RSA NETWITNESS® PLATFORM

NetWitness Plaform API User Guide

for RSA NetWitness® Platform 11.3

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

November 2019

Table of Contents

Overview

The NetWitness Platform API can be accessed using the same host and port as the NetWitness user interface.

Current Version

By default, all requests to the REST API will automatically use the latest version of the API available. To provide API stability, clients can specify the API version to use by adding the `NetWitness-Version` HTTP header:

```
NetWitness-Version: 1.0
```

Schema

All data is sent and received as JSON. Any resources containing fields without values will have those fields included with `null` as the value instead of being omitted.

Any fields containing timestamps or dates will be in ISO 8601 format:

```
YYYY-MM-DDTHH:MM:SS.SSSZ
```

HTTP Usage

The RSA NetWitness API tries to adhere as closely as possible to standard HTTP and REST conventions in its use of HTTP verbs and status codes.

HTTP Verbs

Verb	Usage
`GET`	Used to retrieve a resource.
`POST`	Used to create a new resource.
`PATCH`	Used to update an existing resource, including partial updates. Only fields that are modified should be included in the request.
`PUT`	Used to replace an existing resource.
`DELETE`	Used to delete an existing resource.

HTTP Status Codes

Status code	Usage
`200 OK`	The request completed successfully.

`201 Created`	A new resource has been created successfully. The resource's URI is available from the response's `Location` header.
`204 No Content`	An update to an existing resource has been applied successfully.
`400 Bad Request`	The request was malformed. The response body will include an error providing further information. See Error Response.
`401 Unauthorized`	Similar to `403 Forbidden`, but specifically for use when authentication is required and has failed or has not yet been provided. See Authentication and Authorization.
`403 Forbidden`	The request was valid, but the server is refusing the action. The user might not have the necessary permissions for a resource.
`404 Not Found`	The requested resource does not exist.
`500 Internal Server Error`	An unexpected error has occurred. The response body will include a message providing further information.

Case Sensitive

All URLs, request parameters and JSON fields are case sensitive.

Error Response

A common JSON structure is always returned for errors:

Path	Type	Description
`status`	`Number`	The HTTP status code returned.
`timestamp`	`String`	The timestamp of the request.
`errors[]`	`Array`	An array of errors for the given request.
`errors[].message`	`String`	A user-friendly error message explaining what went wrong.
`errors[].field`	`String`	The field or parameter containing the error.

```
{
  "status" : 400,
  "timestamp" : "2019-12-03T14:08:19.944Z",
  "errors" : [ {
    "message" : "Value must be less than or equal to \"10\"",
    "field" : "start"
  }, {
    "message" : "Invalid range"
  } ]
}
```

Pagination

A common JSON structure is always used for paginated results:

Path	Type	Description
`items`	`Array`	An array containing the requested resources.
`pageNumber`	`Number`	The requested page number.
`pageSize`	`Number`	The requested number of items to return in a single page.
`totalPages`	`Number`	The total number of pages available.
`totalItems`	`Number`	The total number of items available.
`hasNext`	`Boolean`	Indicates if there is a page containing results after this page.
`hasPrevious`	`Boolean`	Indicates if there is a page containing results before this page.

```
{
  "items" : [ ],
  "pageNumber" : 0,
  "pageSize" : 10,
  "totalPages" : 3,
  "totalItems" : 25,
  "hasNext" : true,
  "hasPrevious" : false
}
```

Authentication and Authorization

All requests must include the `NetWitness-Token` HTTP header containing a valid JSON Web Token (JWT):

```
NetWitness-Token:
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1MTEyNDczODYyNjMsImlzcyI6InNlY3VyaXR5L
XNlcnZlci0zODA1NTA0OS0xZWMyLTQ0MDAtOTUwYS0zZTVkMmJiYTljMjIiLCJpYXQiOjE1MTEyMTEzODYyNjM
sImF1dGhvcml0aWVzIjpbIkFkbWluaXN0cmF0b3JzIl0sInVzZXJfbmFtZSI6ImFkbWluIn0.StBjg9ruIX4Fr
yfCX8qvrSBGZHF8DN3qHZM0Ei9-
thFndm1q_DLP_cnh8Fpm43fdKcs1ErcVRTqhaYvVULYmsF9ShUaSThpLts6zbJVEKlq3ldUGWWCY9bfVGRH3n5
KmWzITPi7xZ-
Rf_Kp2Sj8ecVAip3qDwha7TxYrReXefCnUj0UxgaaXjeZIFjwxFmK6NPZ7TAK9OcvcVhozaR8V92g1kUVP8_54
x7iZ2jL4JvDPaScWBjBTvVEffHNbX9_iLNoRmKqvDELSla6E_trkSREogCt6pZh709Qh70uoC3BsKwNQKbHNEO
U1tRPFaUFfRH7bCdp8v3Aeh3PTaKEuQA
```

The JSON Web Token is defined in RFC-7519. Tokens can be obtained using the methods outlined below.

In the remainder of this document, the token will be truncated to just `eyJ...AT` for brevity.

Obtaining a Token

A JSON Web Token can be obtained using the methods below.

Using a Username and Password

Users can retrieve an access token using their username and password credentials. Since the API gateway is secured using TLS, all credentials will be encrypted in transit.

```
POST /rest/api/auth/userpass
```

Request Parameters

Parameter	Description
`username`	The username of the account to authenticate.
`password`	The password of the account.

Response Fields

Path	Type	Description
`id`	`String`	The account identifier.
`roles`	`Array`	The roles assigned to the user.

Path	Type	Description
accessToken	String	A digitally signed access token that is acceptable as proof of authentication at any Launch service that trusts the public key of this service. The string holds a JSON web-token. See RFC-7519.
refreshToken	String	A digitally signed refresh token that can be used to refresh an expired access token. Refresh tokens have longer expiry periods and can be used by services to re-authenticate users without (storing and) presenting credentials.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/auth/userpass' -i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1' \
    -d 'username=ian&password=changeMe'
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2019 14:07:21 GMT
Content-Length: 106
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```

```
{
  "id" : "ian",
  "roles" : [ "Analyst" ],
  "accessToken" : "eyJ...AT",
  "refreshToken" : "eyJ...AT"
}
```

Using a Refresh Token

Users can also retrieve an access token using a refresh token.

```
POST /rest/api/auth/token
```

Request Parameters

Parameter	Description
token	A refresh token.

Response Fields

Path	Type	Description
id	String	The account identifier.
roles	Array	The roles assigned to the user.
accessToken	String	A digitally signed access token that is acceptable as proof of authentication at any Launch service that trusts the public key of this service. The string holds a JSON web-token. See RFC-7519.
refreshToken	String	A digitally signed refresh token that can be used to refresh an expired access token. Refresh tokens have longer expiry periods and can be used by services to re-authenticate users without (storing and) presenting credentials.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/auth/token' -i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1' \
    -d
'token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1Nzc5NzQwNDE1NzIsImlzcyI6InNlY3
VyaXR5LXNlcnZlci0yNGNlYjMwMi1mMDdlLTQ1ZjAtYTg4My1lZWQ1NmQ0NDQ2ZmQiLCJpYXQiOjE1NzUzODIw
NDE1NzIsInJlZnJlc2giOnRydWUsInVzZXJfbmFtZSI6ImlhbiJ9.1Yo_uLFThnPUCrNzUi9BbkgaMwSdCJLIe
e1h-
gZKfoeYsqKeS13Ayk0KjCDR5_JFe9LkohEnNB92jLA0goU4BQyQQgV7ladAGcSmT1SXd9YyTxZvKTklJ_jWC-
UChy54ZWKbrhMwd9GDrEbpT7vXGd8cSsW6jY_1Jg2YeKYBdOh2ZA5L4aGeCqUmzVVkFfdtIrce7LVC0j3ISeYB
15S6XV6K5UYx18xUhI5eNPlQsTdG0bKby5tTG1BMOIjJg9GHjrRaJyPYM9u7kf7ZVz2i-
D4ZrceURa2TzCXAVOZnv3gKpnYm3hYR4R5q_6LAJNC5CQU5tQ0shhLyti9GJGFzhQ'
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2019 14:07:21 GMT
Content-Length: 106
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```

```
{
  "id" : "ian",
  "roles" : [ "Analyst" ],
  "accessToken" : "eyJ...AT",
  "refreshToken" : "eyJ...AT"
}
```

Authorization

In order to make requests through the NetWitness Platform API, users must belong to roles that have the `integration-server.api.access` permission, as well as any underlying permissions required to fulfill the request.

Incidents

An Incident is a logically grouped set of alerts created automatically by the Incident Aggregation Engine and grouped by a specific criteria. An Incident, available in the Respond Interface, allows an Analyst to triage, investigate, and remediate these groups of alerts. Incidents can be moved between users, notated, and explored via the nodal graph. Incidents allow users to ensure they understand the full scope of an attack or event in their NW system and then take action.

Attributes

The incident resource is comprised of the following attributes:

Path	Type	Description
`id`	`String`	The unique identifier of the incident.
`title`	`String`	The title of the incident.
`summary`	`String`	The summary of the incident.
`priority`	`String`	The incident priority. See the valid values.
`riskScore`	`Number`	The incident risk score is calculated based on the associated alert's risk score. Risk score ranges from 0 (no risk) to 100 (highest risk).
`status`	`String`	The current status. See the valid values.
`alertCount`	`Number`	The number of alerts associated with an incident.
`averageAlertRiskScore`	`Number`	The average risk score of the alerts associated with the incident. Risk score ranges from 0 (no risk) to 100 (highest risk).
`sealed`	`Boolean`	Indicates if additional alerts can be associated with an incident. A `sealed` incident cannot be associated with additional alerts.
`totalRemediationTaskCount`	`Number`	The number of total remediation tasks for an incident.
`openRemediationTaskCount`	`Number`	The number of open remediation tasks for an incident.
`created`	`String`	The timestamp of when the incident is created.
`lastUpdated`	`String`	The timestamp of when the incident was last updated.
`lastUpdatedBy`	`String`	The NetWitness user identifier of the user who last updated the incident.
`assignee`	`String`	The NetWitness user identifier of the user currently working on the incident.
`sources`	`Array`	Unique set of sources for all of the alerts in an incident.

Path	Type	Description
`ruleId`	`String`	The unique identifier of the rule that created the incident.
`firstAlertTime`	`String`	The timestamp of the earliest occurring Alert in this incident.
`categories`	`Array`	The list of categories this incident is categorized under.
`categories[].id`	`String`	The unique category identifier.
`categories[].parent`	`String`	The parent name of the category.
`categories[].name`	`String`	The friendly name of the category.
`journalEntries`	`Array`	Set of notes about the incident investigation, also known as the JournalEntry.
`journalEntries[].id`	`String`	The unique journal entry identifier.
`journalEntries[].author`	`String`	The author of this entry.
`journalEntries[].notes`	`String`	Notes and observations about the incident.
`journalEntries[].created`	`String`	The timestamp of the journal entry created date.
`journalEntries[].lastUpdated`	`String`	The timestamp of the journal entry last updated date.
`journalEntries[].milestone`	`String`	Incident milestone classifier. See the valid values.
`createdBy`	`String`	The NetWitness user id or name of the rule that created the incident.
`deletedAlertCount`	`Number`	The number of alerts that are deleted from the incident.
`eventCount`	`Number`	The number of events associated with incident.
`alertMeta`	`String`	An object containing unique set of meta values, by type, across all alerts associated with this incident.
`alertMeta.SourceIp`	`Array`	Unique source IP addresses.
`alertMeta.DestinationIp`	`Array`	Unique destination IP addresses.

Incident Priority

The `priority` field can contain these values:

Value	Description
`Low`	Low Priority
`Medium`	Medium Priority
`High`	High Priority
`Critical`	Critical

Incident Status

The `status` field can contain these values:

Value	Description
`New`	New incident.
`Assigned`	Incident is assigned to a user.
`InProgress`	Incident response is in progress.
`RemediationRequested`	Remediation tasks have been requested.
`RemediationComplete`	Remediation tasks are complete.
`Closed`	Incident is closed.
`ClosedFalsePositive`	Incident is closed as it was created due to false positive.

Milestone

Each journal entry can contain a `milestone` consisting of these values:

Value	Description
`Reconnaissance`	Intruder is in the initial phase of the attack where targets and vulnerabilities are identified.
`Delivery`	Intruder transmitted malware to the target.
`Exploitation`	Malware code triggers, which takes action on target network to exploit vulnerability.
`Installation`	Malware weapon installs access point usable by intruder.
`CommandAndControl`	Malware enables intruder to have persistent access to target network.
`ActionOnObjective`	Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.
`Containment`	Incident is contained.
`Eradication`	Necessary actions taken to eliminate components of incident and restore the system status.
`Closure`	Incident is addressed.

Requests

Get a Single Incident

A single incident can be retrieved using an incident's unique identifier.

```
GET /rest/api/incidents/{id}
```

Path Parameters

Parameter	Description
`id`	The unique identifier of the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 1329
Date: Tue, 03 Dec 2019 14:09:46 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```

```
{
  "id" : "INC-100",
  "title" : "Suspected C&C with suspicious-domain.com",
  "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
  "priority" : "Critical",
  "riskScore" : 100,
  "status" : "InProgress",
  "alertCount" : 1,
  "averageAlertRiskScore" : 100,
  "sealed" : true,
  "totalRemediationTaskCount" : 4,
  "openRemediationTaskCount" : 5,
  "created" : "2018-01-01T04:49:27.870Z",
  "lastUpdated" : "2019-12-03T14:09:47.002Z",
  "lastUpdatedBy" : "norm",
  "assignee" : "ian",
  "sources" : [ "Malware Analysis" ],
  "ruleId" : "55e49a79e4b01a1d2be502bc",
  "firstAlertTime" : "2017-08-04T16:49:22Z",
  "categories" : [ {
    "id" : "55e49a79e4b01a1d2be5022e",
    "parent" : "Malware",
    "name" : "Password dumper"
  }, {
    "id" : "55e49a79e4b01a1d2be50228",
    "parent" : "Hacking",
    "name" : "Path traversal"
  } ],
  "journalEntries" : [ {
    "id" : "20",
    "author" : "admin",
    "notes" : "Updated status",
    "created" : "2017-11-15T20:20:54.785Z",
    "lastUpdated" : "2017-11-15T20:20:54.785Z",
    "milestone" : "Containment"
  } ],
  "createdBy" : "norm",
  "deletedAlertCount" : 100,
  "eventCount" : 0,
  "alertMeta" : {
    "SourceIp" : [ "10.11.12.345" ],
    "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
  }
}
```


Get Incidents by Date Range

Incidents can be retrieved by the date and time they were created.

```
GET /rest/api/incidents
```

The requested date range can be unbounded, by only supplying either the `since` or `until` parameter, or bounded, by providing both parameters.

Request Parameters

Parameter	Description
`pageNumber`	The requested page number.
`pageSize`	The maximum number of items to return in a single page.
`since`	A timestamp in ISO 8601 format (e.g., `1018-01-01T14:00:00.000Z`). Retrieve incidents created on and after this timestamp.
`until`	A timestamp in ISO 8601 format (e.g., `1018-01-01T14:00:00.000Z`). Retrieve incidents created on and before this timestamp.

All results will be returned using the paginated response payload sorted by the `created` date, in descending order.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents?since=2018-01-
01T04%3A00%3A00.000Z&until=2018-01-01T05%3A00%3A00.000Z&pageSize=100&pageNumber=0' -i
-X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 1560
Date: Tue, 03 Dec 2019 14:09:45 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```


```
{
  "items" : [ {
    "id" : "INC-100",
    "title" : "Suspected C&C with suspicious-domain.com",
    "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
    "priority" : "Critical",
    "riskScore" : 100,
    "status" : "Assigned",
    "alertCount" : 1,
    "averageAlertRiskScore" : 100,
```

```
    "sealed" : true,
    "totalRemediationTaskCount" : 4,
    "openRemediationTaskCount" : 5,
    "created" : "2018-01-01T04:49:27.870Z",
    "lastUpdated" : "2017-08-04T16:49:27.870Z",
    "lastUpdatedBy" : "norm",
    "assignee" : "tony",
    "sources" : [ "Malware Analysis" ],
    "ruleId" : "55e49a79e4b01a1d2be502bc",
    "firstAlertTime" : "2017-08-04T16:49:22Z",
    "categories" : [ {
      "id" : "55e49a79e4b01a1d2be5022e",
      "parent" : "Malware",
      "name" : "Password dumper"
    }, {
      "id" : "55e49a79e4b01a1d2be50228",
      "parent" : "Hacking",
      "name" : "Path traversal"
    } ],
    "journalEntries" : [ {
      "id" : "20",
      "author" : "admin",
      "notes" : "Updated status",
      "created" : "2017-11-15T20:20:54.785Z",
      "lastUpdated" : "2017-11-15T20:20:54.785Z",
      "milestone" : "Containment"
    } ],
    "createdBy" : "norm",
    "deletedAlertCount" : 100,
    "eventCount" : 0,
    "alertMeta" : {
      "SourceIp" : [ "10.11.12.345" ],
      "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
    }
  } ],
  "pageNumber" : 0,
  "pageSize" : 100,
  "totalPages" : 1,
  "totalItems" : 1,
  "hasNext" : false,
  "hasPrevious" : false
}
```


Update an Incident

Currently an incident's `status` and `assignee` can be modified using the incidents endpoint.

```
PATCH /rest/api/incidents/{id}
```

The `assignee` field must include the unique identifier for a valid NetWitness user. The list of users can be found in the security section of the administration user interface.

Request Fields

Path	Type	Description
`status`	`String`	The current status. See the valid values.
`assignee`	`String`	The NetWitness user identifier of the user currently working on the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i -X PATCH \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Content-Type: application/json;charset=UTF-8' \
    -d '{"status":"InProgress"}'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 1330
Date: Tue, 03 Dec 2019 14:09:46 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```

```
{
  "id" : "INC-100",
  "title" : "Suspected C&C with suspicious-domain.com",
  "summary" : "Security Analytics detected communications with suspicious-domain.com
that may be command and control malware.",
  "priority" : "Critical",
  "riskScore" : 100,
  "status" : "InProgress",
  "alertCount" : 1,
  "averageAlertRiskScore" : 100,
  "sealed" : true,
  "totalRemediationTaskCount" : 4,
  "openRemediationTaskCount" : 5,
  "created" : "2018-01-01T04:49:27.870Z",
  "lastUpdated" : "2019-12-03T14:09:46.620Z",
  "lastUpdatedBy" : "norm",
  "assignee" : "tony",
  "sources" : [ "Malware Analysis" ],
  "ruleId" : "55e49a79e4b01a1d2be502bc",
  "firstAlertTime" : "2017-08-04T16:49:22Z",
  "categories" : [ {
    "id" : "55e49a79e4b01a1d2be5022e",
    "parent" : "Malware",
    "name" : "Password dumper"
  }, {
    "id" : "55e49a79e4b01a1d2be50228",
    "parent" : "Hacking",
    "name" : "Path traversal"
  } ],
  "journalEntries" : [ {
    "id" : "20",
    "author" : "admin",
    "notes" : "Updated status",
    "created" : "2017-11-15T20:20:54.785Z",
    "lastUpdated" : "2017-11-15T20:20:54.785Z",
    "milestone" : "Containment"
  } ],
  "createdBy" : "norm",
  "deletedAlertCount" : 100,
  "eventCount" : 0,
  "alertMeta" : {
    "SourceIp" : [ "10.11.12.345" ],
    "DestinationIp" : [ "11.11.11.111", "11.22.33.444" ]
  }
}
```


Remove an Incident

A single incident can be removed using the incident's unique identifier.

```
DELETE /rest/api/incidents/{id}
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100' -i -X DELETE \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 204 No Content
Date: Tue, 03 Dec 2019 14:09:47 GMT
```

```
```

Add a Journal Entry

A journal entry, or note, can be added to an existing incident.

```
POST /rest/api/incidents/{id}/journal
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Request Fields

Path	Type	Description
author	String	The NetWitness user id of the user creating the journal entry.
notes	String	Notes and observations about the incident.
milestone	String	The incident milestone classifier.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-100/journal' -i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Content-Type: application/json;charset=UTF-8' \
    -d '{"author":"duke","notes":"This incident is
contained.","milestone":"Containment"}'
```

Sample Response

```
HTTP/1.1 201 Created
Location: https://api.netwitness.local/rest/api/incidents/INC-100
Date: Tue, 03 Dec 2019 14:09:47 GMT
```

```
```

Get an Incident's Alerts

All the alerts that are associated with an incident can be retrieved using the incident's unique identifier.

```
GET /rest/api/incidents/{id}/alerts
```

Path Parameters

Parameter	Description
id	The unique identifier of the incident.

Request Parameters

Parameter	Description
pageNumber	The requested page number.
pageSize	The maximum number of items to return in a single page.

Response Fields

Path	Type	Description
items	Array	An array containing the requested resources.
pageNumber	Number	The requested page number.
pageSize	Number	The requested number of items to return in a single page.
totalPages	Number	The total number of pages available.
totalItems	Number	The total number of items available.

Path	Type	Description
hasNext	Boolean	Indicates if there is a page containing results after this page.
hasPrevious	Boolean	Indicates if there is a page containing results before this page.
items[].id	String	The unique alert identifier.
items[].title	String	The title or name of the rule that created the alert.
items[].detail	String	The details of the alert. This can be the module name or meta that the module included.
items[].created	String	The timestamp of the alert created date.
items[].source	String	The source of this alert. For example, "Event Stream Analysis", "Malware Analysis", etc.
items[].riskScore	Number	The risk score of this alert, usually in the range 0 - 100.
items[].type	String	The type of alert, "Network", "Log", etc.
items[].events	Array	The events that make up this alert.
items[].events[].source	Object	The source of the event.
items[].events[].source.device	Object	The device contains the endpoint network information.
items[].events[].source.device.ipAddress	String	The IP address.
items[].events[].source.device.port	Number	The port.
items[].events[].source.device.macAddress	String	The ethernet MAC address.
items[].events[].source.device.dnsHostname	String	The DNS resolved hostname.
items[].events[].source.device.dnsDomain	String	The top-level domain from the DNS resolved hostname.
items[].events[].source.user	Object	The user contains the endpoint user information.
items[].events[].source.user.username	String	The unique username.
items[].events[].source.user.emailAddress	String	An email address.
items[].events[].source.user.adUsername	String	An Active Directory (AD) username.
items[].events[].source.user.adDomain	String	An Active Directory (AD) domain.
items[].events[].destination	Object	The destination of the event.
items[].events[].destination.device	Object	The device contains the endpoint network information.
items[].events[].destination.device.ipAddress	String	The IP address.

Path	Type	Description
items[].events[].destination.device.port	Number	The port.
items[].events[].destination.device.macAddress	String	The ethernet MAC address.
items[].events[].destination.device.dnsHostname	String	The DNS resolved hostname.
items[].events[].destination.device.dnsDomain	String	The top-level domain from the DNS resolved hostname.
items[].events[].destination.user	Object	The user contains the endpoint user information.
items[].events[].destination.user.username	String	The unique username.
items[].events[].destination.user.emailAddress	String	An email address.
items[].events[].destination.user.adUsername	String	An Active Directory (AD) username.
items[].events[].destination.user.adDomain	String	An Active Directory (AD) domain.
items[].events[].domain	String	The top-level domain or Windows domain.
items[].events[].eventSource	String	The source of the event. This may be a fully-qualified hostname with a port, or simple name.
items[].events[].eventSourceId	String	The unique identifier of the event on the source. For Network and Log events, this is the Nextgen Session ID.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/incidents/INC-
100/alerts?pageSize=10&pageNumber=0' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 1301
Content-Type: application/json;charset=UTF-8
Date: Tue, 03 Dec 2019 14:09:47 GMT
Transfer-Encoding: chunked
```


```
{
  "items" : [ {
    "id" : "5a6b81639491573f1e73676c",
    "title" : "LogOn Rule",
    "detail" : "Module_5a5cddb3e4b0ac40016df562_Alert",
```

```
    "created" : "2018-01-26T19:28:35Z",
    "source" : "Event Stream Analysis",
    "riskScore" : 90,
    "type" : "Network",
    "events" : [ {
      "source" : {
        "device" : {
          "ipAddress" : "58.229.117.56",
          "port" : 57429,
          "macAddress" : "00:13:c3:3b:c7:00",
          "dnsHostname" : null,
          "dnsDomain" : null
        },
        "user" : {
          "username" : "wwwrun",
          "emailAddress" : null,
          "adUsername" : null,
          "adDomain" : null
        }
      },
      "destination" : {
        "device" : {
          "ipAddress" : "128.164.35.184",
          "port" : 21,
          "macAddress" : "00:17:df:6b:c8:00",
          "dnsHostname" : null,
          "dnsDomain" : null
        },
        "user" : {
          "username" : "wwwrun",
          "emailAddress" : null,
          "adUsername" : null,
          "adDomain" : null
        }
      },
      "domain" : null,
      "eventSource" : "10.4.61.48:56005",
      "eventSourceId" : "9318"
    } ]
  } ],
  "pageNumber" : 0,
  "pageSize" : 10,
  "totalPages" : 1,
  "totalItems" : 1,
  "hasNext" : false,
  "hasPrevious" : false
}
```

Services Information

Get Service IDs of all Services

The following API lists all services with their service IDs.

The response resource is comprised of the following attributes:

Path	Type	Description
`[]`	`Array`	Array of service information.
`[].id`	`String`	Unique identifier of each service installed in the RSA NetWitness suite.
`[].name`	`String`	Name of the service. For example, endpoint-server.
`[].displayName`	`String`	Display name of the service.
`[].host`	`String`	Host details of the service.
`[].version`	`String`	Version of the service.

A list of all services can be retrieved using the following API:

```
GET /rest/api/services
```

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/services' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Content-Type: application/json;charset=UTF-8'
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2019 14:05:58 GMT
Content-Type: application/json;charset=UTF-8
Content-Length: 542
Transfer-Encoding: chunked
```

```
[ {
  "id" : "a488e498-7a48-4fa2-a276-5524e5b86af6",
  "name" : "endpoint-broker-server",
  "displayName" : "Endpoint Broker Server",
  "host" : "endpoint-server",
  "version" : "11.4.0.0"
}, {
  "id" : "571262a0-4ecf-4b78-92f2-01001e7e9945",
  "name" : "endpoint-server",
  "displayName" : "Endpoint Server",
  "host" : "endpoint-server",
  "version" : "11.4.0.0"
}, {
  "id" : "3c1e0db0-e01f-4b4e-96cf-af1cd6cd60c0",
  "name" : "respond-server",
  "displayName" : "Respond Server",
  "host" : "endpoint-server",
  "version" : "11.4.0.0"
} ]
```


Get List of Service IDs by Service Name

```
GET /rest/api/services?name=<service-name>
```

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/services?name=endpoint-broker-server' -i
-X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT' \
    -H 'Content-Type: application/json;charset=UTF-8'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 192
Date: Tue, 03 Dec 2019 14:05:58 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```

```
[ {
  "id" : "a488e498-7a48-4fa2-a276-5524e5b86af6",
  "name" : "endpoint-broker-server",
  "displayName" : "Endpoint Broker Server",
  "host" : "endpoint-server",
  "version" : "11.4.0.0"
} ]
```

Endpoint APIs

Endpoint Log Hybrid collects and manages endpoint data from hosts. Using the APIs, analyst can:

- View list of host names with agent IDs from one or more endpoint servers.
- Retrieve host data, such as drivers, processes, DLLs, files (executables), services, autoruns, security information, anomalies, system configurations, and scripts found on the host.
- Filter hosts on indexed values and sort columns.

Note: All endpoint APIs require a service ID to connect to the specific endpoint server.

Get Hosts

The Get Hosts API lists all hosts' information from a particular endpoint server. It provides a paged response with a standard paged response structure as mentioned in the 'Pagination' section.

The "items" field in paged response consists of individual host information.

Path	Type	Description
`items`	`Array`	An array containing the requested resources.
`pageNumber`	`Number`	The requested page number.
`pageSize`	`Number`	The requested number of items to return in a single page.
`totalPages`	`Number`	The total number of pages available.
`totalItems`	`Number`	The total number of items available.
`hasNext`	`Boolean`	Indicates if there is a page containing results after this page.
`hasPrevious`	`Boolean`	Indicates if there is a page containing results before this page.
`items[].agentId`	`String`	Agent ID of the host.
`items[].hostName`	`String`	Name of the host.
`items[].riskScore`	`Number`	Risk score of the host.
`items[].networkInterfaces`	`Array`	List of network interfaces with details, such as IP address and MAC address.
`items[].networkInterfaces[].name`	`String`	Name of the network interface.
`items[].networkInterfaces[].macAddress`	`String`	MAC Address of the network interface.
`items[].networkInterfaces[].ipv4`	`Array`	List of IPV4 in the network interface.
`items[].networkInterfaces[].ipv6`	`Array`	List of IPV6 in the network interface.
`items[].networkInterfaces[].networkIdv6`	`Array`	List of network IDV6 in the network interface.
`items[].networkInterfaces[].gateway`	`Array`	List of gateway in the network interface.

Path	Type	Description
items[].networkInterfaces[].dns	Array	List of DNS in the network interface.
items[].networkInterfaces[].promiscuous	String	Specifies if the network interface is in the promiscuous mode.
items[].lastSeenTime	String	Agent last seen time.

```
GET /rest/api/hosts?serviceId=<service-id>&&pageNumber=0&pageSize=100
```

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/hosts?serviceId=571262a0-4ecf-4b78-92f2-
01001e7e9945&pageNumber=0&pageSize=1' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 717
Date: Tue, 03 Dec 2019 14:05:59 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```

```
{
  "items" : [ {
    "agentId" : "B27DDED7-6FFA-A9D3-6577-3DDE367B2820",
    "hostName" : "HOSTNAME",
    "riskScore" : 0,
    "networkInterfaces" : [ {
      "name" : "Cisco AnyConnect Secure Mobility Client Virtual Miniport Adapter for
Windows x64 #2 #2",
      "macAddress" : "00:05:9A:3C:7A:00",
      "ipv4" : [ "10.2.2.2" ],
      "ipv6" : [ "2001:0db8:85a3:0000:0000:8a2e:0370:7334" ],
      "networkIdv6" : [ "10.1.1.1" ],
      "gateway" : [ "g1" ],
      "dns" : [ "10.4.4.4", "10.5.5.5" ],
      "promiscuous" : false
    } ],
    "lastSeenTime" : "2017-12-22T17:03:03.005Z"
  } ],
  "pageNumber" : 0,
  "pageSize" : 1,
  "totalPages" : 2,
  "totalItems" : 2,
  "hasNext" : true,
  "hasPrevious" : false
}
```


Get Hosts with Filter

The following fields are supported for filtering and sorting on Get Hosts API - 'agentId', 'hostName', 'riskScore', 'networkInterface.ipv4'

Filter and Sort are specified as a part of the request body.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/hosts?serviceId=571262a0-4ecf-4b78-92f2-
01001e7e9945&pageNumber=0&pageSize=1' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/json; charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT' \
    -d
'{"criteria":{"criteriaList":[{"criteriaList":[],"expressionList":[{"propertyName":"ag
entId","restrictionType":"EQUAL","propertyValues":[{"value":"B27DDED7-6FFA-A9D3-6577-
3DDE367B2820","relative":false}]}],"predicateType":"AND"}],"expressionList":[],"predic
ateType":"AND"},"sort":{"keys":["riskScore"],"descending":true}}'
```

HTTP request

```
GET /rest/api/hosts?serviceId=571262a0-4ecf-4b78-92f2-
01001e7e9945&pageNumber=0&pageSize=1 HTTP/1.1
Accept: application/json;charset=UTF-8
Host: api.netwitness.local
Content-Type: application/json; charset=UTF-8
NetWitness-Token: eyJ...AT
Content-Length: 320

{"criteria":{"criteriaList":[{"criteriaList":[],"expressionList":[{"propertyName":"age
ntId","restrictionType":"EQUAL","propertyValues":[{"value":"B27DDED7-6FFA-A9D3-6577-
3DDE367B2820","relative":false}]}],"predicateType":"AND"}],"expressionList":[],"predic
ateType":"AND"},"sort":{"keys":["riskScore"],"descending":true}}
```

Get List of Snapshots for Host

This API provides a list of snapshots, which are IDs to fetch the snapshot details of the host.

```
GET /rest/api/host/<Host-Agent-Id>/snapshots?serviceId=<service-id>
```

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/host/B27DDED7-6FFA-A9D3-6577-
3DDE367B2820/snapshots?serviceId=571262a0-4ecf-4b78-92f2-01001e7e9945' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 30
Date: Tue, 03 Dec 2019 14:05:59 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```

```
[ "2017-12-22T14:34:05.985Z" ]
```

Get Snapshot details for the host

This API provides snapshot details of the given host for the provided snapshot time.

Response Fields

Path	Type	Description
[]	Array	Array of scan snapshot for the agent.
[].machineOsType	String	Type of operating system (Windows, Mac, Linux).
[].hostName	String	Name of the host.
[].agentId	String	Agent ID of the host.
[].agentVersion	String	Version of the agent.
[].scanStartTime	String	Start time of the scan snapshot.
[].directory	String	Directory of the file.
[].fileName	String	Name of the file.
[].owner.username	String	User name of the owner of the file.
[].owner.groupname	String	Group name of the owner of the file.
[].owner.uid	String	UID of the user name.
[].owner.gid	String	GID of the user name.
[].timeCreated	String	Time when file was created.
[].timeModified	String	Time when file was modified.
[].timeAccessed	String	Time when file was last accessed.
[].attributes	Array	List of file attributes.
[].accessMode	Number	Access mode of the file.
[].sameDirectoryFileCounts.nonExe	Number	Number of non-exe files in the same directory of the file.
[].sameDirectoryFileCounts.exe	Number	Number of exe files in the same directory of the file.
[].sameDirectoryFileCounts.subFolder	Number	Number of sub-folders in the same directory of the file.
[].sameDirectoryFileCounts.exeSameCompany	Number	Number of executables with the same company name in the same directory of the file.
[].sameDirectoryFileCounts.hiddenFiles	Number	Count of hidden files in the same directory of the file.
[].fileContext	Array	List of file context.
[].directoryContext	Array	List of directory context.
[].autorunContext	Array	List of autorun context.
[].networkContext	Array	List of network context.
[].kernelModeContext	Array	List of kernel mode context.
[].userModeContext	Array	List of user mode context.
[].processContext	Array	List of process context.
[].rpm.packageName	String	RPM package name to which the file belongs.

Path	Type	Description
[].rpm.category	String	Category to which the rpm package belongs.
[].windows.processes[].eprocess	String	Identifier of the process.
[].windows.processes[].sessionId	Number	Session ID of the process.
[].windows.processes[].parentPath	String	Directory of the parent process.
[].windows.processes[].imageSize	Number	Size of the process image.
[].windows.processes[].integrityLevel	Number	Integrity level of the process.
[].windows.processes[].context	Array	List of process context.
[].windows.processes[].pid	Number	ID of the process.
[].windows.processes[].parentPid	Number	ID of the parent process.
[].windows.processes[].imageBase	Number	Base address of the process.
[].windows.processes[].createUtcTime	String	Creation time of the process.
[].windows.processes[].owner	String	Name of the user.
[].windows.processes[].launchArguments	String	Launch arguments of the process.
[].windows.processes[].threadCount	Number	Number of threads running in the process.
[].windows.dlls[].createTime	String	Creation time of the process.
[].windows.dlls[].eprocess	String	Identity of the process.
[].windows.dlls[].imageSize	Number	Size of the DLL image in memory.
[].windows.threads[].processName	String	Name of the process.
[].windows.threads[].processTime	String	Creation time of the process.
[].windows.threads[].eprocess	String	Identifier of the process.
[].windows.threads[].pid	Number	PID of the process.
[].windows.threads[].ethread	String	Identifier of the thread.
[].windows.threads[].tid	Number	ID of the thread.
[].windows.threads[].teb	String	Address of thread environment block.
[].windows.threads[].startAddress	String	Start address of the thread in memory.
[].windows.threads[].state	Array	Thread state.
[].windows.threads[].behaviorKey	String	Floating behavior resolution of the thread.
[].windows.drivers[].windows.imageBase	Number	Base address of the driver image.
[].windows.drivers[].windows.imageSize	Number	Size of the driver image.

Path	Type	Description
[].windows.services[].windows.serviceName	String	Service name as identified by the system.
[].windows.services[].displayName	String	Display name for the service.
[].windows.services[].description	String	Description of the service.
[].windows.services[].account	String	Name of the user the service executes as.
[].windows.services[].launchArguments	String	Launch arguments of the service.
[].windows.services[].windows.serviceMain	String	Service's main.
[].windows.services[].hostingPid	Number	Service's hosting process ID.
[].windows.services[].state	String	Current state of the service.
[].windows.services[].win32ErrorCode	Number	Last Windows 32 error code from registry.
[].windows.services[].context	Array	List of service context.
[].windows.tasks[].name	String	Name of the task.
[].windows.tasks[].executeUser	String	Name of the user the task executes as.
[].windows.tasks[].creatorUser	String	Name of the user who created the task.
[].windows.tasks[].launchArguments	String	Launch arguments of the task.
[].windows.tasks[].status	Array	Status of the task.
[].windows.tasks[].lastRunTime	String	Time when the task was last run.
[].windows.tasks[].nextRunTime	String	Next scheduled time of the task.
[].windows.tasks[].triggerString	String	Textual trigger string of the task.
[].windows.autoruns[].type	String	Type of the autorun.
[].windows.autoruns[].registryPath	String	Registry path where autorun is located.
[].windows.autoruns[].launchArguments	String	Launch argument of the autorun.
[].windows.imageHooks[].process.pid	String	PID of the process in which hook was detected.
[].windows.imageHooks[].process.fileName	String	Filename of the process in which hook was detected.
[].windows.imageHooks[].process.createUtcTime	String	Creation time of the process in which hook was detected.
[].windows.imageHooks[].hookLocation.section	String	Name of the image section that was modified by the hook.
[].windows.imageHooks[].hookLocation.sectionBase	String	Base of the image section that was modified by the hook.

Path	Type	Description
[].windows.imageHooks[].hookLocation.symbol	String	Closest symbol name to the memory location that was modified.
[].windows.imageHooks[].hookLocation.symbolOffset	Number	Closest symbol +/- offset to the hook location when relevant.
[].windows.imageHooks[].inlinePatch.originalBytes	String	Hexadecimal bytes which were replaced.
[].windows.imageHooks[].inlinePatch.originalAsm	Array	Array of decoded ASM instructions that were replaced.
[].windows.imageHooks[].inlinePatch.currentBytes	String	Hexadecimal bytes which have overwritten the original code.
[].windows.imageHooks[].inlinePatch.currentAsm	Array	Array of decoded ASM instructions that have overwritten the original code.
[].windows.kernelHooks[].hookLocation.objectName	String	Name of the object that was hooked in kernel.
[].windows.kernelHooks[].hookLocation.objectFunction	String	Name of the object function that was hooked in kernel.
[].mac.processes[].priority	Number	Priority of the process.
[].mac.processes[].flags	Number	Process flags.
[].mac.processes[].nice	Number	Nice value of process.
[].mac.processes[].openFilesCount	Number	Number of open files by process at scan time.
[].mac.processes[].context	Array	Process context.
[].mac.processes[].pid	Number	ID of the process.
[].mac.processes[].parentPid	Number	ID of the parent process.
[].mac.processes[].imageBase	Number	Base address of the process.
[].mac.processes[].createUtcTime	String	Creation time of the process.
[].mac.processes[].owner	String	Name of the user.
[].mac.processes[].launchArguments	String	Launch arguments of the process.
[].mac.processes[].threadCount	Number	Number of threads running in the process.
[].mac.dylibs[].pid	Number	Process ID in dylib which is loaded.
[].mac.dylibs[].processName	String	Name of the process.
[].mac.dylibs[].imageBase	String	Base address of image in the process.
[].mac.drivers[].preLinked	Boolean	True if Kext bundle is prelinked.
[].mac.drivers[].numberOfReferences.	Number	Number of references.
[].mac.drivers[].dependencies	Array	List of kexts(name) the driver is linked against.
[].mac.drivers[].imageBase	String	Base address of the driver image.
[].mac.drivers[].imageSize	String	Size of the driver image.

Path	Type	Description
[].mac.daemons[].name	String	Label of the daemon.
[].mac.daemons[].sessionName	String	Name of the session in which daemon runs.
[].mac.daemons[].user	String	Name of the user under which the daemon runs.
[].mac.daemons[].pid	Number	ID of the process.
[].mac.daemons[].onDemand	Boolean	True if daemon is configured to run on demand.
[].mac.daemons[].lastExitCode	Number	Last exit code.
[].mac.daemons[].timeout	Number	Time out value.
[].mac.daemons[].daemons.launchArguments	String	Launch argument of the daemon.
[].mac.daemons[].daemons.configFile	String	Full path of the configuration file used to configure this daemon.
[].mac.tasks[].name	String	Name of the task.
[].mac.tasks[].cronJob	Boolean	True if the task is cron job, else launchd.
[].mac.tasks[].launchArguments	String	Launch argument of the task.
[].mac.tasks[].user	String	Name of the user under which this task will run.
[].mac.tasks[].triggerString	String	Trigger string of the task.
[].mac.tasks[].configFile	String	Full path of the configuration file used to configure this task.
[].mac.autoruns[].type	String	Type of autorun.
[].mac.autoruns[].user	String	Name of the user under which the autorun is run.
[].mac.autoruns[].name	String	Label of the autorun.
[].mac.autoruns[].detail	String	Details of the autorun.
[].linux.processes[].priority	Number	Priority of the process.
[].linux.processes[].uid	Number	UID of the user.
[].linux.processes[].environment	String	Environment variables.
[].linux.processes[].nice	Number	Nice value of the process.
[].linux.processes[].securityContext	String	Security context.
[].linux.processes[].pid	Number	ID of the process.
[].linux.processes[].parentPid	Number	ID of the parent process.
[].linux.processes[].imageBase	Number	Base address of the process.
[].linux.processes[].createUtcTime	String	Time of creation of the process.
[].linux.processes[].owner	String	Name of the user.
[].linux.processes[].launchArguments	String	Launch arguments of the process.
[].linux.processes[].threadCount	Number	Number of threads running in the process.

Path	Type	Description
[].linux.loadedLibraries[].pid	String	Process ID in which library is loaded.
[].linux.loadedLibraries[].processName	String	Name of the process.
[].linux.loadedLibraries[].imageBase	String	Base address of image in the process.
[].linux.drivers[].numberOfInstances	Number	Number of instances loaded in memory.
[].linux.drivers[].loadState	String	Load state of the driver.
[].linux.drivers[].dependencies	Array	Dependent driver names.
[].linux.drivers[].author	String	Name of the author of driver.
[].linux.drivers[].description	String	Description of the driver.
[].linux.drivers[].sourceVersion	String	Source version of the driver.
[].linux.drivers[].versionMagic	String	Version magic of the driver.
[].linux.initds[].initdHashSha256	String	Hash of the init-d script file.
[].linux.initds[].initdPaths	String	Path of the init-d script file.
[].linux.initds[].pid	Number	ID of the process.
[].linux.initds[].description	String	Description of the init-d.
[].linux.initds[].status	String	Status of the init-d.
[].linux.initds[].runLevels	Array	List of run levels in which the init-d is enabled.
[].linux.systemds[].systemdHashSha256	String	Hash value of the systemd script file.
[].linux.systemds[].systemdPaths	String	Path value of the systemd script file.
[].linux.systemds[].name	String	Name of the systemd.
[].linux.systemds[].description	String	Description of the systemd.
[].linux.systemds[].state	String	State of the systemd.
[].linux.systemds[].launchArguments	String	Launch argument of the systemd.
[].linux.systemds[].pid	Number	ID of the process.
[].linux.systemds[].triggeredBy	Array	Triggered by list of the systemd.
[].linux.systemds[].triggerStrings	Array	Trigger strings of the systemd.
[].linux.autoruns[].type	String	Type of autorun.
[].linux.autoruns[].label	String	Label of the autorun.
[].linux.autoruns[].comments	String	Comments of the autorun.
[].linux.crons[].user	String	User account under which cron job was created.
[].linux.crons[].triggerString	String	Trigger string that would launch the cron job.
[].linux.crons[].launchArguments	String	Launch arguments of the cron job.
firstFileName	String	First name of the file sent by the agent.

Path	Type	Description
reputationStatus	String	Reputation status of the file.
globalRiskScore	String	Global risk score.
firstSeenTime	String	Time when the file was first seen by the Endpoint Server.
machineOsType	String	Type of operating system (Windows, Mac, Linux).
signature	Object	Signatory information of the file.
signature.timeStamp	String	Timestamp of the signature.
signature.thumbprint	String	Thumbprint of the certificate.
signature.context	Array	Context information of the certificate.
signature.signer	String	Signer information of the certificate.
size	String	Size of the file.
checksumMd5	String	MD5 of the file.
checksumSha1	String	SHA1 of the file.
checksumSha256	String	SHA256 of the file.
pe	Object	PE information of the file. This is applicable for Windows files.
pe.timeStamp	String	Timestamp of the PE File.
pe.imageSize	String	Image size of the PE file.
pe.numberOfExportedFunctions	String	Number of exported function in the PE file.
pe.numberOfNamesExported	String	Number of names exported in the PE file.
pe.numberOfExecuteWriteSections	String	Number of execute write sections in the PE file.
pe.context	Array	Context information of the PE file.
pe.resources	Object	Resources of the PE file.
pe.resources.originalFileName	String	Original filename as per PE information.
pe.resources.company	String	Company name as per PE information.
pe.resources.description	String	Description of the file as per PE information.
pe.resources.version	String	Version of the file as per PE information.
pe.sectionNames	Array	List of section names in the PE file.
pe.importedLibraries	Array	List of imported libraries in the PE file.
elf	Object	ELF information of the file. This is applicable for Linux files.
elf.classType	String	Class type of the ELF file.
elf.data	String	Data of ELF file.
elf.entryPoint	String	Entry point for the ELF file.
elf.context	Array	Context information of ELF file.
elf.type	String	Type of ELF file.

Path	Type	Description
elf.sectionNames	Array	List of section names in ELF file.
elf.importedLibraries	Array	List of imported libraries in ELF file.
macho	Object	Macho information of the file. This is applicable for Mac files.
macho.uuid	String	UUID of the Macho file.
macho.identifier	String	Identifier of the Macho file.
macho.minOsxVersion	String	Minimum OSx version for the Macho file.
macho.context	Array	Context information of the Macho file.
macho.flags	String	Flags of Macho file.
macho.numberOfLoadCommands	String	Number of load commands for the Macho file.
macho.version	String	Version of the Macho file.
macho.sectionNames	Array	Section names in the Macho file.
macho.importedLibraries	Array	Imported libraries list in the Macho file.
entropy	String	Entropy of the file.
format	String	Format of the file.
fileStatus	String	Status of the file as assigned by the analyst. (Whitelist, Blacklist, Neutral, and Graylist).
remediationAction	String	Remediation action as assigned by the analyst. For example, Blocked.
[].localRiskScore	Number	File's score based on alerts triggered in the given agent.

```
GET /rest/api/host/<Host-Agent-Id>/snapshots/2019-06-
17T04:24:14.608Z?serviceId=<service-id>
```

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/host/B27DDED7-6FFA-A9D3-6577-
3DDE367B2820/snapshots/2017-12-22T14%3A34%3A05.985Z?serviceId=67a84b72-3d9a-4377-9096-
7e6af9f13306' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Date: Mon, 22 Jul 2019 08:34:38 GMT
Content-Length: 6710
Content-Disposition: inline;filename=f.txt
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
```


```
[ {
  "machineOsType" : "windows",
  "hostName" : "HOSTNAME",
  "agentId" : "B27DDED7-6FFA-A9D3-6577-3DDE367B2820",
  "agentVersion" : "11.1.0.0",
  "scanStartTime" : "2017-12-22T14:34:05.985Z",
  "directory" : "F\\SonarQube\\DIRECTCP\\PolicyDefinitions",
  "fileName" : "shtctky.bat",
  "owner" : {
    "username" : "Sinha, Vidya",
    "groupname" : "CORP",
    "uid" : 9,
    "gid" : 1
  },
  "timeCreated" : "2017-12-22T10:00:15.000Z",
  "timeModified" : "2017-12-22T06:00:15.000Z",
  "timeAccessed" : "2017-12-22T11:00:15.000Z",
  "attributes" : null,
  "accessMode" : 15,
  "sameDirectoryFileCounts" : {
    "nonExe" : 1,
    "exe" : 4,
    "subFolder" : 0,
    "exeSameCompany" : 3,
    "hiddenFiles" : 0
  },
  "fileContext" : [ "ads", "accessDenied", "hiddenDifferentialView", "encrypted" ],
  "directoryContext" : [ "desktop" ],
  "autorunContext" : [ "winlogon" ],
  "networkContext" : [ "accessNetwork", "listen" ],
  "kernelModeContext" : [ "loaded", "hookEat", "hookSsdt", "createThreadNotification",
"imageMismatch", "remoteThreadCreator" ],
  "userModeContext" : [ "loaded", "hookEat", "mapped", "image", "threadFloating",
"remoteMemoryAllocator", "setWindowsHook" ],
  "processContext" : [ "accessDenied", "dyldInserted", "ldPreloaded" ],
  "rpm" : null,
  "windows" : {
    "processes" : [ {
      "pid" : 46270,
      "parentPid" : 4,
      "imageBase" : 55076,
      "createUtcTime" : null,
```

```
      "owner" : "Sinha, Vidya",
      "launchArguments" : "/B /nologo %systemroot%\\system32\\calluxxprovider.vbs
$(Arg0) $(Arg1) $(Arg2)",
      "threadCount" : 0,
      "eprocess" : "0x8F76",
      "sessionId" : 1,
      "parentPath" : null,
      "imageSize" : 0,
      "integrityLevel" : 0,
      "context" : [ "UsingNamedPipe" ]
    } ],
    "dlls" : [ {
      "pid" : 46270,
      "processName" : null,
      "imageBase" : 55590,
      "createTime" : "2017-12-22T16:00:15.000+0000",
      "eprocess" : "0x3DFE",
      "imageSize" : 55459
    } ],
    "threads" : [ ],
    "drivers" : [ ],
    "services" : [ {
      "serviceName" : "wlanext",
      "displayName" : "wlanext",
      "description" : "wlanext description",
      "account" : "Sinha, Vidya",
      "launchArguments" : "-id 1",
      "serviceMain" : "ServiceMain",
      "hostingPid" : 0,
      "state" : null,
      "win32ErrorCode" : 26218,
      "context" : null
    } ],
    "tasks" : [ {
      "name" : "Shaktiman",
      "executeUser" : "Sinha, Vidya",
      "creatorUser" : "Sinha, Vidya",
      "launchArguments" : "-Embedding",
      "status" : null,
      "lastRunTime" : null,
      "nextRunTime" : null,
      "triggerString" : null
    } ],
    "autoruns" : [ ],
    "imageHooks" : [ ],
    "kernelHooks" : [ ]
  },
  "mac" : null,
  "linux" : null,
  "fileProperties" : null,
  "localRiskScore" : 0
```

```
} ]
```

Get Files

The Get Files API lists all related information of files from a specific Endpoint Server. These information are specific to the unique file and does not include any host information.

It provides a paged response with a standard paged response structure as mentioned in the 'Pagination' section.

The "items" field in paged response consists of individual file information.

Path	Type	Description
items	Array	An array containing the requested resources.
pageNumber	Number	The requested page number.
pageSize	Number	The requested number of items to return in a single page.
totalPages	Number	The total number of pages available.
totalItems	Number	The total number of items available.
hasNext	Boolean	Indicates if there is a page containing results after this page.
hasPrevious	Boolean	Indicates if there is a page containing results before this page.
items[].firstFileName	String	First name of the file sent by the agent.
items[].reputationStatus	String	Reputation status of the file.
items[].globalRiskScore	String	Global risk score.
items[].firstSeenTime	String	Time when the file was first seen by the Endpoint Server.
items[].machineOsType	String	Type of operating system (Windows, Mac, Linux).
items[].signature	Object	Signatory information of the file.
items[].signature.timeStamp	String	Timestamp of the signature.
items[].signature.thumbprint	String	Thumbprint of the certificate.
items[].signature.context	Array	Context information of the certificate.
items[].signature.signer	String	Signer information of the certificate.
items[].size	String	Size of the file.
items[].checksumMd5	String	MD5 of the file.
items[].checksumSha1	String	SHA1 of the file.
items[].checksumSha256	String	SHA256 of the file.
items[].pe	Object	PE information of the file. This is applicable for Windows files.

Path	Type	Description
items[].pe.timeStamp	String	Timestamp of the PE File.
items[].pe.imageSize	String	Image size of the PE file.
items[].pe.numberOfExportedFunctions	String	Number of exported function in the PE file.
items[].pe.numberOfNamesExported	String	Number of names exported in the PE file.
items[].pe.numberOfExecuteWriteSections	String	Number of execute write sections in the PE file.
items[].pe.context	Array	Context information of the PE file.
items[].pe.resources	Object	Resources of the PE file.
items[].pe.resources.originalFileName	String	Original filename as per PE information.
items[].pe.resources.company	String	Company name as per PE information.
items[].pe.resources.description	String	Description of the file as per PE information.
items[].pe.resources.version	String	Version of the file as per PE information.
items[].pe.sectionNames	Array	List of section names in the PE file.
items[].pe.importedLibraries	Array	List of imported libraries in the PE file.
items[].elf	Object	ELF information of the file. This is applicable for Linux files.
items[].elf.classType	String	Class type of the ELF file.
items[].elf.data	String	Data of ELF file.
items[].elf.entryPoint	String	Entry point for the ELF file.
items[].elf.context	Array	Context information of ELF file.
items[].elf.type	String	Type of ELF file.
items[].elf.sectionNames	Array	List of section names in ELF file.
items[].elf.importedLibraries	Array	List of imported libraries in ELF file.
items[].macho	Object	Macho information of the file. This is applicable for Mac files.
items[].macho.uuid	String	UUID of the Macho file.
items[].macho.identifier	String	Identifier of the Macho file.
items[].macho.minOsxVersion	String	Minimum OSx version for the Macho file.
items[].macho.context	Array	Context information of the Macho file.
items[].macho.flags	String	Flags of Macho file.
items[].macho.numberOfLoadCommands	String	Number of load commands for the Macho file.
items[].macho.version	String	Version of the Macho file.
items[].macho.sectionNames	Array	Section names in the Macho file.
items[].macho.importedLibraries	Array	Imported libraries list in the Macho file.
items[].entropy	String	Entropy of the file.
items[].format	String	Format of the file.

Path	Type	Description
items[].fileStatus	String	Status of the file as assigned by the analyst. (Whitelist, Blacklist, Neutral, and Graylist).
items[].remediationAction	String	Remediation action as assigned by the analyst. For example, Blocked.

Note: The following is a sample response with all fields populated. However, the response for pe, macho, and elf is generated based the operating system type. The fields without values will display as null.

```
GET /rest/api/hosts?serviceId=<service-id>&&pageNumber=0&pageSize=100
```

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/files?serviceId=571262a0-4ecf-4b78-92f2-
01001e7e9945&pageNumber=0&pageSize=1' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 2054
Content-Type: application/json;charset=UTF-8
Date: Tue, 03 Dec 2019 14:06:01 GMT
Transfer-Encoding: chunked
```


```
{
  "items" : [ {
    "firstFileName" : "cmd.exe",
    "reputationStatus" : "Known",
    "globalRiskScore" : 0,
    "firstSeenTime" : "2019-04-28T05:40:20.000Z",
    "machineOsType" : "windows",
    "signature" : {
      "timeStamp" : "2019-04-28T05:40:20.000Z",
      "thumbprint" : "ae9c1ae54763822eec42474983d8b635116c8452",
      "context" : [ "microsoft", "signed", "valid", "catalog" ],
      "signer" : "Microsoft Windows"
    },
    "size" : 278528,
    "checksumMd5" : "0d088f5bcfa8f086fba163647cd80cab",
    "checksumSha1" : "08cc2e8dca652bdda1acca9c446560d4bc1bcdf9",
    "checksumSha256" :
"9023f8aaeda4a1da45ac477a81b5bbe4128e413f19a0abfa3715465ad66ed5cd",
```

```
    "pe" : {
      "timeStamp" : "2019-04-28T05:40:20.000Z",
      "imageSize" : 413696,
      "numberOfExportedFunctions" : 0,
      "numberOfNamesExported" : 0,
      "numberOfExecuteWriteSections" : 0,
      "context" : [ "file.exe" ],
      "resources" : {
        "originalFileName" : "Cmd.Exe",
        "company" : "Microsoft Corporation",
        "description" : "Windows Command Processor",
        "version" : null
      },
      "sectionNames" : [ ".text" ],
      "importedLibraries" : [ "msvcrt.dll" ]
    },
    "elf" : {
      "classType" : 0,
      "data" : 0,
      "entryPoint" : 0,
      "context" : [ "file.arch64", "file.lkm" ],
      "type" : 1,
      "sectionNames" : [ ".note.gnu.build-id", ".text" ],
      "importedLibraries" : null
    },
    "macho" : {
      "uuid" : "277163DE-842E-390D-A7FF-EC4CF2D211A4",
      "identifier" : "com.apple.geod",
      "minOsxVersion" : "10.11.0",
      "context" : [ "file.arch64" ],
      "flags" : 2097285,
      "numberOfLoadCommands" : 22,
      "version" : "1151.49.1",
      "sectionNames" : [ "__PAGEZERO" ],
      "importedLibraries" : [ "Foundation" ]
    },
    "entropy" : 6.17224886172381,
    "format" : "pe",
    "fileStatus" : "Blacklist",
    "remediationAction" : "Unblock"
  } ],
  "pageNumber" : 0,
  "pageSize" : 1,
  "totalPages" : 2,
  "totalItems" : 2,
  "hasNext" : true,
  "hasPrevious" : false
}
```

Request Scan

The Request Scan API starts a scan for the host with the specified agent ID.

```
POST /rest/api/host/{agentId}/scan?serviceId=<service-id>&scanType=<scanType>
```

Path Parameters

Parameter	Description
agentId	Unique identifier of the host.

Request Parameters

Parameter	Description
serviceId	Service ID of the endpoint server to be connected.
scanType	Type of scan command.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/host/B27DDED7-6FFA-A9D3-6577-
3DDE367B2820/scan?serviceId=571262a0-4ecf-4b78-92f2-01001e7e9945&scanType=QUICK_SCAN'
-i -X POST \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'Content-Type: application/x-www-form-urlencoded; charset=ISO-8859-1' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2019 14:06:01 GMT
```

```
```

Request Stop Scan

The Stop Scan API stops a scan for the host with the specified agent ID.

```
DELETE /rest/api/host/{agentId}/scan?serviceId=<service-id>&scanType=<scanType>
```

Path Parameters

Parameter	Description
agentId	Unique identifier of the host.

Request Parameters

Parameter	Description
serviceId	Service ID of the endpoint server to be connected.
scanType	Type of scan command.

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/host/B27DDED7-6FFA-A9D3-6577-
3DDE367B2820/scan?serviceId=571262a0-4ecf-4b78-92f2-01001e7e9945&scanType=CANCEL_SCAN'
-i -X DELETE \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Date: Tue, 03 Dec 2019 14:06:01 GMT
```

```
```

Get Alerts for a host

The Get alerts for a host API gets all alerts triggered for a given host. Alerts are categorized as 'Critical', 'High', 'Medium' and 'Low'. The response provides category level count of alerts triggered along with list of alerts.

Path	Type	Description
id	String	ID of the entity for which score needs to be queried. Agent ID in case of host and checksum in case of files.
distinctAlertCount	Object	Count of distinct Alert/category for the entity.
distinctAlertCount.critical	String	Number of critical alerts.
distinctAlertCount.high	String	Number of high alerts.
distinctAlertCount.medium	String	Number of medium alerts.
distinctAlertCount.low	String	Number of low alerts.

Path	Type	Description
categorizedAlerts	String	Count of alert and events for a file/host, categorized by severity.

```
GET /rest/api/host/{agentId}/alerts?serviceId=<service-id>
```

Sample Request

```
$ curl 'https://api.netwitness.local/rest/api/host/B27DDED7-6FFA-A9D3-6577-
3DDE367B2820/alerts?serviceId=571262a0-4ecf-4b78-92f2-01001e7e9945' -i -X GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 831
Content-Type: application/json;charset=UTF-8
Date: Tue, 03 Dec 2019 14:06:01 GMT
Transfer-Encoding: chunked
```

```
{
  "id" : "B27DDED7-6FFA-A9D3-6577-3DDE367B2820",
  "distinctAlertCount" : {
    "critical" : 0,
    "high" : 4,
    "medium" : 2,
    "low" : 0
  },
  "categorizedAlerts" : {
    "All" : {
      "Possibly Renamed net.exe Detected" : {
        "alertCount" : 1,
        "eventCount" : 1
      },
      "Powershell Injects Remote Process" : {
        "alertCount" : 3,
        "eventCount" : 3
      },
      "Unexpected taskhostw.exe Parent" : {
        "alertCount" : 1,
        "eventCount" : 1
      },
      "Unexpected runtimebroker.exe Parent" : {
        "alertCount" : 1,
        "eventCount" : 1
      },
      "Performs Scripted File Transfer" : {
        "alertCount" : 1,
        "eventCount" : 1
      },
      "Unexpected Svchost.Exe Parent" : {
        "alertCount" : 1,
        "eventCount" : 1
      }
    }
  }
}
```


Get Alerts for a file

The Get alerts for a file API gets all alerts triggered for a given file. Alerts are categorized as 'Critical', 'High', 'Medium' and 'Low'. The response provides category level count of alerts triggered along with list of alerts.

Path	Type	Description
id	String	ID of the entity for which score needs to be queried. Agent ID in case of host and checksum in case of files.

Path	Type	Description
distinctAlertCount	Object	Count of distinct Alert/category for the entity.
distinctAlertCount.critical	String	Number of critical alerts.
distinctAlertCount.high	String	Number of high alerts.
distinctAlertCount.medium	String	Number of medium alerts.
distinctAlertCount.low	String	Number of low alerts.
categorizedAlerts	String	Count of alert and events for a file/host, categorized by severity.

```
GET /rest/api/file/{checksum}/alerts?serviceId=<service-id>
```

Sample Request

```
$ curl
'https://api.netwitness.local/rest/api/file/d1c79a36593f0d5f7d07502b963d97acc851dc0291
f4556ce8f110a58a48fda4/alerts?serviceId=571262a0-4ecf-4b78-92f2-01001e7e9945' -i -X
GET \
    -H 'Accept: application/json;charset=UTF-8' \
    -H 'NetWitness-Token: eyJ...AT'
```

Sample Response

```
HTTP/1.1 200 OK
Content-Length: 545
Content-Type: application/json;charset=UTF-8
Date: Tue, 03 Dec 2019 14:06:01 GMT
Transfer-Encoding: chunked
```

```
{
  "id" : "d1c79a36593f0d5f7d07502b963d97acc851dc0291f4556ce8f110a58a48fda4",
  "distinctAlertCount" : {
    "critical" : 0,
    "high" : 2,
    "medium" : 1,
    "low" : 0
  },
  "categorizedAlerts" : {
    "All" : {
      "Possibly Renamed net.exe Detected" : {
        "alertCount" : 1,
        "eventCount" : 1
      },
      "Powershell Injects Remote Process" : {
        "alertCount" : 3,
        "eventCount" : 3
      },
      "Performs Scripted File Transfer" : {
        "alertCount" : 1,
        "eventCount" : 1
      }
    }
  }
}
```