

authorization-control-inter

Service Description

Abstract

This document provides service description for the **authorization-control-inter** service.

Contents

1 Overview	3
1.1 How This Service Is Meant to Be Used	3
1.2 Important Delimitations	3
1.3 Access policy	3
2 Service Interface	4
2.1 interface HTTP/TLS/JSON	4
3 Information Model	5
3.1 struct CheckAuthRuleRequest	5
3.2 struct CloudDescriptor	5
3.3 struct ProviderInterfaceIds	5
3.4 struct CheckAuthRuleResponse	5
3.5 Primitives	6
4 References	7
5 Revision History	8
5.1 Amendments	8
5.2 Quality Assurance	8

1 Overview

This document describes the **authorization-control-inter** service, which enables authorization control between local clouds. The purpose of this service is to grant access right for a consumer cloud to a provider-service-interface triplet.

The rest of this document is organized as follows. In Section 2, we describe the abstract message functions provided by the service. In Section 3, we end the document by presenting the data types used by the mentioned functions.

1.1 How This Service Is Meant to Be Used

Primarily the Gatekeeper Core System should consume this service during the global service discovery process to check whether the specified consumer cloud has right to consume the actually matching provider-service-interface triplet.

1.2 Important Delimitations

The inter-cloud authorization rules are possible to define by database record ids, so when a cloud or service definition or interface name has been unregistered or removed, then the authorization rule is going to be removed as well.

1.3 Access policy

This service is available only for the Orchestrator and the Gatekeeper Core Systems.

2 Service Interface

This section describes the interfaces to the service. The **authorization-control-inter** service is used to verify authorization rules. The various parameters are representing the necessary cloud, system and service input information. In particular, each subsection names an interface, an input type and an output type, in that order. The input type is named inside parentheses, while the output type is preceded by a colon. Input and output types are only denoted when accepted or returned, respectively, by the interface in question. All abstract data types named in this section are defined in Section 3.

The following interfaces are available.

2.1 interface **HTTP/TLS/JSON** (**CheckAuthRuleRequest**) : **CheckAuthRuleResponse**

Profile ype	Type	Version
Transfer protocol	HTTP	1.1
Data encryption	TLS	1.3
Encoding	JSON	RFC 8259 [1]
Compression	N/A	-

Table 1: HTTP/TLS/JSON communication details.

3 Information Model

Here, all data objects that can be part of the **authorization-control-inter** service provides to the hosting System are listed in alphabetic order. Note that each subsection, which describes one type of object, begins with the *struct* keyword, which is used to denote a collection of named fields, each with its own data type. As a complement to the explicitly defined types in this section, there is also a list of implicit primitive types in Section 3.5, which are used to represent things like hashes and identifiers.

3.1 struct CheckAuthRuleRequest

Field	Type	Mandatory	Description
cloud	CloudDescriptor	yes	Descriptor of the consumer cloud.
providerInterfacelds	List<ProviderInterfacelds>	yes	Array of provider and interface reference objects.
serviceDefinition	Name	yes	Service definition name.

3.2 struct CloudDescriptor

Field	Type	Mandatory	Description
name	Name	yes	Name of the cloud.
operator	Name	yes	Name of the cloud operator.

3.3 struct ProviderInterfacelds

Field	Type	Mandatory	Description
id	Number	yes	Database record identifier of the provider system.
idList	List<Number>	yes	List of interface database record identifiers.

3.4 struct CheckAuthRuleResponse

Field	Type	Description
authorizedProviderInterfacelds	List<ProviderInterfacelds>	Array of the authorized provider and interface reference objects.
cloud	CloudDescriptor	Descriptor of the consumer cloud.
serviceDefinition	Name	Service definition name.

3.5 Primitives

Types and structures mentioned throughout this document that are assumed to be available to implementations of this service. The concrete interpretations of each of these types and structures must be provided by any IDD document claiming to implement this service.

Type	Description
List<A>	An <i>array</i> of a known number of items, each having type A.
Name	A string identifier that is intended to be both human and machine-readable.
Number	Decimal number



ARROWHEAD

Document title
authorization-control-inter
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
7 (8)

4 References

- [1] T. Bray, "The JavaScript Object Notation (JSON) Data Interchange Format," RFC 8259, Dec. 2017. [Online]. Available: <https://rfc-editor.org/rfc/rfc8259.txt>

5 Revision History

5.1 Amendments

No.	Date	Version	Subject of Amendments	Author
1	YYYY-MM-DD	4.6.0		Xxx Yyy

5.2 Quality Assurance

No.	Date	Version	Approved by
1	YYYY-MM-DD	4.6.0	