REDSHIFT
NETWORKS
SECURING VOIP AND CLOUD COMMUNICATIONS

Redshift Networks

UCTM REST API

Document

Revision: 0.6

Date: 2023/03/21

Notes:

1. Subject to change without notice.
2. Released under non-disclosure agreements

Redshift Networks
12647 Alcosta Boulevard, Suite 450
San Ramon, CA 94583, USA
Tel: +1 925 272 0100, Tel: +1 866 824 5775 (toll free)
www.redshiftnetworks.com

Revision History

Revision	Date	Author	Comments
0.1	01/10/2019		Initial Draft version
0.2	07/01/2019		Updated with System status and statistics
0.3	10/03/2019		Updated with HDD and Ethernet Usage details
0.4	05/28/2021		Updated with new APIs for getting CPU, memory and other data
0.5	03/16/2023		Updated with new APIs for gre interface configuration
0.6	03/21/2023		Updated with new APIs for network group configuration

Table of Contents

1 Introduction

Redshift Networks REST API enables configuring and fetching data from RSN UCTM .

1.1. Purpose of this Document

The purpose of this document is to mainly explain REST APIs used for communication from Data Collector to RSN UCTM systems.

1.2. Intended Audience

Redshift Networks personnel involved in the development and testing of configuring RSN UCTMs through Data Collector.

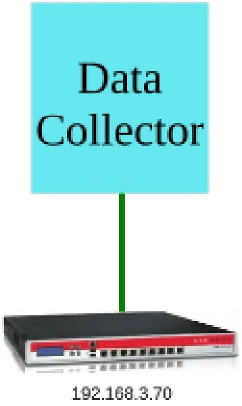
1.3. Abbreviations

RSN	Redshift Networks
UCTM	Unified Communications Threat Management
REST	REpresentational State Transfer
API	Application Programming Interface

1.4. Limitations

2 REST API

All the configuration data and get requests from Data Collector to each of the RSN UCTM systems will be sent through REST APIs.



3 REST APIs Explained

3.1. API Request Format

The API is a https request. This request should be created and sent to RSN UCTM. Https URL formed should be in below format.

```
req = requests.Session()    //create a session first
```

The request URL format:

```
resp = req.post('https://'+IP+':443/rs/rest/'+URL,verify=False,timeout=300)
```

Request parameters:

IP = Selected RSN UCTM IP address

URL = Path of the RESI API implementation in RSN UCTM including arguments

3.2. Response Format

A response for configuration requests contains success or failure. It can be checked as follows:

```
status = resp.content
if(status.lower() == 'success'):
    status = 'successfully updated.'
elif(status.lower() == 'failure'):
    status = 'failed to update.'
```

3.3. Response Format for Get Status/Statistics API

A response for get requests for system status and statistics gets the statistics data.

A code example of extracting the data using json is as follows:

```
jsondata = sendConfig.send('systemstatusandstatistics/statsandstatus')
    parsed_json = json.loads(jsondata)
    for i in parsed_json:
        Type    = "\""+i['type']+"\""
        count   = i['totalPktCnt']
        prate   = i['pktRate']
        drate   = i['dropPktCnt']
        print "%s,%s,%s,%s" % (Type,count,prate,drate)
```

The output of above json code is as follows: (in a typical example)

```
"Total Memory","    16173828 kB"

"Used Memory","3747460 kB (23.0%)"

"CPU Usage","0.0%"
"Days To Expire","Permanent License"
"eth0","up"
"Speed"," 100Mb/s"
"eth1","down"
"Speed"," 100Mb/s"
"eth2","up"
"Speed"," 100Mb/s"
"eth3","up"
"Speed"," 100Mb/s"
"eth4","down"
"Speed"," 100Mb/s"
"eth5","up"
"Speed"," 100Mb/s"
```

3.4. Response Format for Get HDD and Ethernet usage API

Example Output format for HDD and Ethernet usage is as follows: (in a typical example):

```
{
"HDD Usage Details" : {
  "Total Space":"469452 MB",
  "Used Space":"14785 MB",
  "Available Space":"430821 MB",
  "Used Percentage":"3%"
 }
"Ethernet usage" : [
{
  "Iface":"eth0",
   "IPAddress":"192.168.3.21",
    "MTU":"1500",
    "Met":"0",
   "RX-OK":"63235",
  "RX-ERR":"0",
  "RX-DRP":"0",
  "RX-OVR":"0",
  "TX-OK":"389",
  "TX-ERR":"0",
  "TX-DRP":"0",
  "TX-OVR":"0"
 }
 {
  "Iface":"eth2",
  " IPAddress":"n/a",
  "MTU":"1500",
  "Met":"0",
  "RX-OK":"3276521",
  "RX-ERR":"0",
  "RX-DRP":"0",
  "RX-OVR":"0",
  "TX-OK":"2959466",
  "TX-ERR":"0",
  "TX-DRP":"0",
  "TX-OVR":"0"
 }
]
}
```

4 Get REST APIs Explained

4.1 API for getting System status and statistics

URL	*'systemstatusandstatistics/statsandstatus'*
result	*1. Total memory – Total memory available* *2. Used memory – Memory used* *3. CPU Usage – CPU utilization of server* *4. Days To Expire – contains license details* *5. Each network port, its status up/down and speed of each port*

4.2 API for getting HDD and Ethernet usage

URL	'ethernet/ethernetUsage'
result	*1. Total Space - Total HDD space* *2. Used Space – Space Used* *3. Available Space – HDD space available* *4. Used Percentage – Used HDD percentage* *5. Ethernet Usage Details – Each Interface , its IPAddress , MTU, Met, RX-OK, RX-ERR, RX-DRP, RX-OVR, TX-OK, TX-ERR, TX-DRP , TX-OVR*

4.3 API for getting ifconfig information

URL	'/systemdevicestats/ifconfig/' + interface interface please provide interface for which ifconfig information is to be retrieved
result	*1. Type – interface name* *2. Value – ifconfig information for the <interface>*

4.4 API for getting up time information

URL	'/systemdevicestats/uptime'
result	*1. Value – Up time information*

4.5 API for getting Free memory space

URL	'/systemdevicestats/freespace'
result	*1. Type – type of memory (mem, swap or total)* *2. info – amount of memory used* *3. total – total memory* *4. free – amount of memory available for use*

4.6 API for getting up time information

URL	'/systemdevicestats/uptime'
result	*1. Value – Up time information*

4.7 API for getting Chassis information

URL	'/systemdevicestats/chassisInfo'
result	*1. smbios – System Management BIOS version* *2. DMI – Desktop Management Interface* *3. handle* *4. manufacturer* *5. type* *6. lock* *7. version* *8. serialNumber* *9. assetTag* *10. boot_upState* *11. powerSupplyState* *12. thermalState* *13. securityStatus* *14. OEMInformation - Original Equipment Manufacturer Information* *15. height* *16. NumberOfPowerCords* *17. containedElements*

4.8 API for getting per-processor statistics

URL	'/systemdevicestats/mpstat'	
result	*type - mpstat*	
	Parameter	***Description***
	time	*Command Execution time*
	cpu	*Processor number. The keyword all indicates that statistics are calculated as averages among all processors.*
	usr	*Show the percentage of CPU utilization that occurred while executing at the user level*
	nice	*Show the percentage of CPU utilization that occurred while executing at the user level with nice priority.*
	sys	*Show the percentage of CPU utilization that occurred while executing at the system level (kernel). Note that this does not include time spent servicing hardware and software interrupts.*
	iowait	*Show the percentage of time that the CPU or CPUs were idle during which the system had an outstanding disk I/O request.*
	irq	*Show the percentage of time spent by the CPU or CPUs to service hardware interrupts.*
	soft	*Show the percentage of time spent by the CPU or CPUs to service software interrupts.*
	steal	*Show the percentage of time spent in involuntary wait by the virtual CPU or CPUs while the hypervisor was servicing another virtual processor.*
	guest	*Show the percentage of time spent by the CPU or CPUs to run a virtual processor.*
	idle	*Show the percentage of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.*

4.9 API for getting Disk space

URL	'/systemdevicestats/diskspace'
result	*1. info – Disk Space* *2. filesystem – name of the file system* *3. blocks_1k – block size in 1024 bytes* *4. used – blocks of memory used* *5. available – blocks of memory available* *6. use_percentage – total memory blocks usage percentage* *7. mountedOn – mount point of the file system* ***Note:*** *The above set of parameter-value pairs will be repeated for each of the disk partitions.*

5 Configuration REST APIs Explained

5.1 Configuration API for Error Response Rate Monitor

URL	*‘/protectionconfig/applyConfig/errorResponseRateMonitor/'+record*
record	*“errorcount::interval::errorset::action::enabled”*
Error Count	The maximum number of error responses allowed in the interval. Default value is 20.
Interval (ms)	The interval (time window) in which the error responses are counted. Default value is 60000.
Error Response Set	Defines the error responses, such as 400-600.

5.2 Configuration API for For Flood Monitor

URL	*‘/protectionconfig/applyConfig/floodMonitor/'+record*
record	*“samplesize::deltafactor::reductionfactor::enabled”*
Window Size	The window size used to calculate request rates. Default value is 10.
Delta Increase in factor	The threshold used by the algorithm. Default value is 2.0.
Reduction Factor	A factor (between 0 and 0.99) determining the memory of the algorithm. Default value is 0.25.

5.3 Configuration API for Options Rate Monitor

URL	*‘/protectionconfig/applyConfig/optionsRateMonitor/'+record*
record	*“requestcount::interval::enabled”*
Options count	The maximum number of requests allowed in the interval. Default is 20.
Interval (ms)	The interval (time window) in which the requests are counted. The default value is 60000.

5.4 Configuration API for Request Rate Monitor

URL	*/protectionconfig/applyConfig/requestRateMonitor/'+record*
record	*“count::interval::action::enabled”*
Request count	The maximum number of requests allowed in the interval. Default is 30.
Session Limit	The interval (time window) in which the requests are counted. The default value is 60000.

5.5 Configuration API for Simultaneous Monitor

URL	*‘/protectionconfig/applyConfig/simultaneousSessionRateMonitor/'+record*
record	*“sessions::action::enabled”*
Request count	The maximum number of requests allowed in the interval. Default is 30.

5.6 Configuration API for Session Duration Monitor

URL	*‘/protectionconfig/applyConfig/sessionDurationRateMonitor/'+record*
record	*”maxduration::mindeviation::minduration::count::action::enabled”*
MaxDuration (s)	It is assumed that most calls are shorter than MaxDuration. (Example 1 hr)
MinDuration (s)	It is assumed that most calls are longer than MinDuration (Example 5 sec)
MinDeviation (s)	The minimum allowed deviation between the longest and the shortest call.
SampleCount	Enter the sampleCount it should be in range between 1 to 10,000.

5.7 Configuration API for War Dialing Monitor

URL	*‘/protectionconfig/applyConfig/warDialingMonitor/'+record*
record	*”maxwardialling::interval::wardiallingtype::action::enabled”*
MaxWarDialing Attempts	Number of maximum war dialing attempts during the configured time interval.
Time Interval (s)	Time duration during which if MaxwarDialing attempts reached and alert or action should happen.

WarDialing Type	To track only Source Number irrespective of IP Address.

5.8 Configuration API for Wangiri Fraud Monitor

URL	*'/protectionconfig/applyConfig/wangiriFraud/'+record*
record	*"callAttempts::interval::calltype::action::enabled"*
Number Of One Ring Call Attempts	Number Of One Ring Call Attempts
Time Interval (s)	Time duration in seconds during which One Ring and Cut Call Attempts are monitored.
Call Type	Enter the Type of call from "Call Type" – Local, Long Distance, International OR All

5.9 Configuration API for SQL Injection Monitor

URL	*'/protectionconfig/applyConfig/sqlInjectionMonitor/'+record*
record	*"sqlPattern::action::enabled"*
Pattern	Enter the SQL commands to which the policy applies. Use a pipe symbol (|) to separate multiple commands (for example, SELECT|INSERT|UPDATE).

5.10 Configuration API for RTP Monitor

URL	*'/protectionconfig/applyConfig/rtpMonitor/'+record*
record	*"seqNumber::action::enabled"*
Sequence number Range	Specify the range of sequence numbers allowed from next expected sequence number in the system.

5.11 Configuration API for Error Rate Tracking

URL	*'/protectionconfig/addRule/errorRateTracking/'+record*
record	*enable::rulename::errorgroup::timewindow::limit::trackingtype::serveraddress::clientaddress::action::comment*
Rule name	A unique string to identify the rule.

Error group	Enter group name from the list of configured Error response code groups.
Time window	(In Minutes) Window duration for which the calls need to be tracked. This is a sliding window which ends at the current system time.
Limit	The limit to be applied for the Error responses (in number).
Tracking Type	Enter Server IP Address Group or Client IP Address Group to track responses from the server.
Server address	Enter the required Server IP Address Group to track only specified IP Addresses in that group.
Client address	Enter the required Client IP Address Group to track only specified IP Addresses in that group.

5.12 Configuration API for Country Call Rate Tracking

URL	*'/protectionconfig/addRule/countrycallrate/'+record*
record	*enabled::name::trackingType::timeWindow::limit::countryGroup::callDirection::action::comment*
Name	A unique string to identify the rule.
Tracking Type	Enter "Call Volume" for tracking the count of calls made by the user OR "Call Minutes" for duration based tracking.
Time Window	(In Minutes) Window duration for which the calls need to be tracked.
Limit	The limit to be applied on "Call Volume" (in number) or "Call Minutes" (in minutes).
Country group	Enter the Country Group from Country Groups. "Any" indicates applicable for all the Countries call Rate.
Call Direction	Call Direction describes the call type(Incoming/outgoing). All for both.

5.13 Configuration API for Source Call Rate Tracking

URL	*'/protectionconfig/addRule/sourcecallrate/'+record*
record	*enabled::dispersionEnabled::name::dispersionIndex::trackingType::timeWindow::sourceType::limit::sourcetracking::sourcePattern::skipSourcePattern::srcUserGroup::desUserGroup::callDirection::action::comment*

Name	A unique string to identify the rule.
Dispersion Index	Enter the percentage value in dispersion index.
Tracking type	Enter one of the following: **Call Volume** for tracking based on the the calls count made by the user **Call Minutes** for call duration based tracking. **Call Cost** for tracking based on on call cost. The cost will be taken from the call cost file uploaded through Call Cost configuration.
Time Window	(In Minutes) Window duration for which the calls need to be tracked. This is a sliding window which ends at the current system time.
Source Type	Enter "Source Pattern" to track all the calls matching with the configured pattern of Phone Number. OR enter "Source Group" to track all the Source Numbers from that Group.
Limit	The limit to be applied on "Call Volume" (in number) or "Call Minutes" (in minutes).
Source Tracking	If "Source Pattern" is entered in "Source Type", it will enable Originating Phone Number, Originating IP Address and Phone Number and Originating IP Address only. If "Source Group" is entered in "Source Type", it will enable all of the following: **Originating Phone Number :** To track only Source Number irrespective of IP Address. **Originating IP Address and Phone Number :** To track Source Number along with IP Address. **Originating IP Address :** To track Source Number from particular IP Address. **Originating Group :** To track configured Source User Group. **Originating Group With Individual entities :** To track individual entities from that Source User Group.
Source Pattern	Dial Call format to be specified as an alpha numeric character list. Check on "**Control -> Dial Call Format**" screen for more details on the format. Source numbers matching this pattern will be tracked.
Skip Source Pattern	Enter the source pattern to skip source pattern from source number
Src User Group	Enetr a user group or enter ANY to apply all gorups that initiate calls.

Dst User Group	Enter a user group or enter ANY to apply all groups that initiate calls.
Call Direction	Call Direction describes the call type(Incoming/outgoing) of the call. All describes both incoming and outgoing calls.

5.14 Configuration API for New Country Call Rate Tracking

URL	*'/protectionconfig/addRule/newcountrycallrate/'+record*
record	*enabled::Name::timeWindow::limit::days::fromTime::toTime::action::comment*
Name	A unique string to identify the rule.
Rime Window	(In Minutes) Window duration for which the calls need to be tracked.
Limit	The limit to be applied for the calls (in number).
Days	It is used to configure the call limit in specific days.
From Time	Enter the from time, when the configured rule has to start.
To Time	Enter the to time, when the configured rule has to stop.

5.15 Configuration API for Device Integrity

URL	*'/protectionconfig/addRule/deviceIntegrity/'*+record
record	*user number::src address::server address::user agent::reason*
The Device Integrity feature does not allow clients to get registered from different locations. An administrator can decide to allow if a certain set of clients can register from different locations (for example, wireless clients) by adding the new client to this list.	

5.16 Configuration API for Malicious User Agent Enable

URL	*'/protectionconfig/enable/maliciousUserAgent/'*+record
record	enable
Enable the feature to raise alerts when there are call to/from the malicious user agent.	

5.17 Configuration API for Malicious User Agent

URL	*‘/protectionconfig/addRule/maliciousUserAgent/’+record*
record	*useragent*
User agent	Malicious User Agent name

5.18 Configuration API for Safelist Numbers

URL	*‘/protectionconfig/addRule/safeListNumber/’+record*
record	*user number::comment*
Number	*Number to be added to the safelist.*
Comment	*Comments about SafeList Number.*

5.19 Configuration API for Blacklist Numbers

URL	*‘/protectionconfig/addRule/blacklistcountry/‘*+record
record	*type::value*
Type	Type specifies the Banned Terminating Country to ban the country for calling.
Value	This is Country name. Add banned country name

6 GRE Configuration REST APIs

6.1 Configuration API for adding GRE interface

URL	*'/rs/rest/greConfig/gre/'+record*
record	*"greName::Ifname::localAddr::remoteAddr"*
greName	This is the name for the gre interface to be created.
Ifname	Network interface name of the gre interface
localAddr	This is the local IP address of the gre interface
remoteAddr	This is the remote IP address of the gre interface

6.2 Configuration API for For delete GRE interface

URL	*'/rs/rest/greConfig/gre/'+record*
record	*"greName"*
greName	This is the name of the GRE interface to be deleted.

6.3 Configuration API for getting GRE interface

URL	*'/rs/rest/greConfig/gre/'+record*
record	*"greName" or "all"*
greName	*Specify greName for details of a specific gre interface* *Specify "all" for getting all the gre interfaces.*

7 Network Group Configuration REST APIs

7.1 Configuration API for adding Network Group

URL	*'rs/rest/networkGroup/group/'+record*
record	*"GrpName::TargetType::TargetTypeValue::Afi_action::Description"*
GrpName	This is a unique name to identify the network group.
TargetType	Target type is one of the following: vlan, usergroup, ipaddress OR tunnelGroup
TargetTypeValue	Choose the Target type value as per below description based on the selected target type **vlan**: This is vlan name. For multiple valn names, use them separated with comma like 1111,123,456. **userGroup**: This is user name. User group names can be viewed in UCTM GUI page at Control->Policy->User Groups. **ipaddress**: This is user IP group name. User IP group names can be viewed in UCTM GUI page at Control->Policy->User IP Groups. **tunnelGroup**: This is Tunnel group name. Use comma separated tunnel group names for multiple values like tungr1,tungr2,tungr3.
Afi_action	Use one of the actions as required: block, un-block OR none.
Description	This is the Description for group creation. Please use '%20' wherever space is needed.
Example	curl -X POST -H "Content-Type: application/json" -k https://10.20.4.124:443/rs/rest/networkGroup/group/VP6::tunnelGroup::gr::block::New%20Proxy

7.2 Configuration API for For deleting Network Group

URL	*'rs/rest/networkGroup/group/'+record*
record	*"grpName"*
greName	This is the name of the Network Group to be deleted.
Example	curl -X DELETE -H "Content-Type: application/json" -k https://10.20.4.124:443/rs/rest/networkGroup/group/nwgrpname

7.3 Configuration API for getting Network Groups

URL	*‘rs/rest/networkGroup/group/'+record*
record	*“grpName” or “all”*
grpName	*Specify grpName for details of a specific Network Group* *Specify “all” for getting all the Network groups.*
Example	curl -X GET "Content-Type: application/json" -k https://10.20.4.124:443/rs/rest/networkGroup/group/nwgrpname or all