Schema

title:	OpenC2 Language Objects
module:	oasis-open.org/openc2/v1.0/openc2-lang
patch:	wd08-slpf
description:	OpenC2 Language content used by Stateless Packet Filters.
exports:	OpenC2-Command, OpenC2-Response
imports:	**slpf**: /oasis-open.org/openc2/v1.0/ap-slpf **jadn**: /oasis-open.org/openc2/v1.0/jadn

Structure Types

OpenC2-Command

The OpenC2 Command describes an action performed on a target. It can be directive or descriptive depending on the context.

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	actuator	Actuator	0..1	The subject of the action. The actuator executes the action on the target
4	args	Args	0..1	Additional information that applies to the command
5	id	Command-ID	0..1	Identifier used to link responses to a command

Action

Action (Enumerated)

ID	Name	Description
3	query	Initiate a request for information. Used to communicate supported options and determine state or settings.
6	deny	Prevent traffic or access.
8	allow	Permit traffic or access.
16	update	Instruct the actuator to update its configuration by retrieving and processing a configuration file and update.
20	delete	Remove a rule.

Target

OpenC2 Target datatypes

Target (Choice)

ID	Name	Type	Description
10	file	File	Properties of a file
11	ip_addr	IP-Addr	The representation of one or more IP addresses (either version 4 or version 6) expressed using CIDER notation
15	ip_connection	IP-Connection	A network connection that originates from a source and is addressed to a destination
16	openc2	OpenC2	A set of items used with the query action to determine an actuator's capabilities
1024	slpf	slpf:Target	Targets defined in the Stateless Packet Filter profile

Actuator

Actuator (Choice)

ID	Name	Type	Description
1024	slpf	slpf:Specifiers	Specifiers as defined in the Stateless Packet Filter profile, oasis-open.org/openc2/oc2ap-slpf/v1.0/csd01

Specifiers

Specifiers (Map)

ID	Name	Type	#	Description
2	asset_id	String	0..1	Hardware identifier of a physical actuator device, such as a serial number or inventory barcode

Args

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
1024	slpf	slpf:Args	0..1	Command arguments defined in the Stateless Packet Filter profile

OpenC2-Response

OpenC2-Response (Record)

ID	Name	Type	#	Description
1	id	Command-ID	1	Id of the ommand that induced this response
2	status	Status-Code	1	An integer status code
3	status_text	String	0..1	A free-form human-readable description of the response status
4	*	Results	1	Data or extended status information that was requested from an OpenC2 command

Status-Code

Status-Code (Enumerated.Tag)

Value	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 server 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 server understood the request but refuses to authorize it.
500	Server Error -- The server encountered an unexpected condition that prevented it from fulfilling the request.
501	Not Implemented -- The server does not support the functionality required to fulfill the request.

Results

Results (Map)

ID	Name	Type	#	Description
4	versions	Version	0..n	Supported OpenC2 Language versions
5	profiles	jadn:Uname	0..n	Supported actuator profiles
6	schema	jadn:Schema	0..n	Schema supported by this actuator
7	pairs	ActionTargets	0..n	List of targets applicable to each supported action
1024	slpf	slpf:Results	0..n	Results from Stateless Packet Filter profile

ActionTargets

ActionTargets (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

OpenC2

A target used to query Actuator for its supported capabilities

OpenC2 (ArrayOf.Query–Item ['max', 'min'])

Query-Item

Results to be included in response to query openc2 command

Query–Item (Enumerated)

ID	Name	Description
1	versions	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

IP-Connection

5-tuple that specifies a tcp/ip connection

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	layer4–protocol	L4–Protocol	0..1	Protocol (IPv4) / Next Header (IPv6)

L4-Protocol

protocol (IPv4) or next header (IPv6) field - any IANA value, RFC 5237

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

File

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

Response-Type

Response–Type (Enumerated)

ID	Name	Description
0	none	No response
1	ack	Respond when command received
2	complete	Respond when all aspects of command completed

Hashes

Cryptographic Hash values

Hashes (Map)

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

Primitive Types

Name	Type	Description
Command-ID	String	Uniquely identifies a particular command - TBD syntax
Date-Time	String (date-time)	RFC 3339 date-time
Duration	String (duration)	RFC 3339 / ISO 8601 duration
IP-Addr	String (ip)	IPv4 or IPv6 address per RFC 2673 section 3.2, and RFC 4291 section 2.2
Port	String (port)	Service Name or Transport Protocol Port Number, RFC 6335
Version	String	Version string - TBD syntax