ETSI GS ZSM 009-2 V1.1.1 (2022-06)

Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 2: Solutions for automation of E2E service and network management use cases

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-009-2_CLA_sol

Keywords
automation, network management, use case

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 of ETSI GS ZSM 009-1 [3].

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 presents solutions to scenarios related to closed loops using the ZSM specified service capabilities. New service capabilities are specified where the need arises based on the scenarios solution requirements.

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.

[1] ETSI GS ZSM 007 (V1.1.1): "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

[2] ETSI GS ZSM 002 (V1.1.1): "Zero-touch network and Service Management (ZSM); Reference Architecture".

[3] ETSI GS ZSM 009-1 (V1.1.1): "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers".

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 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 [1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ZSM 007 [1] apply.

3.4 Conventions

Clause 5 of the present document specifies expected solutions to typical automation scenarios using ZSM specified capabilities. For each step a corresponding capability is referenced from ETSI ISG ZSM specifications. The scenarios are briefly described in the description part of each clause. The solutions are provided in a table similar to table 3.4-1 that provides a pre-condition, a target, examples of expected steps for the solution and references to ZSM capabilities that may be used to achieve that step.

The table format with explanation of each of the parts is provided in table 3.4-1.

Table 3.4-1: Table used for solutions to scenarios

Precondition: The conditions/assumptions of the scenario **Target:** The target to be achieved by the solution of the scenario
Solution alternative
Step 1: Step 1 of the solution. For this the capability X specified in clause Y.x is used. Step 2: (Steps may refer to a picture).

4 Introduction

The present document specifies solutions to automation scenarios. The scenarios and corresponding solutions are presented together in clause 5. Scenarios are grouped in four categories, namely:

1) Generic management scenario solutions addressed in clause 5.1.

2) Scenario solutions relating to analytics in clause 5.2.

3) Scenario solutions relating to closed loops' coordination in clause 5.3.

4) Scenarios to solutions relating to closed loops' governance in clause 5.4.

Clause 6 specifies additional capabilities which extend existing ZSM services supporting the solutions.

5 Solutions supporting selected scenarios

5.1 Generic management using closed loops

5.1.1 Inclusion of a new physical resource into a management domain

5.1.1.1 Description

When a new physical resource is added to a management domain all other relevant authorized management domains should become aware of the management domain's ability to provide services based on the inclusion of the new resource. For example: when a new radio is added to the RAN domain of an operator the E2E management domain of the operator detects that it has the ability to provide services in an updated coverage area. This scenario is related to the scenario in clause 6.2.3.6 of ETSI GS ZSM 001 [i.1].

5.1.1.2 Proposed Solution

Table 5.1.1.2-1: Steps in solution

Pre-condition: The operator network exists and is operational, and a new physical resource is added into a management domain, say MD1. **Target:** To notify relevant management domains of the update in services based on the availability of the new resource in a management domain.	
Solution alternative	
Step 1:	MD1 updates its inventory and service capabilities based on the inclusion of a new resource. This is an internal capability of the management domain.
Step 2:	Other management domains authorized to view the changes in service/resource capabilities of MD1 can view these changes at their respective abstraction level. The solution to do this is specified in clause 5.1.4.
Step 3:	The management domains can use the updated capabilities of MD1.

5.1.2 Provisioning services in back up domains

5.1.2.1 Description

A new E2E Service may be provisioned in one or more management domain(s) as determined by the E2E management domain. However, if during the lifetime of the service one of the management domains, (say MD1) becomes unable to host its part of the E2E service (for example: MD1 encounters a failure) then the E2E service may need to provision an equivalent part of the E2E service that was hosted by MD1 to another management domain (say MD2) to ensure the continued operation of the E2E service. This solution is related to scenarios in clause 6.2.3 of ETSI GS ZSM 001 [i.1].

5.1.2.2 Proposed Solution

Table 5.1.2.2-1: Steps in solution

Precondition: The E2E management domain has deployed an E2E service across management domains MD1, MD2, MD3. The E2E management domain detects that MD1 is unable to support its part of the E2E service. **Target:** The E2E management domain can deploy the E2E Service in a new set of management domains, say, MD-A, MD-B, MD-C. NOTE 1: The relationship between MD-A-C , MD1-3 is intentionally not specified. That is to say that, for example MD-B could be identical to MD-2.	
Solution alternative:	
Step 1:	E2E management domain evaluates E2E service requirements and deploys the E2E service across multiple Management domains, say MD1, MD2, MD3. The manage service lifecycle capability as in clause 6.5.5.2.1 of ETSI GS ZSM 002 [2] is used for this purpose.
Step 2:	The E2E management domain detects that the domain MD1 is no longer able to support its part of the requested service and re-evaluates that the desirable new solution is MD-A, MD-B and MD-C. If the E2E MD is unable to find a new set of MDs to support the E2E Service, it issues an alarm to the ZSM consumer. See clause 5.1.5 on the solution for how this is done.
Step 3:	The E2E MD deactivates the request from MD2, MD3 and deploys it on MD-A, MD-B, MD-C. The manage service lifecycle capability as in clause 6.5.5.2.1 of ETSI GS ZSM 002 [2] is used for this purpose.
NOTE 2:	The use case focuses on deployment, other procedures required to support the deployment are not addressed.

5.1.3 Automated service healing capability

5.1.3.1 Description

An E2E service is deployed across a set of management domains. During the lifetime of the E2E service a failure occurs in one management domain which then intends to automatically heal the service without involving the other management domains of the E2E management domain. If self-healing is not possible in the management domain local scope, the management domain escalates the problem towards the E2E management domain, which then evaluates the problem, initiates service self-healing actions in the E2E scope, and drives the management domains to perform the required reconfigurations in the underlying management domains. The solution is related to clauses 6.2.3.3 and 6.5.3 of ETSI GS ZSM 001 [i.1].

5.1.3.2 Proposed Solution

Table 5.1.3.2-1: Steps in solution

Precondition: The E2E management domain has deployed an E2E service across a set of management domains, e.g. MD1, MD2, MD3. **Target:** The service is automatically self-healed by a management domain or by the E2E management domain when an infrastructure failure occurs in a management domain.	
Solution alternative:	
Step 1:	Domain analytics management functions subscribe to fault events service running at management domains to detect fault events regarding the deployed E2E service originating from the infrastructure resources of the respective management domain, e.g. MD1, MD2, MD3. For this the provide notification capability of the fault events service as specified in table 6.5.2.2.1-2 of ETSI GS ZSM 002 [2] is used.
Step 2:	The E2E domain analytics management functions subscribe to anomaly detection service running at management domains and/or E2E anomaly detection service. For this the provide analysis results capability of the anomaly detection service as specified in table 6.5.3.2.1-2 of ETSI GS ZSM 002 [2] is used.
Step 3:	When a failure occurs in a domain, the reactive incident analysis service of the corresponding management domain (e.g. MD1) tries to heal the impacted service locally. This capability is domain internal.
Step 4:	When the service healing is not possible in the management domain's local scope then the problem is escalated towards the E2E management domain using the health issue reporting service. For this the provide health issue notification of the health issue reporting service as specified in clause 6.5.4.2.5 of ETSI GS ZSM 002 [2] is used.
Step 5:	The E2E management domain evaluates the situation using the E2E anomaly detection service and the responsible E2E service closed loop determines the required management domain level reconfiguration actions, e.g. in MD1 and MD2. This capability is domain internal
Step 6:	The required actions are performed in the respective MDs using the manage resource configuration capability of the Resource configuration management service.

5.1.4 Capability change notification across management domains

5.1.4.1 Description

In this scenario a Management Domain (MD) A use capabilities provided by another management domain B. Over the course of time management domain B may improve or remove capabilities such as, for example: management domain B adds the capability to support new geographies, or technologies that support shorter delay in the network, no support for an older technology. In such cases MD A should automatically become aware of these changes.

5.1.4.2 Proposed Solution

Table 5.1.4.2-1: Steps in solution

Precondition: Management Domain A and B exist. **Target:** Management domain A is informed of any changes in Management Domain B's resources. NOTE: Either of the domains could be the E2E MD.	
Solution Alternative 1: Event driven.	
Step 1:	Management Domain A configures a condition using the condition detection service of Management Domain B, requiring to report any changes in inventory of management domain A (this is typically done via the integration fabric). For this the manage conditions detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) in an MD is used.
Step 2:	After a new resource appears in MD B, the condition management service publishes an event over the integration fabric notifying MD A that new capability is available in MD B. For this, the event publication capability Provide condition state change Notifications of condition detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) in an MD is used.
Solution Alternative 2: Using monitoring closed loop.	
Step 1:	MD A creates a periodic closed loop, with a configurable period, consisting only of the observe, decide, and act stages. For this the Request M2O CL capability as specified in clause 6 is used.
Step 2:	In the observe stage MD A gets updated with the set of resources from MD B, if any. For this the manage inventory capability of the domain inventory management service as specified in clause 6.5.5.2.6 of ETSI GS ZSM 002 [2] is used.
Step 3:	In the decide stage, MD A checks internally if there are changes in the set of resources of MD B as reported in Step 2. if yes, the act state is triggered. This is an internal capability.
Step 4:	In the act stage, MD A updates the related inventories. For this the manage inventory capability of the domain inventory management service as specified in clause 6.5.5.2.6 of ETSI GS ZSM 002 [2] is used.
Step 5:	MD A checks for updates again same as in step 2 after the period has passed.

5.1.5 Automated detection of a management domain's inability to support the assigned part of the E2E Service

5.1.5.1 Description

In this scenario a E2E Management Domain (MD) A use a service provided by another management domain B to support the E2E Service. Over the course of time management domain B may not be able to support its part of the E2E service such as, for example: due to removal of an older technology, failure in MD B network. In such cases MD A should automatically become aware of these changes.

5.1.5.2 Proposed Solution

Table 5.1.5.2-1: Steps in solution

Precondition: E2E MD A and MD B exist. MD B supports E2E A in at least one E2E service. **Target:** E2E MD A shall be notified if MD B is unable to support the part of at least one E2E service in MD B	
Solution Alternative 1: Event driven	
Step 1:	E2E MD A asks the inter-domain integration fabric to configure a condition relating to the SLA/SLS of the part of the E2E Service using the condition detection service in Management domain B. For this the post execution coordination service detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) in an MD is used.
Step 2:	The integration fabric uses the condition detection service instance in management domain B to evaluate if it is possible to set such a condition. If yes, the condition is set using the manage conditions detection service (as specified in clause 6.6.3.2.2 of ETSI GS ZSM 002 [2]).
Step 3:	When an SLA/SLS is violated in MD B, the MD B condition management service publishes an event over the integration fabric. MD A is notified of the failure since it has subscribed to such notifications. For this the event publication capability Provide condition state change Notifications of domain condition detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) is used.
Step 4:	The inter-domain integrations fabric informs E2E MD A about event.
Solution Alternative 2: Monitoring closed loop	
Step 1:	E2E MD A creates a periodic closed loop consisting of observe, decide, and act stages. For this the Request M2O CL capability as specified in clause 6 is used.
Step 2:	In the observe stage E2E MD A monitors the performance KPIs of the MD B part of the E2E Service. For this the get batch measurements capability of the performance measurements collection service as specified in clause 6.5.2.2.3 of ETSI GS ZSM 002 [2] is used.
Step 3:	In the decide stage, E2E MD A checks if the monitored KPIs meet the requirement of the respective E2E Service. If not, act state is triggered with the appropriate resolution. This is an internal capability.
Step 4:	In the act state the appropriate resolutions from the decision state are carried out. This uses the capabilities related to domain orchestration (clause 6.5.5) or domain control (clause 6.5.6) of ETSI GS ZSM 002 [2] as required.
Step 5:	After the period, MD A checks for performance updates again repeating step 2.

5.2 Analytics in closed loops

5.2.1 Dynamic configurability of E2E service monitoring

5.2.1.1 Description

Every time a new E2E Service is deployed, various aspects of the E2E Service need to be monitored to ensure that the overall service KPIs (with regards to maintaining the SLA/SLS of the service) are being met. In addition to basic monitoring for adherence to SLA/SLS, the E2E service may, for example, also be monitored to draw inference about the expected performance of the E2E service by the respective analytics service. In this scenario the analytics service may require different information at different levels of detail (for example periodicity) at different times. Hence there may be a need for the E2E management domain to dynamically change the requested monitoring details from the respective management domains where the E2E service is deployed. This solution is related to clauses 6.4.1 and 6.4.4 of ETSI GS ZSM 001 [i.1].