Schema

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

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 (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 (Choice)

ID	Name	Type	#	Description
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) expressed using CIDER notation
15	ip_connection	IP-Connection	1	A network connection that originates from a source and is addressed to a destination
16	openc2	OpenC2	1	A set of items used with the query action to determine an actuator's capabilities
1024	slpf	slpf:Target	1	Targets defined in the Stateless Packet Filter profile

Actuator (Choice)

ID	Name	Type	#	Description
1024	slpf	slpf:Specifiers	1	Specifiers as defined in the Stateless Packet Filter profile, oasis-open.org/openc2/oc2ap-slpf/v1.0/csd01

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 (Record)

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

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 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.

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

Name	Type	Description
IP-Addr	String (ip)	IPv4 or IPv6 address per RFC 2673 section 3.2, and RFC 4291 section 2.2

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)

OpenC2

Name	Type	Description
OpenC2	ArrayOf(Query-Item) ['max', 'min']	A target used to query Actuator for its supported capabilities

Command-ID

Name	Type	Description
Command-ID	String	Uniquely identifies a particular command

Date-Time

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

Duration

Name	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

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

Port

Name	Type	Description
Port	Integer (port)	Transport Protocol Port Number, RFC 6335

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
4	pairs	List of supported actions and applicable targets

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

Name	Type	Description
Version	String	TBSL

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..1	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 (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

slpf:Target (Choice)

ID	Name	Type	#	Description
1	rule_number	slpf:Rule-ID	1	Uniquely identifies a rule associated with a previously-issued deny or allow.

slpf:Args (Map)

ID	Name	Type	#	Description
1	drop_process	slpf:Drop-Process	0..1	Specifies how to handle denied packets
2	running	Boolean	0..1	Normal operation assumes updates are persistent. If TRUE, updates are not persistent in the event of a reboot or restart. Default=FALSE.
3	direction	slpf:Direction	0..1	Specifies whether to apply rules to incoming or outgoing traffic. If omitted, rules are applied to both.
4	insert_rule	slpf:Rule-ID	0..1	Specifies the identifier of the rule within a list, typically used in a top-down rule list.

slpf:Drop-Process (Enumerated)

ID	Name	Description
1	none	Drop the packet and do not send a notification to the source of the packet.
2	reject	Drop the packet and send an ICMP host unreachable (or equivalent) to the source of the packet.
3	false_ack	Drop the traffic and send a false acknowledgement that the data was received by the destination.

slpf:Direction (Enumerated)

ID	Name	Description
1	ingress	Apply rules to incoming traffic only
2	egress	Apply rule to outbound traffic only

slpf:Rule-ID

Name	Type	Description
slpf:Rule-ID	Integer	Immutable identifier assigned when an access rule is created.

slpf:Specifiers (Map)

ID	Name	Type	#	Description
1	hostname	String	0..1	RFC 1123 hostname (can be a domain name or IP address) for a particular device with SLPF functionality
2	named_group	String	0..1	User-defined collection of devices with SLPF functionality
3	asset_id	String	0..1	Unique identifier for a particular SLPF
4	asset_tuple	String	0..10	Unique tuple identifier for a particular SLPF consisting of a list of up to 10 strings

slpf:Results (Map)

ID	Name	Type	#	Description
1	rule_number	slpf:Rule-ID	0..1	Rule identifier returned from allow or deny command.

jadn:Schema (Record)

ID	Name	Type	#	Description
1	meta	jadn:Meta	1	Information about this schema module
2	types	jadn:Type	1..n	Types defined in this schema module

jadn:Meta (Map)

ID	Name	Type	#	Description
1	module	jadn:Uname	1	Schema unique name/version
2	patch	String	0..1	Patch version
3	title	String	0..1	Title
4	description	String	0..1	Description
5	imports	jadn:Import	0..n	Imported schema modules
6	exports	jadn:Identifier	0..n	Data types exported by this module
7	bounds	jadn:Bounds	0..1	Schema-wide upper bounds

jadn:Import (Array)

ID	Type	#	Description
1	jadn:Nsid	1	nsid -- A short local identifier (namespace id) used within this module to refer to the imported module
2	jadn:Uname	1	uname -- Unique name of imported module

jadn:Bounds (Array)

ID	Type	#	Description
1	Integer	1	max_msg -- Maximum serialized message size in octets or characters
2	Integer	1	max_str -- Maximum string length in characters
3	Integer	1	max_bin -- Maximum binary length in octets
4	Integer	1	max_fields -- Maximum number of elements in ArrayOf

jadn:Type (Array)

ID	Type	#	Description
1	jadn:Identifier	1	tname -- Name of this datatype
2	jadn:JADN-Type.*	1	btype -- Base type. Enumerated value derived from list of JADN data types
3	jadn:Option	1..n	opts -- Type options
4	String	1	desc -- Description of this data type
5	jadn:JADN-Type	1..n	fields -- List of fields for compound types. Not present for primitive types

jadn:JADN-Type (Choice)

ID	Name	Type	#	Description
1	Binary	Null	1	Octet (binary) string
2	Boolean	Null	1	True or False
3	Integer	Null	1	Whole number
4	Number	Null	1	Real number
5	Null	Null	1	Nothing
6	String	Null	1	Character (text) string
7	Array	jadn:FullField	1..n	Ordered list of unnamed fields
8	ArrayOf	Null	1	Ordered list of fields of a specified type
9	Choice	jadn:FullField	1..n	One of a set of named fields
10	Enumerated	jadn:EnumField	1..n	One of a set of id:name pairs
11	Map	jadn:FullField	1..n	Unordered set of named fields
12	Record	jadn:FullField	1..n	Ordered list of named fields

jadn:EnumField (Array)

ID	Type	#	Description
1	Integer	1	Item ID
2	String	1	Item name
3	String	1	Item description

jadn:FullField (Array)

ID	Type	#	Description
1	Integer	1	Field ID or ordinal position
2	jadn:Identifier	1	Field name
3	jadn:Identifier	1	Field type
4	jadn:Options	1	Field options
5	String	1	Field description

jadn:Identifier

Name	Type	Description
jadn:Identifier	String	A string starting with an alpha char followed by zero or more alphanumeric / underscore / dash chars

jadn:Nsid

Name	Type	Description
jadn:Nsid	String	Namespace ID – a short identifier

jadn:Uname

Name	Type	Description
jadn:Uname	String	Unique name (e.g., of a schema) – typically a set of Identifiers separated by forward slashes

jadn:Options

Name	Type	Description
jadn:Options	ArrayOf(jadn:Option) ['max', 'min']	Options list may be empty but may not be omitted

jadn:Option

Name	Type	Description
jadn:Option	String	Option string: 1st char = option id