Assurance_-_Anomaly_detection - ZSM(18)000587r7_ZSM002_Clean_up_Discuss_and_accept_options_for_consistently_ - ZSM(18)000589r2_ZSM002_Lifecycle_change_report_provided_by_orchestration_ser - ZSM(18)000610r7_ZSM002_Further_architecture_building_block_refinement_and_al (this contribution was already implemented in V 0.9.0, but Change 0 has been missed. This change is implemented in V 0.10.0) - ZSM(19)000039r3_ZSM002_Proposed_changes - ZSM(19)000068r1_ZSM002_Rapporteur_s_clean-up_of_V092 - ZSM(19)000069r2_ZSM002_Changes_to_support_ML - ZSM(19)000070r1_ZSM002_Rapporteur_resolving_ENs_part_1 - ZSM(19)000071r2_ZSM002_align_catalogue_management_services - ZSM(19)000072r1_ZSM002_Proposal_to_restructure_the_Misc_group - ZSM(19)000075r1_ZSM002_Streamlining_the_Data_Services_clause - ZSM(19)000078r1_ZSM002_Removing_EN_about_E2E_service_catalog_in_CDS - ZSM(19)000079r2_ZSM002_Streamlining_the_Integration_fabric_clause - ZSM(19)000080r3_ZSM002_Ingest_service_model - ZSM(19)000084r2_ZSM002_Changes_to_architeture_diagram (also, replaced all occurrences of "common data services" with "cross-domain data services" as an editorial action) - ZSM(19)000085r1_ZSM002_Changes_to_clause_3 - ZSM(19)000086r1_ZSM002_Changes_to_clause_4_and_5 - ZSM(19)000087r1_ZSM002_Adding_available_network_topology_service - ZSM(19)000090r1_ZSM002_common_data_services_definition - ZSM(19)000094r1_ZSM002_Clarification_and_Modifications_on_data_services_in - ZSM(19)000096r1_ZSM002_Func-Gen-07_small_modification - ZSM(19)000100_ZSM002_Changes_in_domain_orchestration_services

Date	Version	Information about changes
		- ZSM(19)000103r1_ZSM002_gap_requirements_for_service_integration - ZSM(19)000112r1_ZSM002_Adding_capabilities_for_defining_policies_for_access_ - ZSM(19)000113_ZSM002_check_and_reserve_optional - ZSM(19)000114_ZSM002_Moving_data_optimization_service - ZSM(19)000126r1_ZSM002_Additional_general_non-functional_requirements__chapt - ZSM(19)000127r1_ZSM002_Additional_general_non-functional_requirements__chapt - ZSM(19)000137r1_ZSM002_Align_AI_model_management Editorials - Typos and wrong capitalizations - Consistently "notification about" not "notification of". - Put CRUDL always in the same sequence. - Align table captions.
26 Mar 2019	0.10.1	Incorporated contributions - ZSM(19)000088r3_ZSM002_Changes_to_domain_analytics_services - ZSM(19)000097r2_ZSM002_E2E_service_topology_management_service - ZSM(19)000166_ZSM002_Fixing_the_issue_with_contribution_126r1 - ZSM(19)000150r1_ZSM002_alternative_resolution_for__managed_domain__from_cont - ZSM(19)000155r1_ZSM002_Executing_the_removal_of_Category - ZSM(19)000164r1_ZSM002_rapporteur_s_clean-up_after_v_0_10_0 - ZSM(19)000165_ZSM002_consistent_terminology Editorials - Added authors missed when creating V 0.10.0
01 Apr 2019	0.10.2	Incorporated contributions - ZSM(19)000045r5_ZSM002_architecture_mods_to_align_with_requirements - ZSM(19)000116r2_ZSM002_Analytics_service_capabilities_update - ZSM(19)000134r2_ZSM002_scope_update - ZSM(19)000135r2_ZSM002_6_1_2_4_service_composition_update - ZSM(19)000136r2_ZSM002_SLA_management_update - ZSM(19)000138r1_ZSM002_E2E_testing_service_fixes - ZSM(19)000156_ZSM002_changes_to_exposure_function_pulled_out_from_0070 - ZSM(19)000163r1_ZSM002_data_services_condition_fix Editorials - Added authors missed when creating V 0.10.1 - Fixed typos etc. - Deleted empty Bibliography annex - Terminology: producer service -> service producer; consumer service -> service consumer - Consistently using "provide notifications" (plural) - Consistently using "Manage subscriptions" pattern "Manage (create, read, update, delete, list) subscriptions to xyz"
02 May 2019	0.11.0	Incorporated contributions - ZSM(18)000309r4_ZSM002_Additional_architectural_principle_about__designed_fo - ZSM(19)000015r5_ZSM002_Integration_Fabric_Patterns - ZSM(19)000032r3_ZSM002_Management_communication_service_to_solve_pub-sub_deb - ZSM(19)000048r3_ZSM002_Annex_E2E_Closed_Loop_Example - ZSM(19)000049r2_ZSM002_Annex_Deploy_a_new_CFS_Example - ZSM(19)000074r3_ZSM002_removing_note_about_external___internal_services - ZSM(19)000082r7_ZSM002_Changes_to_AI_model_service - ZSM(19)000089r3_ZSM002_data_store_types_discovery_and_data_store_creation_in - ZSM(19)000115r7_ZSM002_Adding_introductory_text_on_data_services (added to 6.4.1) - ZSM(19)000119r6_ZSM002_Adding_Analytics_and_Intelligence_services - ZSM(19)000124r5_ZSM002_Update_to_exposure_service - ZSM(19)000128r3_ZSM002_Additional_architecture_principle__section_4_2 - ZSM(19)000152r3_ZSM002_Modifications_related_to_discussion_in_141

Date	Version	Information about changes
		- ZSM(19)000171r1_ZSM002_Catalog_alignment_and_modifications - ZSM(19)000172r2_ZSM002_Removing_category_part_2 - ZSM(19)000173_ZSM002_Fixing_network_inventory_service - ZSM(19)000176r2_ZSM002_applying_analytics_pattern_proposed_in_132 - ZSM(19)000177r2_ZSM002_simplifying_events_services_in_domain_data_collection - ZSM(19)000178_ZSM002_NFR_small_fixes - ZSM(19)000179_ZSM002_Inventory_in_E2E_service_MD - ZSM(19)000180r1_ZSM002_resolving_the_EN_on_SLA__SLO_and_SLS - ZSM(19)000181r1_ZSM002_Merge_Exposure_and_Discovery_Services - ZSM(19)000183r1_ZSM002_Update_domain_intelligence_and_E2E_service_intelligen - ZSM(19)000188r1_ZSM002_editorial_modifications_of_management_domains_concept - ZSM(19)000193r1_ZSM002_Update_to_condition_detection_service - ZSM(19)000195r2_ZSM002_update_of_service_feasibility_check - ZSM(19)000196r2_ZSM002_update_security_requirements - ZSM(19)000199r2_ZSM002_closed_loops_support (put into a different annex than A.3.1 as it does not really fit the scope of A.3 anymore after applying another change) - ZSM(19)000200r3_ZSM002_E2E_fault_events_exposure - ZSM(19)000202r2_ZSM002_security_principle - ZSM(19)000203r2_ZSM002_Informative_examples_on_ZSM_deployment_architectures - ZSM(19)000204r1_ZSM002_Data_services_security_capability - ZSM(19)000206_ZSM002_security_anomalies - ZSM(19)000207r1_ZSM002_Management_data_communication_pattern_complementing.docx - ZSM(19)000208_ZSM002_adding_list_to_manage_policies - ZSM(19)000213r1_ZSM002_Removing_category_part_3__leftovers_from_172r1 - ZSM(19)000215_ZSM002_Figure_changes_pulled_out_from_152r1 - ZSM(19)000216r1_ZSM002_Data_Security - ZSM(19)000217r2_ZSM002_closed_loops_support_-_main_body - ZSM(19)000236_Correction_to_124r5_pre-approved_changes Editorials - Fixed hanging paragraphs in Annex A - Added missing informative reference ZSM005 - Corrected typos - Fixed history box that was not recording all previously implemented contributions
07 May 2019	0.12.0	Status: Proposed Stable draft. Incorporated contributions - ZSM(19)00191r4 ZSM002 Annex - Example of how management capability exposure service works - ZSM(19)000221r1_ZSM002_add_analytics_services_from_discussion_part_of_176 - ZSM(19)000227r4 Functional requirements Lawful Intercept - ZSM(19)000232r1_ZSM002_ENs_removal_for_stable_draft - ZSM(19)000237r2_ZSM002_rapporteur_s_clean-up_of_V0110 - ZSM(19)000240r2_ZSM002_Delete_Annex_D Editorials - Consistent use of "closed loop" vs. "closed-loop" - Fixed the colouring of the closed loops figure
04 June 2019	0.12.1	Status: Stable Draft Editorials: - Cleaned up by editHelp! - Editorial changes by rapporteur - Removed "Authors and contributors" annex F as per ISG decision documented in ZSM(19)000252 - Included editorial changes in ZSM(19)000284

28 June 2019	0.13.0	Status: Stable Draft Incorporated contributions - ZSM(18)000583r8_ZSM002_Virtualized_resources_lifecycle_management_service_in - ZSM(19)000147r3_ZSM002_Architectural_requirements_around_service_integration - ZSM(19)000220r3_ZSM002_update_security_requirements_pulled_out_from_196 - ZSM(19)000226r3 Replace SLA with SLS - ZSM(19)000270r1_ZSM002_Fixing_condition_detection_service - ZSM(19)000271r2_ZSM002_Rewriting_description_of_intelligence_clause - ZSM(19)000272r1_ZSM002_Fixes_to_architecture_principles - ZSM(19)000273r1_ZSM002_Fixes_to_non-functional_requirements - ZSM(19)000274r1_ZSM002_Fixes_to_6_1_2_2_Management_services - ZSM(19)000276r1_ZSM002_Fixes_to_5_3_3_Functional_requirements_for_CDS - ZSM(19)000277_ZSM002_Fixes_to_6_ZSM002_Fixes_to_6_1_2_5_Integration_fabric - ZSM(19)000278r1_ZSM002_Generalizing_DSF_to_ZSM_framework_consumer - ZSM(19)000281r3_ZSM002_Fixes_to_5_4_Security_requirements - ZSM(19)000283r1_ZSM002_Fixes_to_8_Security_considerations - ZSM(19)000285r2_ZSM002_Review_part_1 - ZSM(19)000288_ZSM002_Fixes_to_3_1_Definitions - ZSM(19)000291r1_ZSM002_Fixes_to_6_1_2_4_Management_domains - ZSM(19)000292r1_ZSM002_Fixes_to_6_3_Integration_fabric - ZSM(19)000293r1_ZSM002_Fixes_to_6_4_Data_services - ZSM(19)000294r2_ZSM002_Fixes_to_6_5_4_Domain_data_collection - ZSM(19)000295_ZSM002_Fixes_to_6_5_5_Domain_analytics - ZSM(19)000296_ZSM002_Fixes_to_Manages_services_catalog_management_service - ZSM(19)000297r1_ZSM002_Harmonizing_AI_and_ML_related_services - ZSM(19)000298r1_ZSM002_Small_fixes_to_testing_service - ZSM(19)000299_ZSM002_Fixes_to_6_5_8_Domain_control - ZSM(19)000301r1_ZSM002_Fixes_to_6_6_1_Overview_of_E2E_domain - ZSM(19)000302_ZSM002_Fixes_to_6_6_5_2_1_E2E_Analytics_services - ZSM(19)000303_ZSM002_Removing_separate_workflow_management_from_E_3_2 - ZSM(19)000304_ZSM002_Replacing_Legacy_domain_EPs_with_capabilities - ZSM(19)000305r1_ZSM002_Removing_the_word__required - ZSM(19)000306r1_ZSM002_Review_part_2__definition - ZSM(19)000307r1_ZSM002_Review_part_3_change_proposals_after_drafting - ZSM(19)000309r2_ZSM002_Review_part_5_remaining_changes_after_drafting - ZSM(19)000310r1_ZSM002_Review_part_6_remaining_comments - ZSM(19)000311r1_ZSM002_Fixes_to_5_3_5_LI_requirements - ZSM(19)000312r1_ZSM002_Fixing_4_2_9_Principle_09 - ZSM(19)000313_ZSM002_Fixes_to_6_1_2_7_E2E_domain - ZSM(19)000315r2_ZSM002_Fixes_to_6_4_2_3_Data_processing_service - ZSM(19)000316r1_ZSM002_Removing_redundancy_related_to_domain_data_services_a - ZSM(19)000317r1_ZSM002_Fixes_to_6_5_5_2_3_Data_optimization_service - ZSM(19)000318_ZSM002_Fixes_to_6_5_6_2_4_and_6_6_6_2_3_Health_issue_reporti - ZSM(19)000319r1_ZSM002_Fixes_to_6_5_7_Domain_orchestration - ZSM(19)000320r2_ZSM002_Fixes_to_inventory_and_topology_services - ZSM(19)000322r1_ZSM002_Fixes_to_6_5_8_2_1_Configuration_management_service - ZSM(19)000323_ZSM002_Fixes_to_6_6_4_1_Description_of_E2E_service_data_coll - ZSM(19)000324r1_ZSM002_Resolve_EN_in_6_6_5_2_1 - ZSM(19)000326r2_ZSM002_Missing_IF_Service_for_Routing_Service_Requests - ZSM(19)000327_ZSM002_Fixes_to_6_5_7_2_2_Feasibility_check_service - ZSM(19)000328_ZSM002_Fixes_to_6_5_9_2_1_and_6_6_8_2_1_Policy_management_se

Date	Version	Information about changes
		- ZSM(19)000330r1_ZSM002_Fixes_to_5_3_4_Functional_requirements_for_cross-doma - ZSM(19)000331_ZSM002_Editorial_Fixes_to_A_2_1_Overview - ZSM(19)000332r2_ZSM002_Clarification_of_management_service_implementation - ZSM(19)000333r2_ZSM002_Clarity_and_readability_of_introductory_materlals_in_ - ZSM(19)000334r2_ZSM002_Fixes_to_clause_1__3__4_and_5 - ZSM(19)000335r2_ZSM002_Fixes_to_clause_6_3 - ZSM(19)000336r2_ZSM002_Fixes_to_clause_6_4 - ZSM(19)000337r1_ZSM002_Fixes_to_clauses_6_5_3_and_6_5_4 - ZSM(19)000339r1_ZSM002_Fixes_to_clause_A_2_2 - ZSM(19)000350_ZSM002_Remove_ENs_in_6_3_2 - ZSM(19)000351r1_ZSM002_Add_Missing_Capability_to_Management_communication_se - ZSM(19)000363r2_ZSM002_Fixes_to_clause_6_5_7_1_domain_orchestration_descript - ZSM(19)000364r2_ZSM002_Fixes_to_clause_E_4_2_Steps_in_the_example_of_closed - ZSM(19)000365r1_ZSM002_Fixes_to_clause_6_5_5_2_1_domain_analytics_services - ZSM(19)000368r1_ZSM002_Correction_of_the_MCEC_service - ZSM(19)000378_ZSM002_Clause_6_3_2_1_comments - ZSM(19)000379r1_ZSM002_Clause_6_3_2_2_comments - ZSM(19)000380r2_ZSM002_Clause_6_3_2_3_comments - ZSM(19)000381_ZSM002_Adding_missing_condition_in_6_3_2_3_Management_commun - ZSM(19)000382_ZSM002_Clause_1_comments - ZSM(19)000385r2_ZSM002_domain_integration_fabric_as_exposure_gatekeeper - ZSM(19)000387r2_ZSM002_Clause_6_4_1_comments - ZSM(19)000388_ZSM002_Clause_6_4_2_comments - ZSM(19)000389r1_ZSM002_Clause_6_5_7_2_5_comments - ZSM(19)000390r2_ZSM002_Clause_6_5_4_2_4_comments - ZSM(19)000391_ZSM002_Sec-03_split_out_from_document_281r2 - ZSM(19)000396_ZSM002_delete_application_level_services - ZSM(19)000397_ZSM002_fixes_to_common_data_services_on_top_of_336r2 - ZSM(19)000398r2_ZSM002_exposure_control_attempt_2 Editorials: - Editorial changes by rapporteur (traced with username r0-rapp) - Fixes to history box
03 July 2019	0.13.5	Status: Stable Draft Incorporated contributions: - ZSM(19)000404r1_ZSM002_rapporteur_s_cleanup_after_Santa_Clara_meeting - ZSM(19)000275_ZSM002_Fixes_to_5_3_1_General_functional_requirements - ZSM(19)000392r5_ZSM002_Clause_6_4_1_change_suggestions - ZSM(19)000405_ZSM002_AI_model_performance_evaluation_service_consistency - ZSM(19)000406r2_ZSM002_conflict_resolution_336r2_and_387r2 - ZSM(19)000407_ZSM002_IF_and_DS_services_re-structuring_as_follow-up_of_398 - ZSM(19)000411r1_ZSM002_Fixing_the_use_of_the_term__implementation - ZSM(19)000412r1_ZSM002_ENs_removal_for_final_draft - ZSM(19)000413_ZSM002_Resolving_ENs_in_management_communication_service Editorials (r0-rapp) - Typos and formatting - Renumbering - Implementation status of ZSM(18)000325r2 and ZSM(19)000103r1 corrected in history box

Date	Version	Information about changes
09 July 2019	0.14.0	Status: Final Draft Incorporated contributions: - ZSM(18)000384_ZSM002_5_4_3_Functional_requirements_for_Common_Data_Service - ZSM(19)000410_ZSM002_align_Annex_E_with_services_terminology - ZSM(19)000416r4_ZSM002_missing_definitions - ZSM(19)000424_ZSM002_data_services_fix - ZSM(19)000425r1_ZSM002_security_fixes - ZSM(19)000427r1_ZSM002_necessary_modifications_of_content_introduced_by_ZSM - ZSM(19)000435_ZSM002_Fallback_solution_for_service_invocation_routing_serv - ZSM(19)000439r1_ZSM002_apply_the_boilerplate_for_reference_to_ZSM007 - ZSM(19)000440r1_ZSM002_Editorial_changes_in_clauses_3_4__6_5_2_2_1__6_5_2_2 Editorials (r0-rapp)
15 Jul 2019	0.14.1	Status: Final Draft Incorporated contributions: - ZSM(19)000446_ZSM002_making_reference_to_ZSM001_informative Editorials (r0-rapp)

History

Document history		
V1.1.1	August 2019	Publication