FIREMON

ZONE APIs

Lumeta API Documentation

TYPE	URL	REQUIRES
GET	/api/rest/zone	no filters
This API will return all zone names and their ids.		

TYPE	URL	REQUIRES
GET	api/rest/zone?filter.zone.name={*zoneName*}&detail.Organization&detail.Collectors	zoneName
This API will return zone information for the zone specified by zone name		

TYPE	URL	REQUIRES
GET	/api/rest/zone/{zoneId}/cidr/{cidrtype}	zoneId cidrtype: Known=0 Eligible=1 Internal=2
This API will return the zone CIDRs		

TYPE	URL	REQUIRES
POST	/api/rest/zone/{zoneId}/cidr/{cidrtype}?append=true	Payload ➔ Content-type: application/xml <ZoneManagement_setZoneCidrs_request> <addresses> <address>10.8.0.0/24</address> . . </addresses> </ZoneManagement_setZoneCidrs_request>
This API will append CIDRs to zone CIDR list (zone CIDR list can be known, eligible or internal based on cidrtype. here, cidrtype is set to 0 for known, 1 for eligible and 2 for internal)		

TYPE	URL	REQUIRES
POST	/api/rest/zone/{zoneId}/cidr/{cidrtype}	Payload ➔ Content-type: application/xml <ZoneManagement_setZoneCidrs_request> <addresses> <address>10.8.0.0/24</address> . . </addresses> </ZoneManagement_setZoneCidrs_request>
This API will replace a zone CIDR list with the ones given in payload (zone CIDR list can be known, eligible or internal based on cidrtype. here, cidrtype is set to 0 for known, 1 for eligible and 2 for internal)		

TYPE	URL	REQUIRES
DELETE	/api/rest/zone/{zoneId}/cidr/{cidrtype}	Payload ➔ Content-type: application/xml <ZoneManagement_setZoneCidrs_request> <addresses> <address>10.8.0.0/24</address> </addresses> </ZoneManagement_setZoneCidrs_request>
This API will delete a CIDR from a zone CIDR list (zone CIDR list can be known, eligible or internal based on cidrtype. here, cidrtype is set to 0 for known, 1 for eligible and 2 for internal)		

TYPE	URL	REQUIRES
POST	/api/rest/zone/	Payload ➔ Content-type: application/xml <updateZone_request> <zone> <name>*zone_name*</name> <description>*description*</description> <organization> <name>*organization_name*</name> </organization> </zone> </updateZone_request>
This API will add a zone. Please fill in the zone_name, description and organization_name (in payload). Must give a unique zone_name and existing organization_name		

TYPE	URL	REQUIRES
POST	/api/rest/zone/{zoneId}/organizations	zoneId Payload ➔ Content-type: application/xml <updateZone_request> <com.lumeta.api.core.model.Organization> <name>organizationName</name> </com.lumeta.api.core.model.Organization> </updateZone_request>
This API will update the organization for a zone. Please fill in the zoneId (in URL), and organizationName (in payload). Must provide an existing organization name		

FIREMON ORGANIZATION APIs

TYPE	URL	REQUIRES
POST	/api/rest/management/role	Payload ➔ Content-type: application/xml <updateRole_request> <role> <name>Manager</name> <users> <user> <name>*user_name*</name> </user> </users> <organization> <name>Organization1</name> </organization> </role> </updateRole_request>
This API will update the Manager Role in an organization with the users in the users list. Please add the role and user_name in the payload. You can use the same API to add users to role Viewer and SysAdmin.		

COLLECTOR APIs

TYPE	URL	REQUIRES
GET	api/rest/zone/collector?filter.collector.name={*collectorName*}&detail.Interface&detail.Config	collectorName
This API will return collector configuration for the collector specified by collectorName		

TYPE	URL	REQUIRES
POST	/api/rest/zone/collector	Payload ➔ Content-type: application/xml <updateCollector_request> <collector> <zone> <name>*zone_name*</name> </zone> <name>*collector_name*</name> <rescanInterval>*rescan_interval*</rescanInterval> <discoveryInterface> <name>*interface_name*</name> </discoveryInterface> </collector> </updateCollector_request>
This API will add a collector. Please fill in: zone_name, collector_name, rescan_interval and interface_name in payload		

TYPE	URL	REQUIRES
POST	/api/rest/zone/collector	Please fill in the following values. Anything with * is mandatory for collector update: *collector_id* *collector_name** *interface_name** *zone_id* *zone_name** *rescan_interval_time** **OSFP:** *ospf_area* *auth_value* *router_id* **LEAK:** *leak_interface_scout_id* *leak_interface* **SNMP:** *alias* *user_name* *context* *community_name* **DNS:** *server_name* **BGP:** *bgp_password* *bgp_ip* *bgp_AS_number* **SEVERAL CONFIGURATIONS:** *port_number*

Payload ➔
Content-type: application/xml

```
<updateCollector_request>
<collector>
        <id>collector_id</id>
        <name>collector_name</name>
        <discoveryInterface>
                <name>interface_name</name>
                <active>true|false</active>
                <ospf>
                        <enabled>true|false</enabled>
                        <area>ospf_area</area>
                        <authType>SIMPLE|CRYPTOGRAPHIC|NONE</authType>
                        <auth>auth_value</auth>
                        <routerId>router_id</routerId>
                </ospf>
```

```
</discoverInterface>
<leakInterface>
        <id>leak_interface_scout_id</id>
        <name>leak_interface</name>
</leakInterface>
<zone>
        <id>zone_id</id>
        <name>zone_name</name>
</zone>
<enabled>true|false</enabled>
<rescanInterval>rescan_interval_time</rescanInterval>
<ospfDiscovery>true|false</ospfDiscovery>
<broadcastDiscovery>
        <enabled>true|false</enabled>
        <arp>true|false</arp>
        <icmpV6>true|false</icmpV6>
        <dhcp>true|false</dhcp>
</broadcastDiscovery>
<pathDiscovery>
        <enabled>true|false</enabled>
        <icmp>true|false</icmp>
        <dns>true|false</dns>
        <snmp>true|false</snmp>
        <udp>true|false</udp>
        <tcpPorts>
                <port><port_number></port>
                .
                .
        </tcpPorts>
        <expandV4Cidrs>
                <range0__7>0</range0__7>
                <range8__15>20</range8__15>
                <range16__23>24</range16__23>
                <range24__32>0</range24__32>
        </expandV4Cidrs>
        <maxStealths>int</maxStealths>
        <maxUnknownHops>int</maxUnknownHops>
        <traceToHosts>true|false</traceToHosts>
        <traceDiscoveredRoutes>true|false</traceDiscoveredRoutes>
</pathDiscovery>
<hostDiscovery>
        <enabled>true|false</enabled>
        <targetDiscoveredRoutes>true|false</targetDiscoveredRoutes>
        <icmp>true|false</icmp>
        <dns>true|false</dns>
        <snmp>true|false</snmp>
        <udp>true|false</udp>
        <tcpPorts>
                <port>port_number</port>
                .
                .
        </tcpPorts>
</hostDiscovery>
```

```
<snmpDiscovery>
        <enabled>true|false</enabled>
        <collectInterfaces>true|false</collectInterfaces>
        <collectLayer2Data>true|false</collectLayer2Data>
        <collectRoutes>true|false</collectRoutes>
        <skipBgpRoutes>true|false</skipBgpRoutes>
        <maxRouteTableSize>int</maxRouteTableSize>
        <credentials>
                <credential>
                        <alias>alias</alias>
                        <privacyProtocol>NONE|SHA|MD5</privacyProtocol>
                        <privacyPassphrase></privacyPassphrase>
                        <authProtocol>NONE|AES|DES</authProtocol>
                        <authPassphrase></authPassphrase>
                        <userName>user_name</userName>
                        <context>context</context>
                </credential>
                .
                .
                <credential>
                        <alias>alias</alias>
                        <community>community_name</community>
                </credential>
                .
                .
        </credentials>
</snmpDiscovery>
<portDiscovery>
        <enabled>true|false</enabled>
        <useVulnerablePorts>true|false</useVulnerablePorts>
        <useInfectionPorts>true|false</useInfectionPorts>
        <tcpPorts>
                <port>port_number</port>
                .
                .
        </tcpPorts>
        <extraPorts>
                <port>port_number</port>
                .
                .
        </extraPorts>
</portDiscovery>
<profileDiscovery>
        <collectHTTP>true|false</collectHTTP>
        <collectCIFS>true|false</collectCIFS>
        <httpPorts>
                <port>port_number</port>
                .
                .
        </httpPorts>
        <httpsPorts>
                <port>port_number</port>
                .
```

```
                .
                </httpsPorts>
        </profileDiscovery>
        <dnsDiscovery>
                <enabled>true|false</enabled>
                <useSystemDNSServer>true|false</useSystemDNSServer>
                <internalDNSServers>
                        <string>server_name</string>
                </internalDNSServers>
        </dnsDiscovery>
        <leakDiscovery>
                <enabled>true|false</enabled>
                <icmp>true|false</icmp>
                <udp>true|false</udp>
                <dns>true|false</dns>
                <snmp>true|false</snmp>
                <tcpPorts>
                        <port>port_number</port>
                        .
                        .
                </tcpPorts>
                <udpPorts>
                        <port>port_number</port>
                        .
                        .
                </udpPorts>
                <doInbound>true|false</doInbound>
                <doOutbound>true|false</doOutbound>
        </leakDiscovery>
        <bgpDiscovery>
                <enabled>true|false</enabled>
                <peers>
                        <bgppeer>
                                <password>bgp_password</password>
                                <address>bgp_ip</address>
                                <remoteAS>bgp_AS_number</remoteAS>
                                <enabled>true|false</enabled>
                        </bgppeer>
                        .
                        .
                </peers>
        </bgpDiscovery>
</collector>
</updateCollector_request>
```

This API will add a FULL collector configuration or update an existing collector configuration.

TYPE	URL	REQUIRES
POST:	/api/rest/zone/collector/{collectorId}/cidr/{cidrtype } ?append=true	Payload ➔ Content-type: application/xml <ZoneManagement_setCollectorCidrs_request> <addresses> <address>10.8.0.0/24</address> . . </addresses> </ZoneManagement_setCollectorCidrs_request>
This API will append CIDRs to collector CIDR list (cidrtype can be target, avoid or stop) **Please specify collectorId, cidrtype in the URL and CIDR list in the payload**		

TYPE	URL	REQUIRES
POST	/api/rest/zone/collector/{collectorId}/cidr/{cidrtype }	Payload ➔ Content-type: application/xml <ZoneManagement_setCollectorCidrs_request> <addresses> <address>10.8.0.0/24</address> . . </addresses> </ZoneManagement_setCollectorCidrs_request>
This API will replace a collector CIDR list with the ones given in payload (cidrtype can be target, avoid or stop) **Please specify collectorId, cidrtype in the URL and CIDR list in the payload**		

TYPE	URL	REQUIRES
DELETE	/api/rest/zone/collector/{collectorId}/cidr/{cidrtype }	Payload ➔ Content-type: application/xml <ZoneManagement_setCollectorCidrs_request> <addresses> <address>10.8.0.0/24</address> </addresses> </ZoneManagement_setCollectorCidrs_request>
This API will delete a CIDR from a collector CIDR list (cidrtype can be target, avoid or stop) **Please specify collectorId, cidrtype in the URL and CIDR list in the payload**		

TYPE	URL	REQUIRES
GET	/api/rest/zone/collector/{collectorId}/property/set/archived?value={0 or 1}	
This API will archive a collector (when value is set to 1). **This API will unarchive a collector (when value is set to 0).** **Please specify the collectorId.**		

TYPE	URL	REQUIRES
POST	/api/rest/zone/collector	Payload ➔ Content-type: application/xml <updateCollector_request> <collector> <id>*collector_id*</id> <name>*collector_name*</name> </collector> </updateCollector_request>
This API will update a collector's name. Please note that to change any attribute of a collector, all one needs is the collector id. Every other attribute that you put in the payload will update that attribute. In this API, please replace the collector_id with the collector id (which you want to update) and collector_name with the new name for the collector.		

TYPE	URL	REQUIRES
POST	/api/rest/zone/collector/{collectorId}/snmpcredential	Payload ➔ Content-type: application/xml <updateCollector_request> <credentials> <credential> <alias></alias> <community></community> </credential> <credential> <alias></alias> <authProtocol></authProtocol> <authPassphrase></authPassphrase> <privacyProtocol></privacyProtocol> <privacyPassphrase></privacyPassphrase> <username></username> <context></context> </credential> </credentials> </updateCollector_request>
This API will add SNMP credential(s) to a collector if no credentials exist and will replace SNMP credential(s) of a collector if there are existing credentials. Please replace the collectorId with the collector id (which you want to add/replace SNMP credentials). authProtocol can be set to SHA|MD5|NONE If authProtocol is set to NONE, we do not need to add authPassphrase privacyProtocol can be set to AES|DES|NONE If privacyProtocol is set to NONE, we do not need to add privacyPassphrase		

TYPE	URL	REQUIRES
POST	/api/rest/zone/collector/{collectorId}/snmpcredential?append=true|false	Payload ➔ Content-type: application/xml

		<updateCollector_request> <credentials> <credential> <alias></alias> <community></community> </credential> <credential> <alias></alias> <authProtocol></authProtocol> <authPassphrase></authPassphrase> <privacyProtocol></privacyProtocol> <privacyPassphrase></privacyPassphrase> <username></username> <context></context> </credential> </credentials> </updateCollector_request>
This API will append or update SNMP credential(s) of a collector. Please replace the collectorId with the collector id (which you want to add/replace SNMP credentials). **authProtocol can be set to SHA|MD5|NONE** **If authProtocol is set to NONE, we do not need to add authPassphrase** **privacyProtocol can be set to AES|DES|NONE** **If privacyProtocol is set to NONE, we do not need to add privacyPassphrase**		

TYPE	URL	REQUIRES
GET	/api/rest/config/feed/configs	no filters
This API will return current Integration configuration		

TYPE	URL	REQUIRES
POST	/api/rest/config/feed/config	Payload ➔ <updateFeedRequest> <feedconfig> <shortName>qualys</shortName> <serverName>*server_name*</serverName> <enabled>true|false</enabled> <pollInterval>*polling_interval*</pollInterval> <username>*username*</username> <password>*password*</password> <autosubscribe>true|false</autosubscribe> </feedconfig> </updateFeedRequest>
This API will set different parameters of qualys Integration. Parameters that can be configured are: **serverName ⇒set it to qualys server name or ip address** **enabled ⇒can be set to true or false** **pollInterval ⇒set it to polling interval in minutes** **username ⇒set it to base64 encoded username** **password ⇒ set it to base64 encoded password** **autosubscribe ⇒ can be set to true or false. If set to true, Lumeta will first subscribe the IPs unmanaged by Qualys and then push it in Asset Group created at Qualys server**		

TYPE	URL	REQUIRES
GET	/api/rest/service/{command}/{service}	We need to make two calls First one with command=enable and service=SNMPD. Second one with command=start and service=SNMPD. To enable and start snmpd.
This API will enable and start snmpd		

TYPE	URL	REQUIRES
GET	/api/rest/service/{command}/{service}	We need to make two calls First one with command=disable and service=SNMPD. Second one with command=stop and service=SNMPD. To disable and stop snmpd.
This API will disable and stop snmpd		

TYPE	URL	REQUIRES
GET	/api/rest/management/snmpd	
This API will return snmpd configuration information		

TYPE	URL	REQUIRES
POST	/api/rest/management/snmpd	Payload ⇒ <set_snmpd_request> <SNMPDaemonConfig> <readOnlyUser> <userName></userName> </readOnlyUser> <sysLocation></sysLocation> <sysContact></sysContact> <readOnlyCommunity> <community></community> </readOnlyCommunity> <readOnlyUser> <userName></userName> <authPassphrase></authPassphrase> <authProtocol></authProtocol> <privacyProtocol></privacyProtocol> <privacyPassphrase></privacyPassphrase> </readOnlyUser> </SNMPDaemonConfig>

	</set_snmpd_request>
This API will update snmpd configuration information	