

**RSA NetWitness® Platform**

Homenet Lab

Custom Content Taxonomy

**Table of Contents**

[Description 2](#_Toc51920285)

[Purpose of This Document 2](#_Toc51920286)

[Creating Custom Metakeys - Things to Know 2](#_Toc51920287)

[Name Length 2](#_Toc51920288)

[Allowed Characters 2](#_Toc51920289)

[Name Construction 2](#_Toc51920290)

[Value Format 2](#_Toc51920291)

[Multivalued Field 2](#_Toc51920292)

[RSA NetWitness Unified Data Model (UDM) References 2](#_Toc51920293)

[Critical Asset 3](#_Toc51920294)

[Metakey Description 3](#_Toc51920295)

[Metakey Values 3](#_Toc51920296)

[hnl.asset.crit 3](#_Toc51920297)

[hnl.asset.cat 4](#_Toc51920298)

[hnl.asset.role 4](#_Toc51920299)

[hnl.asset.host 5](#_Toc51920300)

[hnl.asset.date 5](#_Toc51920301)

[hnl.asset.loc 5](#_Toc51920302)

[Custom Intelligence 6](#_Toc51920303)

[Metakey Description 6](#_Toc51920304)

[Metakey Values 6](#_Toc51920305)

[hnl.intel 6](#_Toc51920306)

[hnl.intel.cat 7](#_Toc51920307)

[hnl.intel.date 7](#_Toc51920308)

[hnl.intel.desc 8](#_Toc51920309)

[hnl.intel.src 8](#_Toc51920310)

# Description

## Purpose of This Document

This document is to provide an agreed upon standard to which all custom content will adhere to for a consistent investigation and content development experience. These metakeys and values can be used in Decoder application rules, Feeds, Reporting Engine and Event Stream Analysis (ESA) Rules.

## Creating Custom Metakeys - Things to Know

### Name Length

You are limited to 16 characters (including the "." dot delimiter) - use lowercase only for the name and values.

### Allowed Characters

Only alpha numeric values are allowed, except for the "." delimiter.

### Name Construction

Metakey names should follow the Unified Data Model (UDM) "3 Logical Parts" and should not conflict with any current RSA keys.



### Value Format

You must decide what your metakey value it will store define it in the appropriate custom index files. The most commonly used formats are "Text" and "Integer". There are other formats, but these are the most common.

### Multivalued Field

You will have to properly identify whether your metakey may contain multiple values in the same session. This is done in the index file with a singleton="true" in the concentrator custom index files. The reason for this is to have the ESA properly identify the field as a multivalued field (array) or a single valued field automatically.

## RSA NetWitness Unified Data Model (UDM) References

* [Standard RSA Metakeys](https://community.rsa.com/community/products/netwitness/rsa-content/udm#meta)
* [Discontinued Metakeys](https://community.rsa.com/community/products/netwitness/rsa-content/udm#deprecated)
* [Meta Entities](https://community.rsa.com/community/products/netwitness/rsa-content/udm#entities)
* [Creating Custom Metakeys](https://community.rsa.com/community/products/netwitness/rsa-content/udm#custom)

# Critical Asset

## Metakey Description

The table below shows the metakey names along with their data types and if they can or will contain multiple values which would define them as an array in the ESA alerting platform.

|  |  |  |  |
| --- | --- | --- | --- |
| **Metakey Name** | **Multivalued** | **Metakey Type** | **Description** |
| hnl.asset.crit | No | UInt8 | A Numerical criticality classification of asset. |
| hnl.asset.cat | Yes | Text | Category of system, this is the basic category the system will fall under. |
| hnl.asset.role | Yes | Text | What role the system performs, more context on what this system does or contains. |
| hnl.asset.host | No | Text | Short hostname of system, to provide easier system identification |
| hnl.asset.date | No | UInt32 | Date system was first added to NetWitness, used to determine age of asset information and can be used with math operators <>= in reports and apprules. |
| hnl.asset.loc | No | Text | Data center location of asset |

## Metakey Values

The table below shows the values to be used in content development for these asset metakeys. Note the spelling and case should always remain consistent to prevent overlap, inconsistencies and gaps in alerting and reporting content.

### hnl.asset.crit

This metakey identifies the criticality of the system. The table below lists the possible values and describes the values to use in this metakey. Note the values are always lowercase.

|  |  |
| --- | --- |
| **Value** | **Description** |
| 1 | Extremely Critical |
| 2 | Highly Critical |
| 3 | Moderately Critical |
| 4 | Low |

### hnl.asset.cat

This metakey identifies the category of the system. The table below lists the possible values and describes the values to use in this metakey. Note the values are always lowercase.

|  |  |
| --- | --- |
| **Value** | **Description** |
| authentication | Systems that provide authentication services, like domain controllers, LDAP servers, RADIUS, SecurID, TACACS, etc. |
| firewall | Systems that provide firewall services. |
| scanner | Systems that perform scanning activities like a port/vulnerability scanner or pen test |
| database | Systems that host database services. |
| pii | Systems that contain sensitive PII data |
| dev | Development Environment |
| qa | Quality Assurance systems |
| ua | User Acceptance systems |
| network | Critical Network Infrastructure |
| endpoint | Endpoint protection software |

### hnl.asset.role

This metakey identifies the role of the system. The table below lists the possible values grouped by category along with the descriptions of the values to use in this metakey. Note the values are always lowercase.

|  |  |  |
| --- | --- | --- |
| **Category** | **Description** | **Value** |
| authentication | Microsoft Active Directory server | domain controller |
| authentication | LDAP server | ldap server |
| authentication | RADIUS server | radius server |
| authentication | SecurID Server | securid server |
| pii | Customer PII Data | customer |
| pii | Employee PII Data | employee |
| firewall | Dmz firewall | dmz |
| firewall | Perimeter firewall | perimeter |
| firewall | Secure hosting firewall | secure hosting |
| scanner | Vulnerability Scanner | vulnerability |
| dev | Game Development Systems | empireii |
| qa | NetWitness Quality Assurance Systems | empirei |
| network | Network Infrastructure, Switch | core switch |
| network | Network Infrastructure, Router | core router |

### hnl.asset.host

This metakey has the short hostname in lowercase.

### hnl.asset.date

This metakey contains the numeric date the system was added to the feed in the YYYYMMDD format. This is used to determine age of the entry and to also know that prior to this date there is no business contextual meta generated.

### hnl.asset.loc

This metakey identifies the location of the system. The table below lists the possible values and describes the values to use in this metakey. Note the values are always lowercase.

|  |  |
| --- | --- |
| **Value** | **Description** |
| hqdc-01 | Headquarters Data Center 1 |
| lvdc-02 | Leonardville Data Center 2 |
| mscwdc-03 | Moscow Data Center 3 |
| raddc-04 | Radium Data Center 4 |

# Custom Intelligence

## Metakey Description

The table below shows the metakey names along with their data types and if they can or will contain multiple values which would define them as an array in the ESA alerting platform.

|  |  |  |  |
| --- | --- | --- | --- |
| **Metakey Name** | **Multivalued** | **Metakey Type** | **Description** |
| hnl.intel | Yes | Text | General Intel metakey for use with feeds and decoder application rules. Text type of data only like hostnames or output from app rules. |
| hnl.intel.ip | No | IPv4 | IP address list of systems. |
| hnl.intel.cat | Yes | Text | Category of system, this is the basic category the intelligence will fall under. |
| hnl.intel.date | Yes | UInt32 | Date the intelligence was first added to NetWitness in YYYMMDD format, used to determine age of intelligence information and can be used with math operators <>= in reports and apprules. |
| hnl.intel.desc | Yes | Text | Short description of intelligence, to provide some context about it. |
| hnl.intel.src | Yes | Text | The source of the intelligence information. |

## Metakey Values

The table below shows the values to be used in content development for these asset metakeys. Note the spelling and case should always remain consistent to prevent overlap, inconsistencies and gaps in alerting and reporting content.

### hnl.intel

This metakey is generally populated for feeds and app rules that identify certain types of activities. The table below lists the possible values and describes the values to use in this metakey. Note the values are always lowercase.

|  |  |
| --- | --- |
| **Value** | **Description** |
| sftp server banned ip | IP address banned by sftp server for too many failed login attempts. |
| sftp server auto unban ip | IP address that was automatically unbanned on sftp server. |
| sftp manual unban ip | IP address that was manually unbanned on sftp server. |
| malware beacon | Identified malware beacon activity. |

### hnl.intel.cat

This metakey identifies the category of the intelligence. The table below lists the possible values and describes the values to use in this metakey. Note the values are always lowercase.

|  |  |
| --- | --- |
| **Value** | **Description** |
| malware | Malware related intelligence |
| phishing domain | Domains used in phishing campaigns. |
| fraudulent domain | Fraudulent domains that are attempting to impersonate legitimate ones to commit fraud. |
| user watchlist | Watchlist for users that are terminated, disabled, privileged, HR watch, legal watch. |
| system watchlist | Watchlist for systems that have been suspect or are compromised. |
|  |  |

### hnl.intel.date

This metakey contains the numeric date the systems were added to the system in the YYYYMMDD format, there is no time in this field. This is used to determine age of the entry and to also know that prior to this date there is no intelligence contextual meta generated.

### hnl.intel.desc

This metakey identifies the role of the system. The table below lists the possible values grouped by category along with the descriptions of the values to use in this metakey. Note the values are always lowercase.

|  |  |  |
| --- | --- | --- |
| **Category** | **Description** | **Value** |
| malware | Malware beacon detected from Decoder application rule. | c2 beacon |
| malware | Possible malware site | urlhaus csv hit |
| phishing domain | Domain used in phishing campaigns | known phishing domain |
| fraudulent domain | Domain used in attempt to steal credentials | fake login |
| fraudulent domain | Domain used in attempt to install software | dropper download |
| user watchlist | Terminated users | terminated user |
| user watchlist | Privileged user accounts | privileged users |
| user watchlist | Disabled users | disabled users |
| user watchlist | HR requested watch | hr watch |
|  |  |  |

### hnl.intel.src

This metakey identifies the location of the system. The table below lists the possible values and describes the values to use in this metakey. Note the values are always lowercase.

|  |  |
| --- | --- |
| **Value** | **Description** |
| urlhaus | Data sourced from Abuse.ch urlhaus |
| active directory | Data retrieved from Active Directory via script or other external feed |
| hr data | Data provided by HR |
| fbi bulletin | FBI issued bulletin |
| internal investigation team | Data uncovered during an internal security investigation. |