Schema

title:	OpenC2 Language Objects
module:	oasis-open.org/openc2/oc2ls/v1.0/oc2ls-v1.0
patch:	0
description:	Datatypes that define the content of OpenC2 commands and responses.
exports:	OpenC2-Command, OpenC2-Response, Message-Type, Status-Code, Request-Id, Date-Time
imports:	jadn: oasis-open.org/openc2/oc2ls/v1.0/jadn-v1.0

Message (Array)

ID	Type	#	Description
1	Message-Type	1	msg_type -- message element
2	String	1	content_type -- message element
3	Null	1	content -- message element
4	Status-Code	0..1	status -- message element
5	Request-Id	0..1	request_id -- message element
6	String	0..n	to -- message element
7	String	0..1	from -- message element
8	Date-Time	0..1	created -- message element

OpenC2-Command (Record)

ID	Name	Type	#	Description
1	**action**	Action	1	The task or activity to be performed (i.e., the 'verb').
2	**target**	Target	1	The object of the action. The action is performed on the target.
3	**args**	Args	0..1	Additional information that applies to the command.
4	**actuator**	Actuator	0..1	The subject of the action. The actuator executes the action on the target.

Action (Enumerated)

ID	Name	Description
1	**scan**	Systematic examination of some aspect of the entity or its environment in order to obtain information.
2	**locate**	Find an object physically, logically, functionally, or by organization.
3	**query**	Initiate a request for information.
6	**deny**	Prevent a certain event or action from completion, such as preventing a flow from reaching a destination or preventing access.
7	**contain**	Isolate a file, process, or entity so that it cannot modify or access assets or processes.
8	**allow**	Permit access to or execution of a target.
9	**start**	Initiate a process, application, system, or activity.
10	**stop**	Halt a system or end an activity.
11	**restart**	Stop then start a system or activity.
14	**cancel**	Invalidate a previously issued action.
15	**set**	Change a value, configuration, or state of a managed entity.
16	**update**	Instruct a component to retrieve, install, process, and operate in accordance with a software update, reconfiguration, or other update.
18	**redirect**	Change the flow of traffic to a destination other than its original destination.
19	**create**	Add a new entity of a known type (e.g., data, files, directories).
20	**delete**	Remove an entity (e.g., data, files, flows.
22	**detonate**	Execute and observe the behavior of a target (e.g., file, hyperlink) in an isolated environment.
23	**restore**	Return a system to a previously known state.
28	**copy**	Duplicate a file or data flow.
30	**investigate**	Task the recipient to aggregate and report information as it pertains to a security event or incident.
32	**remediate**	Task the recipient to eliminate a vulnerability or attack point.

Target (Choice)

ID	Name	Type	#	Description
1	**artifact**	Artifact	1	An array of bytes representing a file-like object or a link to that object.
2	**command**	Request-Id	1	A reference to a previously issued OpenC2 command.
3	**device**	Device	1	The properties of a hardware device.
7	**domain_name**	Domain-Name	1	A network domain name.
8	**email_addr**	Email-Addr	1	A single email address.

16	**features**	Features	1	A set of items used with the query action to determine an actuator's capabilities
10	**file**	File	1	Properties of a file.
11	**ip_addr**	IP-Addr	1	The representation of one or more IP addresses (either version 4 or version 6).
15	**ip_connection**	IP-Connection	1	A network connection that originates from a source and is addressed to a destination.
13	**mac_addr**	MAC-Addr	1	A single Media Access Control (MAC) address.
17	**process**	Process	1	Common properties of an instance of a computer program as executed on an operating system.
25	**properties**	Properties	1	Data attribute associated with an actuator
19	**uri**	URI	1	A uniform resource identifier (URI).
1000	**extension**	PE-Target	1	Targets defined in a Private Enterprise extension profile
1001	**extension_unr**	Unr-Target	1	Targets defined in an unregistered extension profile
1024	**slpf**	slpf:Target	1	Targets defined in the Stateless Packet Filter Profile

Actuator (Choice)

ID	Name	Type	#	Description
1000	**extension**	PE-Specifiers	1	Specifiers defined in a Private Enterprise extension profile.
1001	**extension_unr**	Unr-Specifiers	1	Specifiers defined in an unregistered extension profile.

Args (Map)

ID	Name	Type	#	Description
1	**start_time**	Date-Time	0..1	The specific date/time to initiate the action
2	**stop_time**	Date-Time	0..1	The specific date/time to terminate the action
3	**duration**	Duration	0..1	The length of time for an action to be in effect
4	**response_requested**	Response-Type	0..1	The type of response required for the action
1000	**extension**	PE-Args	0..1	Command arguments defined in a Private Enterprise extension profile
1001	**extension_unr**	Unr-Args	0..1	Command arguments defined in an unregistered extension profile

OpenC2-Response (Map)

ID	Name	Type	#	Description
1	**status**	Status-Code	0..1	An integer status code (Duplicates message status code)
2	**status_text**	String	0..1	A free-form human-readable description of the response status
3	**strings**	String	0..n	Generic set of string values
4	**ints**	Integer	0..n	Generic set of integer values
5	**kvps**	KVP	0..n	Generic set of key:value pairs
6	**versions**	Version	0..n	Supported OpenC2 Language versions
7	**profiles**	jadn:Uname	0..n	List of profiles supported by this actuator
8	**schema**	jadn:Schema	0..1	Syntax of the OpenC2 language elements supported by this actuator
9	**pairs**	Action-Targets	0..n	List of targets applicable to each supported action
10	**rate_limit**	Number	0..1	Maximum number of requests per minute supported by design or policy
1000	**extension**	PE-Results	0..1	Response data defined in a Private Enterprise extension profile
1001	**extension_unr**	Unr-Results	0..1	Response data defined in an unregistered extension profile

Status-Code (Enumerated.ID)

ID	Description
102	Processing -- an interim response used to inform the client that the server has accepted the request but not yet completed it.
200	OK -- the request has succeeded.
301	Moved Permanently -- The target resource has been assigned a new permanent URI
400	Bad Request -- the consumer cannot process the request due to something that is perceived to be a client error (e.g., malformed request syntax.)
401	Unauthorized -- the request lacks valid authentication credentials for the target resources or authorization has been refused for the submitted credentials.
403	Forbidden -- the consumer understood the request but refuses to authorize it.
404	Not Found -- the consumer has not found anything matching the request.
500	Internal Error -- the consumer encountered an unexpected condition that prevented it from fulfilling the request.
501	Not Implemented -- the consumer does not support the functionality required to fulfill the request.
503	Service Unavailable -- the consumer is currently unable to handle the request due to a temporary overloading or maintenance.

PE-Target (Choice.ID)

ID	Type	#	Description
32473	32473:Target	1	Example -- Targets defined in the Example Inc. extension profile

PE-Specifiers (Choice.ID)

ID	Type	#	Description
32473	32473:Specifiers	1	Example -- Actuator Specifiers defined in the Example Inc. extension profile

PE-Args (Map.ID)

ID	Type	#	Description
32473	32473:Args	1	Example -- Command Arguments defined in the Example Inc. extension profile

PE-Results (Map.ID)

ID	Type	#	Description
32473	32473:Results	1	Example -- Results defined in the Example Inc. extension profile

Artifact (Record)

ID	Name	Type	#	Description
1	**mime_type**	String	0..1	Permitted values specified in the IANA Media Types registry
2	**payload**	Payload	0..1	choice of literal content or URL to obtain content
3	**hashes**	Hashes	0..1	Specifies a dictionary of hashes for the contents of the payload

Device (Map)

ID	Name	Type	#	Description
1	**hostname**	Hostname	1	A hostname that can be used to connect to this device over a network
2	**description**	String	0..1	A human-readable description of the purpose, relevance, and/or properties of the device
3	**device_id**	String	0..1	An identifier that refers to this device within an inventory or management system

Domain-Name

Type Name	Base Type	Description
Domain-Name	String (hostname)	RFC 1034, section 3.5

Email-Addr

Type Name	Base Type	Description
Email-Addr	String (email)	Email address, RFC 5322, section 3.4.1

Features

Type Name	Base Type	Description
Features	ArrayOf(Feature) ['min']	A target used to query Actuator for its supported capabilities

File (Map)

ID	Name	Type	#	Description
1	**name**	String	0..1	The name of the file as defined in the file system
2	**path**	String	0..1	The absolute path to the location of the file in the file system
3	**hashes**	Hashes	0..1	One or more cryptographic hash codes of the file contents

IP-Addr

Type Name	Base Type	Description
IP-Addr	Binary (ip-addr)	32 bit IPv4 address or 128 bit IPv6 address

IP-Connection (Record)

ID	Name	Type	#	Description
1	**src_addr**	IP-Addr	0..1	source address
2	**src_port**	Port	0..1	source TCP/UDP port number
3	**dst_addr**	IP-Addr	0..1	destination address

4	**dst_port**	Port	0..1	destination TCP/UDP port number
5	**protocol**	L4-Protocol	0..1	Protocol (IPv4) / Next Header (IPv6)

MAC-Addr

Type Name	Base Type	Description
MAC-Addr	Binary	Media Access Code / Extended Unique Identifier - 48 or 64 bit address

Process (Map)

ID	Name	Type	#	Description
1	**pid**	Integer	0..1	Process ID of the process
2	**name**	String	0..1	Name of the process
3	**cwd**	String	0..1	Current working directory of the process
4	**executable**	File	0..1	Executable that was executed to start the process
5	**parent**	Process	0..1	Process that spawned this one
6	**command_line**	String	0..1	The full command line invocation used to start this process, including all arguments

Properties

Type Name	Base Type	Description
Properties	ArrayOf(String)	A list of names that uniquely identify properties of an actuator

URI

Type Name	Base Type	Description
URI	String (uri)	Uniform Resource Identifier

Message-Type (Enumerated)

ID	Name	Description
0	**notification**	A message that does not solicit a response
1	**request**	A message for which a response is requested
2	**response**	A message containing a response to a request

Request-Id

Type Name	Base Type	Description
Request-Id	Binary	A value of up to 128 bits that uniquely identifies a particular command

Date-Time

Type Name	Base Type	Description
Date-Time	Integer	Milliseconds since 00:00:00 UTC, 1 January 1970.

Duration

Type Name	Base Type	Description
Duration	Integer	Milliseconds

Hashes (Map)

ID	Name	Type	#	Description
1	**md5**	Binary	0..1	MD5 hash as defined in RFC3121
4	**sha1**	Binary	0..1	SHA1 hash as defined in RFC3174
6	**sha256**	Binary	0..1	SHA256 as defined in RFC6234

Hostname

Type Name	Base Type	Description
Hostname	String	A legal Internet host name as specified in RFC 1123

L4-Protocol (Enumerated)

ID	Name	Description
1	**icmp**	Internet Control Message Protocol - RFC 792
6	**tcp**	Transmission Control Protocol - RFC 793-
17	**udp**	User Datagram Protocol - RFC 768
132	**sctp**	Stream Control Transmission Protocol - RFC 4960

Payload (Choice)

ID	Name	Type	#	Description
1	**bin**	Binary	1	Specifies the data contained in the artifact.
2	**url**	URI	1	MUST be a valid URL that resolves to the un-encoded content

Port

Type Name	Base Type	Description
Port	Integer	Transport Protocol Port Number, RFC 6335

Feature (Enumerated)

ID	Name	Description
1	**versions**	List of OpenC2 language versions supported by this actuator
2	**profiles**	List of profiles supported by this actuator
3	**schema**	Definition of the command syntax supported by this actuator
4	**pairs**	List of supported actions and applicable targets
5	**rate_limit**	Maximum number of supported requests per minute

Response-Type (Enumerated)

ID	Name	Description
0	**none**	No response
1	**ack**	Respond when command received
2	**status**	Respond with progress toward command completion
3	**complete**	Respond when all aspects of command completed

Version

Type Name	Base Type	Description
Version	String	Major.Minor version number

KVP (Array)

ID	Type	#	Description
1	String	1	key -- name of this item
2	String	1	value -- string value of this item

Action-Targets (Array)

ID	Type	#	Description
1	Action	1	action -- An action supported by this actuator
2	Target.*	1..n	targets -- List of targets applicable to this action