NetWitness® Platform XDR

Version 12.1.0.0

Service Configuration Properties Guide

NETWITNESS
Platform XDR

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

October, 2022

Contents

Introduction

This guide provides descriptions and consolidated information for each NetWitness Platform management service configuration property in one place, for example, for services like security-server, investigate-server, and correlation-server. All of these configuration properties have valid default values wherever applicable and do not need to be changed. Please use caution if you need to modify any of these values.

Note: Some of the service configuration values are set during the deployment of NetWitness Platform and are not reflected in this guide. If any of these values need to be overridden, the user must have Administrator privileges.

You can use the NetWitness nw-shell utility or the NetWitness Platform user interface to modify these values. For information about how to use the nw-shell utility, see the *Shell User Guide for NetWitness Platform*. For information about how to use the user interface to modify these values, see the *Hosts and Services Getting Started Guide for NetWitness Platform* and the *Deployment Guide for NetWitness Platform*.

Admin-server Configuration

ContextConfigProperties

Name	Default value	Type	Description
rsa.admin-server.contexthub.enabled	false	boolean	Context Hub integration in Admin Server
rsa.admin-server.contexthub.host		string	
rsa.admin-server.contexthub.port	0	integer	
rsa.admin-server.contexthub.query-timeout		seconds	timeout time for async context response query

UsageTrackingConfigurationProperties

Name	Default value	Type	Description
rsa.admin.ceip-viewed	false	boolean	CEIP(customer enhancement improvement program) tracking value, disabled by default
rsa.admin.usage-tracking-enabled	true	boolean	Usage tracking configuration value, enabled by default

SamlProperties

Name	Default value	Type	Description
rsa.security.authentication.web.saml.auto-lookup-idp-metadata	false	boolean	Controls remote lookup of IDP metadata
rsa.security.authentication.web.saml.default-idp		identityprovider metadata$identityprovider	SAML IDP to be used by default

Name	Default value	Type	Description
rsa.security.authentication.web.saml.entity-id		string	A globally unique identifier used to identify this deployment of Netwitness as a client entity in the identity provider. Every SAML message contains the entity ID.
rsa.security.authentication.web.saml.global-logout-enabled	false	boolean	Flag to determine if global logout request has to be sent to IDP
rsa.security.authentication.web.saml.idp-metadata-url		string	URL to fetch IDP metadata
rsa.security.authentication.web.saml.keystore-alias	nw-saml	string	Alias for storing signing/encryption keys in the SAML keystore
rsa.security.authentication.web.saml.metadata-reload-interval	15 minutes	seconds	Time interval between reloading IDP metadata. Defaults to 15 minutes
rsa.security.authentication.web.saml.saml-response-skew	60 minutes	seconds	Sets the maximum allowed difference between the clocks of the IDP and SP systems. Defaults to 60 seconds.
rsa.security.authentication.web.saml.sp-metadata-filename	nw_saml_metadata.xml	string	Default filename to be set when exporting the service provider metadata

Name	Default value	Type	Description
rsa.security.authentication.web.saml.sso-enabled	false	boolean	Flag to enable or disable SAML based SSO authentication
rsa.security.authentication.web.saml.trust-all-certs-for-idp-metadata	false	boolean	Flag to ignore certificate verification while downloading IDP metadata from the given URL
rsa.security.authentication.web.saml.use-proxy	false	boolean	Determines if requests to IDP has to be routed through a proxy (if configured)

WebSocketMessagingProperties

Name	Default value	Type	Description
rsa.websocket.messaging.batch-size	10	long	The number of entries to send, per message.

Analysis-server Configuration

AnalysisProperties

Name	Default value	Type	Description
rsa.analysis.auto-analyze	true	boolean	{@code true} to automatically start analyze
rsa.analysis.definition-files		set	{@link Set} of definition files to be analyzed
rsa.analysis.nws	false	boolean	Enable NWS device support.
rsa.analysis.periodic-task-wait-time	1	seconds	Time period to wait between tasks.
rsa.analysis.time-allowance	15	seconds	Time to wait before issuing the query. Ex: If the time frame is 9-10pm and time allowance is 15 minutes, query at 10:15pm.
rsa.analysis.time-frame-interval	1	seconds	Time Interval to use for each analysis time frame as we advance forward

NwDbProperties

Name	Default value	Type	Description
rsa.analysis.nwdb.host	localhost	string	NetWitness Core Query Broker host address
rsa.analysis.nwdb.password		string	NetWitness Core connection password
rsa.analysis.nwdb.port	50005	integer	NetWitness Core Query Broker port
rsa.analysis.nwdb.ssl	false	boolean	NwtWitness Core SSL flag
rsa.analysis.nwdb.start-time		string	The start time to analyze with the format of "yyyy-MM-dd HH:mm" UTC.
rsa.analysis.nwdb.user	admin	string	NetWitness Core connection user

AnalysisProperties$Temporal

Name	Default value	Type	Description
rsa.analysis.temporal.enabled	true	boolean	Use temporal services instead of Repositories
rsa.analysis.temporal.max-entries	1000	integer	Maximum number of {@link java.util.Map} entries.
rsa.analysis.temporal.retention-period	30	seconds	The period of time to retain the data.

Config-server Configuration

ConfigServerProperties

Name	Default value	Type	Description
rsa.configuration.notify-delay	5	seconds	The length of time to delay notifications to wait for more changes for an identity

Content-server Configuration

DeployProperties

Name	Default value	Type	Description
rsa.content-server.deploy.deploy-timeout	2	seconds	Max time allotted to deploy a single content to an endpoint Default is 2 minutes Minimum of 30 seconds Maximum of 1 hour
rsa.content-server.deploy.max-content-deployer-threads	4	integer	The size of the content deployer thread pool
rsa.content-server.deploy.max-policy-deployer-threads	2	integer	The size of the policy deployer thread pool

LogDeviceParserProperties

Name	Default value	Type	Description
rsa.content.parser.cache-duration	24	seconds	Time it takes for the cache that stores data to expire
rsa.content.parser.cache-duration-for-service-status	5	seconds	Time it takes for the cache that stores service status data to expire

Name	Default value	Type	Description
rsa.content.parser.database-initialization-enabled	true	boolean	Enable database initialization task
rsa.content.parser.json-feature	true	boolean	Feature toggle for whether JSON data types are supported.
rsa.content.parser.log-decoder-sync-interval	12 hours	seconds	The interval between log decoder sync sweeps.
rsa.content.parser.max-try-counter-for-ld-sync-failure	3	integer	Switch to a new Log decoder from environment after trying below configured times to previously/user configured LD
rsa.content.parser.preferred-log-decoder-name-for-sync		string	Display name of the preferred log decoder for sync job. Sync job will use this only if it is online and contains parser details
rsa.content.parser.previously-synced-log-decoder-id		string	ID of the previously synced log decoder
rsa.content.parser.remove-previous-sync-parsers-for-new-log-decoder	false	boolean	Flag to indicate that remove previously synced log device parser information in the case of new log decoder found.
rsa.content.parser.retrieval-timeout	30	seconds	Timeout to wait for nextgen response
rsa.content.parser.sleep-interval-after-notification	60	seconds	Sleep interval before triggering a task after receiving notification
rsa.content.parser.sync-from-log-decoder-enabled	true	boolean	Enable automatic sync of parsers task

Contexthub-server Configuration

LiveConfig

Name	Default value	Type	Description
rsa.cms.client.host		string	
rsa.cms.client.password		string	
rsa.cms.client.port	0	integer	
rsa.cms.client.use-ssl	false	boolean	
rsa.cms.client.username		string	

LiveConnectPathConfig

Name	Default value	Type	Description
rsa.cms.client.lc-auth-path	/authlive/authenticate/LIVECONNECT	string	
rsa.cms.client.lc-feedback-path	/liveconnect/v2/feedback/meta	string	

ServiceProperties

Name	Default value	Type	Description
rsa.contexthub.backup-data-path		string	Migration data backup location
rsa.contexthub.config-dir-path		string	Config directory which contains all the configuration files
rsa.contexthub.data-dir-path		string	Data Directory
rsa.contexthub.file-system-service		filesystemservice	
rsa.contexthub.jobs-dir-path		string	Jobs directory which contains all the job configurations

Name	Default value	Type	Description
rsa.contexthub.max-entries-for-list	100000	integer	List datasource max limit
rsa.contexthub.ootb-list-version		string	OOTB List Version
rsa.contexthub.prefetch-pool-size	3	integer	Prefetch job pool size
rsa.contexthub.replace-config	false	boolean	Replace the batch config files on service boot
rsa.contexthub.templates-dir-path		string	Template directory which contains all the templates
rsa.contexthub.tried-adding-respond-server	false	boolean	Now when the service boots-up and if there is Respond-Server already in the deployment, we should try to add that as a CH data-source, but this should be done already once, so in case user deletes the source we shouldn't add it again.

ServiceDataProperties

Name	Default value	Type	Description
rsa.contexthub.data.disk-size	120	bytes	Max database disk space allocated for the Contexthub service.
rsa.contexthub.data.used-disk-upper-threshold	95	double	

GlobalQueryResponseCachePolicy

Name	Default value	Type	Description
rsa.contexthub.query-response-cache.available-memory	0	long	
rsa.contexthub.query-response-cache.cache-name		string	

Name	Default value	Type	Description
rsa.contexthub.query-response-cache.cache-store-bulk-insert-size	20	integer	
rsa.contexthub.query-response-cache.enabled	true	boolean	
rsa.contexthub.query-response-cache.max-seconds-in-cache	1800	seconds	
rsa.contexthub.query-response-cache.modification-queue	20	integer	
rsa.contexthub.query-response-cache.percentage-of-heap-as-cache	50	double	
rsa.contexthub.query-response-cache.preload	true	boolean	
rsa.contexthub.query-response-cache.thread-pool	2	integer	
rsa.contexthub.query-response-cache.used-cache-upper-threshold	100	double	

AsyncServiceProperites

Name	Default value	Type	Description
rsa.contexthub.query-threads.core-pool-size	20	integer	
rsa.contexthub.query-threads.max-pool-size	250	integer	
rsa.contexthub.query-threads.max-seconds-before-results-expire	0	long	
rsa.contexthub.query-threads.queue-capacity	1000	integer	

ReputationProperties

Name	Default value	Type	Description
rsa.contexthub.reputation.batch-size	1000	integer	Size of the batch to be send to Reputation Server
rsa.contexthub.reputation.max-hashes-to-be-queried	595000	integer	Maximum number of hashes to be considered for refreshing in 1 day
rsa.contexthub.reputation.max-query-supported-by-reputation-server	600000	integer	Maximum number of queries supported by the live reputation service.
rsa.contexthub.reputation.max-staged-count-for-refresh	1	long	Maximum staged entries in staging store if present, prefetch will be retried in refreshCheckInterval seconds. This is done to give priority to new reputation queries. Eg: Prefetch starts at 9 PM on a day. CH checks whether the "Staged" entries in Staging store are less than maxStagedCountForRefresh. If it is less prefetch starts else prefetch is skipped for this time and retried in refreshCheckInterval seconds.
rsa.contexthub.reputation.preferred-hashing-algorithm	md5	string	Algorithms that should be used while interaction with Reputation Server
rsa.contexthub.reputation.refresh-batch-interval	15	seconds	Time Interval between 2 batches sent to reputation server for refresh
rsa.contexthub.reputation.refresh-check-interval	15	seconds	Configuration to handle "Staging Store has entries" or Any other exception/error in case of refresh (prefetch). Staged entries should get priority over refresh job. And in case of any failures CH should retry refresh after this interval. Eg: At t1, CH started refresh job but finds that there are some entries in staging store with status - "Staged" CH will check if the no. of entries are > minStagedCountForRefresh, and if thats the case it will retry refresh after seconds configured here until that day’s 11:55 PM UTC

Name	Default value	Type	Description
rsa.contexthub.reputation.reputation-query-batch-interval	2	seconds	If CH does not gets any batch from staging store for RS, next time it queries staging store for a batch is after the seconds configured here. Eg: At t1, CH got a batch from staging store and RS was queried At t2, CH did not get any batch from staging store Now at t3 (t2 + reputationQueryBatchInterval) , CH again queried staging store for a batch

StixProperties

Name	Default value	Type	Description
rsa.contexthub.stix.data-store-read-page-size	100	integer	When reading the entire data store of a STIX source, this property determines the page size

TaxiiServiceProperties

Name	Default value	Type	Description
rsa.enrichment.stix.config.disabled-xml-features		list	
rsa.enrichment.stix.config.max-taxii-poll-window	7	seconds	Maximum time range to query TAXII server in one cycle. Defaults to 7 days. E.g., If the total range to query the TAXII server is 30 days, the range will be divided into shorter time windows of 7 days each.
rsa.enrichment.stix.config.taxii-service-max-attempts	2	integer	Max number of attempts to query TAXII Service
rsa.enrichment.stix.config.taxii-service-retry-wait-in-sec	10	integer	Max number of attempts to query TAXII Service

HttpProxyProperties

Name	Default value	Type	Description
rsa.transport.http.proxy.enabled	false	boolean	
rsa.transport.http.proxy.host		string	
rsa.transport.http.proxy.ntlm-domain		string	
rsa.transport.http.proxy.password		string	
rsa.transport.http.proxy.port		integer	
rsa.transport.http.proxy.reinitialize-proxy	false	boolean	
rsa.transport.http.proxy.use-ntlm-auth	false	boolean	
rsa.transport.http.proxy.use-ssl	false	boolean	Flag indicating whether we should use HTTP or HTTPS
rsa.transport.http.proxy.user		string	

rryCorrelation-server Configuration

AlertProperties

Name	Default value	Type	Description
rsa.correlation.alert.keep-alive-time	0	long	The keepAlive time for threads
rsa.correlation.alert.max-alerts-queue-size	10000	integer	The max rabbitmq alerter queue size
rsa.correlation.alert.num-threads	3	integer	No. of threads to process
rsa.correlation.alert.respond-enabled	true	boolean	The respond is enabled globally
rsa.correlation.alert.respond-endpoint-severities		list	The list of severities which can be consumed by respond and are related to app-rules
rsa.correlation.alert.retry-delay	1	seconds	retry time for each interval
rsa.correlation.alert.risk-score-severities		list	The list in severities which can be consumed by risk score and are related to app-rules
rsa.correlation.alert.sleep-time	1000	long	The max time to sleep in thread
rsa.correlation.alert.statement-name-max-length	128	integer	The maximum length of the entire statement @Name
rsa.correlation.alert.statement-name-place-holder-max-length	64	integer	The maximum length for each place holder value in the statement @Name
rsa.correlation.alert.timeout-retry-policy	3650	seconds	Retry time in seconds for total timeout
rsa.correlation.alert.total-threads	10	integer	The total number of threads in the pool
rsa.correlation.alert.transient-enabled	true	boolean	The transient is enabled globally. Currently used only for key-value rule and not in basic rule

ContextHubProperties

Name	Default value	Type	Description
rsa.correlation.contexthub.data-expired-in-seconds	5	integer	The duration of time before the ContextHub content is too old and need to be re-retrieved.
rsa.correlation.contexthub.fail-on-retrieve-retry-count	3	integer	Number of times to retry when failed to retrieve data from ContextHub.
rsa.correlation.contexthub.fail-on-retrieve-wait-between-retries	5	seconds	Wait duration between retries when failed to retrieve data from ContextHub.
rsa.correlation.contexthub.fail-on-set-entries-wait-between-retries	5	seconds	Wait duration between retries when failed to add/delete entries to/from ContextHub.
rsa.correlation.contexthub.file-backed-dir		string	Location on local disk where to store the paged files.
rsa.correlation.contexthub.mapped-memory-size	0	integer	Total number of bytes of data that are kept in memory.
rsa.correlation.contexthub.notification-handler-thread-pool-size	8	integer	Number of concurrent notification handler threads.
rsa.correlation.contexthub.page-file-size	4096	integer	The size of each paged file stored on local disk.
rsa.correlation.contexthub.set-entries-thread-pool-size	128	integer	Number of RSAContext set entries concurrent Threads pool size.

DataPrivacyProperties

Name	Default value	Type	Description
rsa.correlation.data-privacy.global-private-fields		list	List of fields that are always removed from the output for data privacy, regardless of source

DebugProperties

Name	Default value	Type	Description
rsa.correlation.debug.actions		string	
rsa.correlation.debug.enabled	false	boolean	
rsa.correlation.debug.resource-ids		string	

EndpointProperties

Name	Default value	Type	Description
rsa.correlation.endpoint.app-rules-paths		list	{@link List} of Endpoint App Rules candidate paths of the resource file.
rsa.correlation.endpoint.enabled	true	boolean	{@code true} if Endpoint Rules processing is enabled.

EngineProperties

Name	Default value	Type	Description
rsa.correlation.engine.auto-start	true	boolean	Determines if all {@link Engine} should start on service deployed.
rsa.correlation.engine.concurrent-deployment	10	integer	Number of asynchronous Engine deployment Tasks.
rsa.correlation.engine.send-event-heart-beat-frequency	1	seconds	Log send Event heartbeat frequency.
rsa.correlation.engine.startup-error-retry-interval	10	seconds	Retry interval if error occurs during startup.

EsperProperties

Name	Default value	Type	Description
rsa.correlation.esper.background-metrics-enabled	true	boolean	Set to {@code false} to get Esper metrics on demand.
rsa.correlation.esper.background-metrics-frequency	5	seconds	How often should the background Esper metrics process should be performed.
rsa.correlation.esper.config-resource	classpath:esper/esper-config.xml	string	Esper Configuration xml Resource.
rsa.correlation.esper.enable-statement-metric	false	boolean	Set true if esper Metrics needs to be enabled. By default it is set to false by Esper. Making it true will allow to capture additional esper-metrics but note that activating Esper metrics may cause performance impacts
rsa.correlation.esper.metrics-memory-back-off	1	seconds	How long to back off for after reaching a metrics timeout error.
rsa.correlation.esper.metrics-num-threads	16	integer	The number of threads to use for calculating metrics, per engine. Each thread gets metrics for a single rule.
rsa.correlation.esper.metrics-timeout	15	seconds	How long we should allow for retrieval of metrics for a single rule. Counting memory for rules that are using a lot of memory takes a lot of time and cpu that blocks processing of new events. <p> In the case of a timeout, we will capture the error for reporting purposes.
rsa.correlation.esper.snapshot-dir		string	RSAPersist snapshot directory.
rsa.correlation.esper.snapshot-frequency	5	seconds	Taking snapshot periodic duration.
rsa.correlation.esper.use-external-clock	true	boolean	{@code true} for Esper to process CurrentTimeEvent.

FileMapProperties

Name	Default value	Type	Description
rsa.correlation.filemap.file-backed-dir		string	Location on local disk where to store the paged files.
rsa.correlation.filemap.page-file-size	4096	integer	The size of each paged file stored on local disk.
rsa.correlation.filemap.total-memory-size	0	integer	Total number of bytes of data that are kept in memory.

GeoIpProperties

Name	Default value	Type	Description
rsa.correlation.geoip.city-resource		string	The City database Resource.
rsa.correlation.geoip.local-dir		string	Local store folder where to store the database files.
rsa.correlation.geoip.org-resource		string	The Organization database Resource.

HealthProperties

Name	Default value	Type	Description
rsa.correlation.health.check-every	15	seconds	The
rsa.correlation.health.fatal-percentage	90	integer	The percentage of memory consumption at which it is considered to be in fatal state
rsa.correlation.health.health-check-id	memory-check	string	The name which is required to set the HealthCheck
rsa.correlation.health.warning-percentage	80	integer	The percentage of memory consumption at which it is considered to be Warning in Warning state

MetricProperties

Name	Default value	Type	Description
rsa.correlation.metric.collectd-max-value-length	64	integer	CollectD field value maximum length.

ServiceProperties

Name	Default value	Type	Description
rsa.correlation.re-deployment-cycle	0	integer	The current re-deployment cycle.
rsa.correlation.re-deployment-required	0	integer	The number of re-deployment required.
rsa.correlation.send-re-deployment-notification	true	boolean	{@code true} to notify SA to re-deploy all active {@code Engine}s.
rsa.correlation.version		string	Project version.
rsa.correlation.wait-before-checking-for-success-re-deployment	1	seconds	Wait duration before checking to see if SA response re-deployment is successful.

RuleProperties

Name	Default value	Type	Description
rsa.correlation.rule.fired-rules-heart-beat		integer	Number of permits for a duration.
rsa.correlation.rule.fired-rules-heart-beat-every	1	seconds	A length of time to apply the permits. Minimum of 1 second and max at 1 day.
rsa.correlation.rule.log-fired-rules	false	boolean	Should we log the rules as soon as it fired with the relevant events.
rsa.correlation.rule.max-constituent-events	0	integer	Maximum number of Events in the List sent to AlertManager.

StatsProperties

Name	Default value	Type	Description
rsa.correlation.stats.days-to-keep-stats-file	3	integer	

StreamProperties

Name	Default value	Type	Description
rsa.correlation.stream.aggregation-queue-size	10	integer	Size of the queue that holds aggregation Events staging them before sending them to Rule Engine.
rsa.correlation.stream.batch-size	0	integer	Controls how many records do we ask for at a time.
rsa.correlation.stream.big-integer-to-long	true	boolean	Choose if we want to convert {@code BigInteger} {@code Meta} value to {@code Long} like sessionid.
rsa.correlation.stream.buffer-size	0	integer	Controls the number of records the stream can keep outstanding.
rsa.correlation.stream.check-supply	false	boolean	Should this source check for supply
rsa.correlation.stream.collection-duration-in-minutes	0	integer	For query based aggregation this parameter determines if it should operate on continuous mode or finite mode. By Default it is 0 which means continuous mode. CollectionDuration should be specified in minutes.
rsa.correlation.stream.compression	0	integer	The number of bytes in each message before it will be compressed. Zero is no compression at all. range:0 to 131071
rsa.correlation.stream.compression-level	0	integer	The level of compression. 1 is fastest and 9 is the best compression. A value of zero means pick the best balance between speed and compression. range:0 to 9
rsa.correlation.stream.connection-time-out	0	integer	Override connection timeout in sources. Only if greater than 0.

Name	Default value	Type	Description
rsa.correlation.stream.default-multi-valued		list	New multi-valued fields for this version. These fields should all be migrated to multi-valued with Rule changes. A warning message will be logged if multi-valued does NOT contain all of these fields.
rsa.correlation.stream.default-single-valued		list	New single-valued fields for this version. These fields should all be migrated to single-valued with Rule changes. A warning message will be logged if single-valued does NOT contain all of these fields.
rsa.correlation.stream.dots-to-underscores	true	boolean	Choose if we want to translate "user.dst" to "user_dst".
rsa.correlation.stream.event-batch-size	1000	integer	Number of Events in a batch store in the queue.
rsa.correlation.stream.event-enrichment-queue-size	10	integer	Size of the queue to be used to enrich the {@code Event} before offer to {@code Rule} {@code Engine}.
rsa.correlation.stream.event-enrichment-thread-pool-size	8	integer	Concurrent Event enrichment Thread pool size.
rsa.correlation.stream.event-polling-timeout-in-milli-seconds	1000	long	Event polling from queue timeout in milliseconds.
rsa.correlation.stream.event-source-id	false	boolean	Controls whether we need to add the event source identifier (ESA compatibility)
rsa.correlation.stream.filter		string	Filter to be sent across to the source
rsa.correlation.stream.idle-retry-interval	0	integer	Controls how long to wait (in milli-seconds) before retrying an idle source.
rsa.correlation.stream.lag-time	15	seconds	Lag time is the expected time an event takes to pass through the different levels of capture/parse etc and become available to query in the concentrator.
rsa.correlation.stream.lowercase		list	Choose if the fields to translate to lower case

Name	Default value	Type	Description
rsa.correlation.stream.max-sessions	0	integer	Controls the number of sessions in a batch. The more you filter out ESA data source traffic, the lower you should set this value.
rsa.correlation.stream.mechanism		string	NextGen core devices send and receive type 'AGGREGATION' or 'QUERY'.
rsa.correlation.stream.minutes-back	5	integer	Controls how far back in time should we go for a fresh start.
rsa.correlation.stream.multi-valued		list	Choose the fields considered as multi-valued.
rsa.correlation.stream.multi-valued-as-array	false	boolean	{@code true} to convert multi-valued Collection to Array.
rsa.correlation.stream.no-system-meta	false	boolean	Controls the addition of system meta to records.
rsa.correlation.stream.pre-fetch	0	integer	Controls how many batches to pull and keep ready in anticipation of demand
rsa.correlation.stream.query		string	Query Based RecordStream select clause for all sources.
rsa.correlation.stream.reader-buffer-size	1048576	integer	
rsa.correlation.stream.retrieve-record-stream-stats-every	2	seconds	How often should the {@code RecordStream} status be retrieved.
rsa.correlation.stream.retrieve-schema-every	5	seconds	A length of time to apply the permits. Minimum of 1 second and max at 1 day.
rsa.correlation.stream.retrieve-schema-frequency	1	integer	Number of permits for a duration.
rsa.correlation.stream.retry-timeout	0	integer	Controls how long to wait (in milli-seconds) before retrying a failed source.
rsa.correlation.stream.save-position-every	1	seconds	A length of time to apply the permits. Minimum of 1 second and max at 1 day.
rsa.correlation.stream.save-position-frequency	1	integer	Number of permits for a duration.

Name	Default value	Type	Description
rsa.correlation.stream.single-valued		list	Uses by Rules deployment process to ensure that these fields are not be treated as multi-valued.
rsa.correlation.stream.socket-timeout	0	integer	Override socket timeout in sources. Only if greater than 0.
rsa.correlation.stream.source-poll-interval	0	integer	Controls the parameters passed to {@code RecordSourceSubscription}.
rsa.correlation.stream.start-session-id	0	long	Override StartSession Id in sources for debug purposes. Only if greater than 0.
rsa.correlation.stream.tcp-no-delay	false	boolean	
rsa.correlation.stream.thread-pool-size	0	integer	Controls the size of the thread pool used the stream executor. Default to 100.
rsa.correlation.stream.time-batch-in-seconds	0	integer	Determines the batch size for the query based aggregation in seconds. By default it will be a 60 second window. This for now will not be configurable for user. This is because concentrator operates most efficiently when the time window is a minute.
rsa.correlation.stream.time-measured-in-seconds	true	boolean	{@code true} if time meta is measured in seconds in the event.
rsa.correlation.stream.time-meta-field	time	string	Decides what field should be used for time.
rsa.correlation.stream.time-order-by-field		string	Controls the name of the field that we consider the timestamp. This must be a long value.
rsa.correlation.stream.time-order-hold-interval	0	integer	To order records from multiple sources, we need to allow some "hold" time for sessions within a time window to arrive from all sources. This parameter specifies the hold interval (in milli-seconds)
rsa.correlation.stream.time-order-no-inflow-give-up-interval	0	integer	Controls the interval (in milliseconds) after which we take a "quiet" source out of the equation to allow progress on a time ordered stream. The default value is 0, which implies that we wait forever for events to arrive.

Name	Default value	Type	Description
rsa.correlation.stream.time-order-offline-give-up-interval	0	integer	Controls the interval (in milli-seconds) after which we take an offline source out of the equation to allow progress on a time ordered stream. The default value is 0, which implies that we wait forever. This parameter does not affect the re-connection retries; those which are performed in all cases.
rsa.correlation.stream.time-ordered	false	boolean	Enables source time synchronization and ordering.
rsa.correlation.stream.use-direct-buffer	false	boolean	
rsa.correlation.stream.use-event-time-for-esper	false	boolean	{@code true} to use the timeMetaField in the Event for Esper CurrentTimeEvent.

MigrationProperties

Name	Default value	Type	Description
rsa.migration.home-data-path	/var/netwitness/esa	string	The location of ESA home directory

RecordStreamMetrics

Name	Default value	Type	Description
rsa.records.stream.version		string	

Endpoint-broker-server Configuration

AggregationProperties

Name	Default value	Type	Description
rsa.endpoint.broker.cache-enabled	true	boolean	Cache enabled
rsa.endpoint.broker.cache-entry-limit	1000	integer	Cache entries limit
rsa.endpoint.broker.fetched-machines-limit	100	integer	The number of machine infos fetched for a given checksum. This is used to fetch the top 'n' risky machine-infos for a given file.
rsa.endpoint.broker.last-accessed-interval	120	seconds	Time interval when server would fetch the accessible endpoint servers in active session
rsa.endpoint.broker.last-updated-interval	600	seconds	Time interval when server would fetch the accessible endpoint servers when no request is sent for a long time
rsa.endpoint.broker.max-response-pages	10	integer	Max pages that an be viewed in UI host and file list views.
rsa.endpoint.broker.ping-timeout	2	seconds	Max time server will wait for the ping query to complete
rsa.endpoint.broker.query-timeout	10	seconds	Max timeout for individual endpoint server query to complete
rsa.endpoint.broker.threads	30	integer	Max number of request handler threads

ExportProperties

Name	Default value	Type	Description
rsa.endpoint.broker.export.directory-context	ExportDirectory	string	Represents the directory context (reference name) for the files to be exported
rsa.endpoint.broker.export.file-cleanup-interval	1800	seconds	Schedule interval for cleanup of files/directories
rsa.endpoint.broker.export.file-expiration-time	3600	seconds	Expiration time for the file(s) created

Name	Default value	Type	Description
rsa.endpoint.broker.export.path-prefix	temp/export	string	Represents the path prefix for files to be exported

FileContextProperties

Name	Default value	Type	Description
rsa.endpoint.broker.file-search.timeout	30	seconds	File context keyword search operation time out in seconds

Endpoint-server Configuration

CertificateStatusProperties

Name	Default value	Type	Description
rsa.endpoint.certificate.status.ignored-notifications-retry-interval	60	seconds	Notifications are ignored once posting file status fails. These ignored notifications are queried periodically. The property defines the interval.
rsa.endpoint.certificate.status.new-files-query-for-automatic-status-interval	300	seconds	Time (in seconds) between subsequent querying of new files for automatic assignment of file status to be send to Contexthub server
rsa.endpoint.certificate.status.query-batch-size	3000	integer	* Max number of thumbprints those should be fetched from repository in a single query
rsa.endpoint.certificate.status.request-batch-size	500	integer	* Max number of thumbprints those should be part of the request sent to Contexthub-Server
rsa.endpoint.certificate.status.request-interval	300	seconds	Time (in seconds) between querying for any new Certificates seen in endpoint server Defaulting to 5 minutes

AgentCommandProperties

Name	Default value	Type	Description
rsa.endpoint.command.cache-reload-delay	5	seconds	Interval delay to reload pending commands cache
rsa.endpoint.command.cancel-interval	24	seconds	Interval to cancel expired commands
rsa.endpoint.command.expiration-count	5	integer	Indicates the maximum number of times command would be resent to agent(s)

Name	Default value	Type	Description
rsa.endpoint.command.expiration-time	20	seconds	Indicates the duration until when command will not be resent to agent(s)

DataRetentionProperties

Name	Default value	Type	Description
rsa.endpoint.config.data-retention.enabled	true	boolean	Indicates if all machine data older than configured threshold {@code #thresholdInDays}, is to be deleted. This is enabled by default.
rsa.endpoint.config.data-retention.initial-rollover-delay	1	seconds	Time to delay before the first execution of the storage size based retention job
rsa.endpoint.config.data-retention.recurrence-interval	0 0 0 * * *	string	Indicates the time and frequency to run the deletion task. Configured to run everyday at 12:00:00 AM, by default.
rsa.endpoint.config.data-retention.rollover-after	80	double	The threshold (in %) indicating the storage size used, after which data should be cleaned up from the database
rsa.endpoint.config.data-retention.rollover-chunk-size	10	double	The chuck of data that should be cleanup up from the database. For example, 10 indicates 10% of the data should be cleaned up. Used for storage size based data retention job.
rsa.endpoint.config.data-retention.rollover-delay	10	seconds	Delay between invocations of the storage size based retention job
rsa.endpoint.config.data-retention.size-based-rollover-enabled	true	boolean	Indicates if storage size based retention job is enabled. This involves clearing up the disk, if it reaches a certain threshold {@see #rolloverAfter}. This is enabled by default.
rsa.endpoint.config.data-retention.threshold-in-days	30	integer	The retention threshold specified (in days)

DownloadedDataRetentionProperties

Name	Default value	Type	Description
rsa.endpoint.config.downloaded-data-retention.enabled	true	boolean	Indicates retention active status. This is enabled by default.
rsa.endpoint.config.downloaded-data-retention.recurrence-interval	0 0 0 * * *	string	Indicates the time and frequency to run the deletion task. Configured to run everyday at 00:00:00 AM, by default.
rsa.endpoint.config.downloaded-data-retention.threshold-in-days	90	integer	The retention threshold specified (in days)

InactiveMachineRetentionProperties

Name	Default value	Type	Description
rsa.endpoint.config.inactive-machine-retention.enabled	true	boolean	Indicates if all machines inactive for more than the configured threshold {@code #thresholdInDays}, is to be deleted. This is enabled by default.
rsa.endpoint.config.inactive-machine-retention.recurrence-interval	0 0 1 * * *	string	Indicates the time and frequency to run the deletion task. Configured to run everyday at 01:00:00 AM, by default.
rsa.endpoint.config.inactive-machine-retention.threshold-in-days	90	integer	The retention threshold specified (in days)

DataStoreHealthProperties

Name	Default value	Type	Description
rsa.endpoint.data-store-thresholds.fatal-percent	95	integer	
rsa.endpoint.data-store-thresholds.warning-percent	85	integer	

DataStoreProperties

Name	Default value	Type	Description
rsa.endpoint.data.application.compression-factor	2.5	double	Indicates the compression ratio used by mongo while writing to the filesystem
rsa.endpoint.data.application.db-path		string	Specify the path/directory allocated for the database files. Assumed to be /var/netwitness/mongo by default

RepositoryProperties

Name	Default value	Type	Description
rsa.endpoint.datastore.index-creation-enabled	true	boolean	Determines whether the indexes should be be created on the service startup

FileDownloadProperties

Name	Default value	Type	Description
rsa.endpoint.download.agent-beacon-threshold	5	seconds	Indicates the agent beacon time considered to (re)attempt file download
rsa.endpoint.download.base-path		string	Path in endpoint server where downloaded files are stored. Assumed to be /var/netwitness/endpoint-server by default
rsa.endpoint.download.batch-size	1000	integer	Number of entries to fetch & process from {@link CollectionConstants#GLOBAL_FILE_DOWNLOAD_REQUEST_COLLECTION} collection
rsa.endpoint.download.command-expiration-time	20	seconds	Indicates the expiration time for automatic file download commands, after which command would be cancelled

Name	Default value	Type	Description
rsa.endpoint.download.disk-check-interval	5	seconds	Indicates the interval to check the health of disk to which files will be downloaded
rsa.endpoint.download.download-threads	10	integer	Max number of auto file download handler threads
rsa.endpoint.download.downloaded-files-cache-size	2000000	integer	Max number of entries to store as part of downloaded files cache
rsa.endpoint.download.file-processor-batch-size	100	integer	Maximum number of concurrent processing requests that should be handled by server
rsa.endpoint.download.max-attempts	50	integer	Maximum number of agents that will be tried against in order to get the file downloaded to server, following which the next server takes over (if any)
rsa.endpoint.download.max-pending-commands	50	integer	Defines the maximum cap of unprocessed file download commands that can exist for a given agent, i.e. although {@link AgentCommandRequestType#Manual} commands can still be created, it is used to restrict addition of {@link AgentCommandRequestType#Automatic} file download commands
rsa.endpoint.download.periodic-cleanup-delay	2	seconds	Interval between successive lookups and attempts made by the server to delete pending requests which are no longer required
rsa.endpoint.download.periodic-hash-cleanup-delay	1	seconds	Interval between successive lookups and attempts made by the server to delete requests for files identified to be downloaded
rsa.endpoint.download.periodic-marking-delay	5	seconds	Interval between marking requests to be considered for processing by server(s)
rsa.endpoint.download.periodic-processing-delay	1	seconds	Interval between successive lookups and attempts made by server to process pending file download requests, i.e. to create/issue file download commands
rsa.endpoint.download.periodic-retry-processing-delay	5	seconds	Interval between successive lookups and attempts made by server to retry processing of older pending file download requests

Name	Default value	Type	Description
rsa.endpoint.download.request-cache-size	2000000	integer	Max number of entries to store as part of downloaded files request cache
rsa.endpoint.download.threads	2	integer	Max number of request handler threads
rsa.endpoint.download.update-interval	5	seconds	Interval in which downloaded status of newly added files is updated

ExecutionRetryProperties

Name	Default value	Type	Description
rsa.endpoint.execution.retry.file-persistence-delay	50	seconds	Indicates the wait time for retrying file data persistence
rsa.endpoint.execution.retry.max-delay	2	seconds	Indicates the maximum delay to be used between retries
rsa.endpoint.execution.retry.min-delay	30	seconds	Indicates the minimum delay to be used between retries

ExportProperties

Name	Default value	Type	Description
rsa.endpoint.export.directory-context	ExportDirectory	string	Represents the directory context (reference name) for the files to be exported
rsa.endpoint.export.file-cleanup-interval	1800	seconds	Schedule interval for cleanup of files/directories
rsa.endpoint.export.file-expiration-time	3600	seconds	Expiration time for the file(s) created
rsa.endpoint.export.max-exportable-entries	100000	integer	Maximum entries that can be exported into csv from the database, for files
rsa.endpoint.export.path-prefix	temp/export	string	Represents the path prefix for files to be exported

FileDownloadDiskHealthProperties

Name	Default value	Type	Description
rsa.endpoint.file-download-disk-thresholds.fatal-percent	70	integer	
rsa.endpoint.file-download-disk-thresholds.warning-percent	60	integer	

FileCacheProperties

Name	Default value	Type	Description
rsa.endpoint.file.cache.expiration-time	1800	seconds	Expiration threshold, since last access of item(s)
rsa.endpoint.file.cache.size	100000	long	Maximum items in the cache

FileReputationStatusProperties

Name	Default value	Type	Description
rsa.endpoint.file.reputation.ignored-notifications-query-interval	300	seconds	Time (in seconds) between subsequent check for ignored notifications querying
rsa.endpoint.file.reputation.known-signed-providers	microsoft,apple	string	List of signature providers for which we don’t need to compute the reputation. This is only accounted when filterOutKnowFiles = true/
rsa.endpoint.file.reputation.query-batch-size	2000	integer	* Max number of hashes those should be fetched from repository in a single query
rsa.endpoint.file.reputation.request-batch-size	500	integer	* Max number of hashes those should be part of the request sent to Contexthub-Server

Name	Default value	Type	Description
rsa.endpoint.file.reputation.request-interval	10	seconds	Time (in seconds) between subsequent requests to be send to Reputation-Server
rsa.endpoint.file.reputation.skip-known-good-files	true	boolean	Should reputation be computed for files from know sources ? This can be files that are signed by known CA's or maybe what the customer might have configured to be white-listed files

RiskScoreProperties

Name	Default value	Type	Description
rsa.endpoint.file.score.query-batch-size	2000	integer	Max number of file/machines to be fetched from repository in a single query
rsa.endpoint.file.score.request-interval	20	seconds	Time (in seconds) between subsequent requests to be sent

FileContextProperties

Name	Default value	Type	Description
rsa.endpoint.file.search.timeout	30	seconds	File context keyword search operation time out in seconds
rsa.endpoint.file.search.total-count	100	integer	Max number of results that will be returned for a/any snapshot response

FileStatusProperties

Name	Default value	Type	Description
rsa.endpoint.file.status.ignored-notifications-query-interval	300	seconds	Time (in seconds) between subsequent check for ignored notifications querying

Name	Default value	Type	Description
rsa.endpoint.file.status.query-batch-size	3000	integer	* Max number of hashes those should be fetched from repository in a single query
rsa.endpoint.file.status.request-batch-size	500	integer	* Max number of hashes those should be part of the request sent to Contexthub-Server
rsa.endpoint.file.status.request-interval	10	seconds	Time (in seconds) between subsequent requests to be send to Reputation-Server

GroupPolicyProperties

Name	Default value	Type	Description
rsa.endpoint.group-policy.bulk-write-count	1000	integer	Number of items to be written as part of a batch/bulk write operation performed, to assign/update group-policy to machines present in the deployment
rsa.endpoint.group-policy.initial-sync-delay	20	seconds	Time to wait for the initial group-policy details to be synced
rsa.endpoint.group-policy.periodic-evaluation-delay	30	seconds	Interval between successive evaluations performed (if required), to assign/update group-policy to machines present in the deployment

MachineFileProperties

Name	Default value	Type	Description
rsa.endpoint.machine-file.delete-task-delay	5	seconds	Initial delay to clean-up {@link CollectionConstants#MACHINE_FILE_ COLLECTION} collection for un-managed agents and decrement host count
rsa.endpoint.machine-file.fetch-limit	50	integer	Number of documents to be fetched from {@link CollectionConstants#MACHINE_ FILE_STAGE_COLLECTION} collection amd merge to the {@link CollectionConstants#MACHINE_FILE_ COLLECTION} collection

Name	Default value	Type	Description
rsa.endpoint.machine-file.periodic-bookmark-update-time	60	seconds	Interval between successive merging of {@link CollectionConstants#MACHINE_FILE_STAGE_COLLECTION} collection to {@link CollectionConstants#MACHINE_FILE_COLLECTION} collection
rsa.endpoint.machine-file.periodic-merge-delay	30	seconds	Interval between successive merging of {@link CollectionConstants#MACHINE_FILE_STAGE_COLLECTION} collection to {@link CollectionConstants#MACHINE_FILE_COLLECTION} collection
rsa.endpoint.machine-file.refresh-time	86400	seconds	Time interval to refresh the files present in a machine. The min value is set to 8h and max value is 48h.
rsa.endpoint.machine-file.refresh-time-delay	900	seconds	This is the time interval to check if agent files needs to be refreshed and create command for the agent if so.
rsa.endpoint.machine-file.retry-count	500	integer	Indicates the number of times it must be retried
rsa.endpoint.machine-file.retry-wait-time	10	seconds	Indicates the wait time for retrying to save machineFileHistory
rsa.endpoint.machine-file.staged-machine-file-deletion-delay	10	seconds	Delay between cleaning up of machine file data from {@link CollectionConstants#MACHINE_FILE_STAGE_COLLECTION} collection
rsa.endpoint.machine-file.threads	20	integer	Max number of merge machine file handler threads
rsa.endpoint.machine-file.update-history-limit	1000	integer	Number of documents to be updated into {@link CollectionConstants#MACHINE_FILE_HISTORY_COLLECTION} collection

MachineServiceProperties

Name	Default value	Type	Description
rsa.endpoint.machine.fetched-machines-limit	100	integer	The number of machine infos fetched for a given checksum. This is used to fetch the top 'n' risky machine-infos for a given file.

Name	Default value	Type	Description
rsa.endpoint.machine.search-query-timeout	10	seconds	Max timeout for machine detail to query to complete in milliseconds
rsa.endpoint.machine.status-persistence-interval	30	seconds	Interval in seconds in which machine/agent status will be persisted to db. Since it is a costly operation higher value is preferred and more higher the value is more inaccuracy will be in status related db queries

MachineFileScoreConfigurationProperties

Name	Default value	Type	Description
rsa.endpoint.machine.file.score.limit-of-checksums-in-batch	500	integer	
rsa.endpoint.machine.file.score.min-delay-for-refresh-seconds	120	seconds	

MetaForwardProperties

Name	Default value	Type	Description
rsa.endpoint.meta.enabled	false	boolean	Enable/Disable Meta integration
rsa.endpoint.meta.ld-buffer-check-enabled	true	boolean	Configuration option to disable the throttling on Log decoder buffer availability.
rsa.endpoint.meta.ld-buffer-limit-percentage	75	integer	Pool.packet.capture / pool.packet.page percentage at which we need to throttle.
rsa.endpoint.meta.logdecoder-host-id		string	The unique identifier of the host in which the Log decoder resides.
rsa.endpoint.meta.logdecoder-port	0	integer	Log decoder Port to which metas are to be posted
rsa.endpoint.meta.logdecoder-rest-password		string	Password to access the logdecoder rest port

Name	Default value	Type	Description
rsa.endpoint.meta.logdecoder-rest-port	0	integer	Log decoder REST Port to which metas are to be posted. This port number is used to query the available buffer before sending the meta.
rsa.endpoint.meta.logdecoder-rest-username		string	Username to access the logdecoder rest port
rsa.endpoint.meta.protobuf-ssl-enabled	false	boolean	SSL or Non SSL communication
rsa.endpoint.meta.rest-ssl-enabled	false	boolean	REST SSL or Non REST SSL communication
rsa.endpoint.meta.logdecoder-host		string	Log decoder Ip or hostname to which metas are to be posted @deprecated (since 6.0.0, To handle DHCP scenarios as well as manual IP change / load balancing scenarios, .use of ` logdecoderHost ` for LD communication is deprecated.The ` logdecoderHostId ` will be used instead of ` logdecoderHost ` for all log decoder communicationin future versions.

PackagerProperties

Name	Default value	Type	Description
rsa.endpoint.packager.agent-cert-name	client.p12	string	
rsa.endpoint.packager.beacon-interval	600	seconds	
rsa.endpoint.packager.packager-dir	/usr/lib/netwitness/endpoint-agents	string	

MachineDataHandlerProperties

Name	Default value	Type	Description
rsa.endpoint.queue.file-properties-drain-at-close	false	boolean	Optionally drain the queued files data to disk when the service is shutdown normally

Name	Default value	Type	Description
rsa.endpoint.queue.file-size	100	integer	Max number of concurrent data requests that should be handled by server for processing file data
rsa.endpoint.queue.file-threads	20	integer	Max number of file persistence threads
rsa.endpoint.queue.size	100	integer	Max number of concurrent data requests that should be handled by server
rsa.endpoint.queue.threads	10	integer	Max number of request handler threads

QueueFileSystemPersistenceProperties

Name	Default value	Type	Description
rsa.endpoint.queue.file.directory-context	dataDirectory	string	Represents the directory context (reference name) for the files to be persisted from file queues
rsa.endpoint.queue.file.path-prefix	temp/queue/files	string	Represents the path prefix for files to be persisted from Files queues

RelayCommunicationProperties

Name	Default value	Type	Description
rsa.endpoint.relay.communication.connect-timeout	30	seconds	Common connect timeout for all connections.
rsa.endpoint.relay.communication.initial-delay	30	seconds	Time to wait before attempting to connect to relay server
rsa.endpoint.relay.communication.max-connections	100	integer	Maximum number of connections allowed to nchan from relay server

Name	Default value	Type	Description
rsa.endpoint.relay.communication.nchan-base-url	https://localhost:7056	string	
rsa.endpoint.relay.communication.publish-channel	/agent/publish	string	
rsa.endpoint.relay.communication.request-timeout	30	seconds	Common request timeout for all connections.
rsa.endpoint.relay.communication.retry-interval	10	seconds	Delay between connection attempts
rsa.endpoint.relay.communication.subscribe-channel	/endpoint_ server/subscribe	string	
rsa.endpoint.relay.communication.subscribe-request-timeout	5	seconds	0s is infinite time.
rsa.endpoint.relay.communication.thread-pool-size	100	integer	

RelayInstallerProperties

Name	Default value	Type	Description
rsa.endpoint.relay.installer.cert-name	relay-server-cert.p12	string	Relay-server certificate file name
rsa.endpoint.relay.installer.dependency-dir	/var/netwitness/ endpoint-server/relay	string	Directory where relay-server dependencies will be downloaded. Non root user must have read, write access.
rsa.endpoint.relay.installer.download-on-restart	true	boolean	Flag to decide whether to delete local copy of relay-server dependencies and download from configured yum repo on every endpoint server restart. It might take sometime for the downloading to complete, during which user will not be able to download relay-server installer.

Name	Default value	Type	Description
rsa.endpoint.relay.installer.init-delay	20	seconds	Delay for Background task which will download relay-server dependencies.

RelayMetricsProperties

Name	Default value	Type	Description
rsa.endpoint.relay.metrics.periodic-evaluation-delay	300	seconds	Time interval to evaluate if any relay-server config was modified and update the metrics if required
rsa.endpoint.relay.metrics.refresh-time	300	seconds	Time interval to refresh the metrics from relay-server server

SslContextProperties

Name	Default value	Type	Description
rsa.endpoint.ssl.ssl-session-cache-size	0	integer	Max number of sessions to be kept in ssl session cache
rsa.endpoint.ssl.ssl-session-timeout	0	seconds	Max time an SSL session can be reused

ThrottlingConfigurationProperties

Name	Default value	Type	Description
rsa.endpoint.throttling.enabled	true	boolean	
rsa.endpoint.throttling.max	70	integer	

UdpProperties

Name	Default value	Type	Description
rsa.transport.udp.enabled	true	boolean	Boolean to indicate if server can consume Udp packet
rsa.transport.udp.port	0	integer	UDP port
rsa.transport.udp.size	5000	integer	Max number of concurrent data requests that should be handled by server
rsa.transport.udp.threads	20	integer	Max number of request handler threads

Enrichment-server Configuration

EngineProperties

Name	Default value	Type	Description
rsa.enrichment.engine.auto-start	true	boolean	Determines if all {@link Engine} should start on service deployed.
rsa.enrichment.engine.startup-error-retry-interval	10	seconds	Retry interval if error occurs during startup.

StreamProperties

Name	Default value	Type	Description
rsa.enrichment.stream.buffer-size	40000	integer	Controls the number of records the stream can keep outstanding.
rsa.enrichment.stream.connection-time-out	0	long	Override connection timeout in sources. Only if greater than 0.
rsa.enrichment.stream.dots-to-underscores	true	boolean	Choose if we want to translate "user.dst" to "user_dst".
rsa.enrichment.stream.event-source-id	true	boolean	Controls whether we need to add the event source identifier (ESA compatibility)
rsa.enrichment.stream.lag-time	15	seconds	Lag time is the expected time an event takes to pass through the different levels of capture/parse etc and become available to query in the concentrator.
rsa.enrichment.stream.mechanism		string	{@link StreamSettings.Mechanism}.
rsa.enrichment.stream.minutes-back	5	integer	Controls how far back in time should we go for a fresh start.
rsa.enrichment.stream.multi-valued		list	Choose the fields considered as multi-valued.
rsa.enrichment.stream.reader-buffer-size	1048576	integer	

Name	Default value	Type	Description
rsa.enrichment.stream.save-position-every	1	seconds	A length of time to apply the permits. Minimum of 1 second and max at 1 day.
rsa.enrichment.stream.save-position-frequency	1	integer	Number of permits for a duration.
rsa.enrichment.stream.socket-timeout	0	long	Override socket timeout in sources. Only if greater than 0.
rsa.enrichment.stream.source-poll-interval	1000	integer	Controls the parameters passed to RecordSource#poll(int, TimeUnit).
rsa.enrichment.stream.start-session-id	0	long	Override StartSession Id in sources for debug purposes. Only if greater than 0.
rsa.enrichment.stream.tcp-no-delay	true	boolean	
rsa.enrichment.stream.time-batch-in-seconds	60	integer	Determines the batch size for the query based aggregation in seconds. By default it will be a 60 second window. This for now will not be configurable for user. This is because concentrator operates most efficiently when the time window is a minute.
rsa.enrichment.stream.time-measured-in-seconds	true	boolean	{@code true} if time meta is measured in seconds in the event.
rsa.enrichment.stream.time-meta-field	time	string	Decides what field should be used for time.
rsa.enrichment.stream.time-ordered	false	boolean	Decides if the stream should be time ordered.
rsa.enrichment.stream.use-event-time-for-esper	false	boolean	{@code true} to use the timeMetaField in the Event for Esper CurrentTimeEvent.

Integration-server Configuration

DeploymentNotificationProperties

Name	Default value	Type	Description
rsa.notification.startup-retry-interval	15s	seconds	The service startup failure retry interval.

Investigate-server Configuration

AliasesProperties

Name	Default value	Type	Description
rsa.investigate.aliases.cache-duration	24	seconds	Time it takes for the cache that stores aliases to expire
rsa.investigate.aliases.retrieval-timeout	30	seconds	Timeout to wait for aliases sdk response

ColumnGroupProperties

Name	Default value	Type	Description
rsa.investigate.column.group.number-of-visible-columns	15	integer	

EventAnalysisProperties

Name	Default value	Type	Description
rsa.investigate.eventanalysis.legacy-events-enabled	false	boolean	Flag to determine if legacy events tab and related links have to be enabled
rsa.investigate.eventanalysis.limit	5000	integer	The default event limit
rsa.investigate.eventanalysis.role-event-limit		map	The per-role event limit

IncidentProperties

Name	Default value	Type	Description
rsa.investigate.incident.max-events-per-alert	60	long	Max. number of events that should be added to a single alert when creating incidents from events

KeyrefsProperties

Name	Default value	Type	Description
rsa.investigate.keyrefs.cache-duration	2	seconds	Time it takes for the cache that stores aliases to expire
rsa.investigate.keyrefs.retrieval-timeout	30	seconds	Timeout to wait for aliases sdk response

MetaKeyCacheProperties

Name	Default value	Type	Description
rsa.investigate.metakey.cache.cache-duration	7	seconds	Number of seconds a metakey should live in the cache. Default: 1 WEEK

ReconstructionProperties

Name	Default value	Type	Description
rsa.investigate.reconstruction.clear-cache-older-than	24	seconds	Cache files which are older than this time interval would be cleared
rsa.investigate.reconstruction.compressed-file-password	netwitness	string	Default zip file password for email recon downloads

Name	Default value	Type	Description
rsa.investigate.reconstruction.content-type-file-extractor-max-size	4	bytes	From NetWitness Core documentation <p> The max number of bytes to return, zero means no limit. This parameter is used to control the maximum bytes that a large network session should return and is mainly meant to prevent an extraordinary large network session from consuming a large number of resources during the transfer. Be careful setting this parameter to zero.
rsa.investigate.reconstruction.email-attachment-hash-provider		reconstructionproperties $emailattachmenthashprovider	The calculated hash type for any email attachments
rsa.investigate.reconstruction.email-full-render	true	boolean	Flag to enable/disable full rendering of email messages. <p> When set to true email bodies will be fully reconstructed which will benefit email's with HTML body content. Styling will be preserved as best as possible—external styles and references must be removed—and inline content (images), if included in the session, will be displayed. Placeholders will be shown for content that is not available or cannot be rendered and any inline script should be made inactive but displayed to the user for informational purposes. <p> If set to false, standard rendering is used which will render the email body as best as possible and return it as text in the `bodyContent` field of the {@link Email} object. <p> This setting is dependent on the Reconstruction Object Cache being enabled. (see {@link ReconstructionProperties#objectCacheEnabled}) It is ignored otherwise.

Name	Default value	Type	Description
rsa.investigate.reconstruction.endpoint-enrichment-time-window	30	seconds	Endpoint Enrichment Query time window in seconds. Network events will be correlated with endpoint events triggered within this time window of the network event's time. If network event time is x, endpoint events will be queried from 'x - @endpointEnrichmentTimeWindow' time
rsa.investigate.reconstruction.endpoint-enrichment-time-window-buffer	5	seconds	Additional buffer time range used to query for endpoint enrichment data. If network event time is x, endpoint events will be queried till 'x + @endpointEnrichmentTimeWindow Buffer' time
rsa.investigate.reconstruction.endpoint-events-query-time-out	5	seconds	Max time allowed in seconds for all endpoint core queries to complete
rsa.investigate.reconstruction.enrichment-instance-init-delay	1	seconds	Initial delay to fetch the investigate service details from all orchestrated endpoint services
rsa.investigate.reconstruction.image-placeholder-url		uri	Url used in Email recon for web email when original images cannot be loaded
rsa.investigate.reconstruction.object-cache-enabled	true	boolean	Flag to enable/disable reconstruction object cache. In addition to caching the content (protobuf files) that are downloaded from core devices, the investigate service will attempt to cache any objects and files that are created while reconstructing sessions. For this release (11.4—the first release with the object cache) this only pertains to email reconstruction.
rsa.investigate.reconstruction.reactive-message-size	256	bytes	Used in reactive streaming to configure the maximum buffer size for holding reconstructed data.

Name	Default value	Type	Description
rsa.investigate.reconstruction.reactive-text-streaming	true	boolean	Flag to turn on reactive streaming for text reconstruction. Reactive streaming prevents web socket overload by sending as many reconstructed text blocks that fit into a known buffer size and stopping until the caller tells the service to proceed.
rsa.investigate.reconstruction.session-enrichment-time-out	10	seconds	Max time allowed in seconds for all enrichment queries to complete including core, endpoint and other enrichment queries
rsa.investigate.reconstruction.support-script-urls		uri[]	If html is generated in reconstruction, that is served to the UI via an IFRAME (as to not interfere with the functionality/styling of the main application) this setting stores an array of strings (url's) to javascript files that will be injected into the html. The javascript is injected via <script /> elements at the time of HTML file creation and therefore will be saved to the object-cache. Any updates to this array would require clearing of the object-cache and/or a service restart.
rsa.investigate.reconstruction.sync-core-timeout	600	seconds	Max time to wait for operations for caching core content to complete to prevent deadlocks. Internal setting. Not recommended for customer use.
rsa.investigate.reconstruction.wire-size-provider		reconstructionproperties $wiresizeprovider	The method used to determine object size when transmitting objects via websocket

ResponseProperties

Name	Default value	Type	Description
rsa.investigate.response.events-batch-size	5000	long	Number of data size to send per message. If client send request with stream batch size and it is smaller than this, the client batch size will be used instead.

EventsStreamProperties

Name	Default value	Type	Description
rsa.investigate.stream.events.factor-of-multiple-meta-values-with-same-key	5	integer	Like the above property. This property is used to calculate a safety threshold if not specified. It's a factor to allow for multiple meta values existing in the same key and should be something reasonably high.
rsa.investigate.stream.events.safe-num-of-column-selected	50	integer	Used to calculate a safety value for "threshold" in the query to avoid the query going unbounded if threshold is not specified. The value of threshold is calculate by the formula below: threshold = (num of sessions desired) * (num of column selected) * (factor of multiple meta values with same key) If the above (num of column selected) can't be inferred from "select" field, this default value would be used.

Launch-framework Configuration

ConfigurationModuleProperties

Name	Default value	Type	Description
rsa.configuration.backoff-duration	1	seconds	Amount of time to wait until a retry is attempted if the config-server is unavailable
rsa.configuration.connection-timeout	30	seconds	A timeout how long to wait if the config-server is unavailable
rsa.configuration.remote-enabled	false	boolean	If the configuration server is even attempted
rsa.configuration.schema-synchronization-retry-interval	1	seconds	This property controls how long to wait before retrying a failed schema synchronization attempt.

ContentProperties

Name	Default value	Type	Description
rsa.content.disk-path		path	The path where the content resides on disk

DataProperties

Name	Default value	Type	Description
rsa.data.application.advanced		map	A set of advanced properties specific to the data provider
rsa.data.application.auth-mechanism	SCRAM	string	Default username/password authentication "SCRAM". Alternative: "PLAIN"
rsa.data.application.connection-timeout	5	seconds	How long to wait before giving up on a connection attempt
rsa.data.application.database		string	The database name

Name	Default value	Type	Description
rsa.data.application.enabled	false	boolean	If true will enable database support
rsa.data.application.map-key-dot-replacement		string	Mongo disallows "." in map keys, if a value is provided, dots in map keys are replaced by it.
rsa.data.application.password		string	The connection password
rsa.data.application.secure	false	boolean	Use an SSL/TLS connection to the database
rsa.data.application.servers	[localhost]	string[]	A comma separated list of database servers
rsa.data.application.stat-cache-timeout	15	seconds	How long to wait before refreshing database statistics?
rsa.data.application.user		string	The connection user
rsa.data.control.advanced		map	A set of advanced properties specific to the data provider
rsa.data.control.auth-mechanism	SCRAM	string	Default username/password authentication "SCRAM". Alternative: "PLAIN"
rsa.data.control.connection-timeout	5	seconds	How long to wait before giving up on a connection attempt
rsa.data.control.database		string	The database name
rsa.data.control.enabled	false	boolean	If true will enable database support
rsa.data.control.map-key-dot-replacement		string	Mongo disallows "." in map keys, if a value is provided, dots in map keys are replaced by it.
rsa.data.control.password		string	The connection password
rsa.data.control.secure	false	boolean	Use an SSL/TLS connection to the database
rsa.data.control.servers	[localhost]	string[]	A comma separated list of database servers
rsa.data.control.stat-cache-timeout	15	seconds	How long to wait before refreshing database statistics?
rsa.data.control.user		string	The connection user

FileSystemProperties

Name	Default value	Type	Description
rsa.filesystem.conf-path	/etc/netwitness	string	The path to directory where all service configuration resides. Ignored if prefix is specified.
rsa.filesystem.data-path	/var/lib/netwitness	string	The path to directory where all service data resides. Ignored if prefix is specified.
rsa.filesystem.logs-path	/var/log/netwitness	string	The path to directory where all service logs reside. Ignored if prefix is specified.
rsa.filesystem.prefix		string	If not empty the prefix specifies the root for all service file system state. When empty, the individual values are used.

HealthCheckProperties

Name	Default value	Type	Description
rsa.health.check-every	15	seconds	Rate at which health checks are scheduled to run.
rsa.health.concurrency	5	integer	Number of concurrent threads that runs health checks.
rsa.health.timeout	30	seconds	Time out for a {@link com.rsa.asoc.launch.api.health.HealthCheck} when service health checks are run. If a component is unable to respond with health status with in this period, it is marked as {@link com.rsa.asoc.launch.api.health.Health.Status#Unhealthy}

LoggingAuditProperties

Name	Default value	Type	Description
rsa.logging.audit.max-file-count	10	integer	The maximum number of archive files to retain.
rsa.logging.audit.max-file-size	10	bytes	The maximum size a log file is allowed to grow

LogForwarderProperties

Name	Default value	Type	Description
rsa.logging.forward.categories		string[]	The log categories to choose for forwarding
rsa.logging.forward.destination		logforwarderproperties$destination	The forwarding destination
rsa.logging.forward.enabled	true	boolean	Is forwarding enabled?
rsa.logging.forward.host	localhost	string	The destination host address
rsa.logging.forward.port	50514	integer	The destination port
rsa.logging.forward.secure	false	boolean	Use TLS for forwarding (only supported with LOGSTASH_TCP)

LoggingProperties

Name	Default value	Type	Description
rsa.logging.levels		string	Service log levels specified as a comma separated sequence of "logger:level". Note logger names are case sensitive.

LoggingOperationalProperties

Name	Default value	Type	Description
rsa.logging.operations.max-file-count	10	integer	The maximum number of archive files to retain.

Name	Default value	Type	Description
rsa.logging.operations.max-file-size	10	bytes	Maximum file size of each file allowed to grow

MetricsAggregationProperties

Name	Default value	Type	Description
rsa.metrics.aggregation.enabled	true	boolean	Is the reporter enabled?
rsa.metrics.aggregation.filter-prefixes		list	What to report? The default behavior is to report everything, if a selection of metrics must be reported add their prefixes to this list.
rsa.metrics.aggregation.host		string	The host name of the aggregator.
rsa.metrics.aggregation.interval	1	seconds	How often to report?
rsa.metrics.aggregation.port	0	integer	The port number.

MetricsElasticProperties

Name	Default value	Type	Description
rsa.metrics.elastic.enabled	true	boolean	Is the reporter enabled?

MetricsHistoricalProperties

Name	Default value	Type	Description
rsa.metrics.historical.enabled	true	boolean	Is the reporter enabled?
rsa.metrics.historical.filter-prefixes		list	What to report? The default behavior is to report everything, if a selection of metrics must be reported add their prefixes to this list.
rsa.metrics.historical.interval	1	seconds	How often to report?

Name	Default value	Type	Description
rsa.metrics.historical.max-file-count	10	integer	The maximum number of archive files to retain.
rsa.metrics.historical.max-file-size	10	bytes	Maximum file size of each file allowed to grow

MetricsJmxProperties

Name	Default value	Type	Description
rsa.metrics.jmx.enabled	true	boolean	Is the reporter enabled?
rsa.metrics.jmx.filter-prefixes		list	What to report? The default behavior is to report everything, if a selection of metrics must be reported add their prefixes to this list.
rsa.metrics.jmx.interval	1	seconds	How often to report?

MetricsProperties

Name	Default value	Type	Description
rsa.metrics.profile-api-invocation	true	boolean	Profiles timing of all {@link com.rsa.asoc.launch.api.annotation.LaunchApi} methods.

NotificationProperties

Name	Default value	Type	Description
rsa.notification.drain-at-shutdown	true	boolean	The flag to control if we drain the notification queue before shutdown. If there are a lot of pending notifications this may cause noticeable delays in shutdown time, particularly if the deployment integration server is unavailable and each forward goes through the retry attempts.

Name	Default value	Type	Description
rsa.notification.max-pending	1000	integer	The maximum number of notifications left pending.
rsa.notification.max-threads	1	integer	The size of the thread pool.
rsa.notification.retry-at-shutdown	true	boolean	The flag to control if we should retry failed notifications when the service is going down. This is true by default but can lead to delayed shutdowns if notifications cannot be forwarded.
rsa.notification.retry-attempts		integer	The number of times we retry if a notification cannot be forwarded to the centralized notification service. The default setting is to never give up but can be changed to smaller value (e.g. 10) if it is OK to drop some notifications.
rsa.notification.retry-delay	10s	seconds	The delay between successive retry attempts.

ProcessJvmMemoryProperties

Name	Default value	Type	Description
rsa.process.jvm.memory-thresholds.fatal-percent	95	integer	Percent of heap memory usage, above which JVM health is marked Fatal
rsa.process.jvm.memory-thresholds.warning-percent	80	integer	Percent of heap memory usage, above which JVM health is marked Unhealthy

ProcessProperties

Name	Default value	Type	Description
rsa.process.shutdown-delay	5	seconds	The delay between a request to shutdown and the eventual shutdown trigger.

AuthenticationProperties

Name	Default value	Type	Description
rsa.security.authentication.prefetch-before	5	seconds	If prefetch service token enabled, fetch next when there is this much seconds left for expiry of current token
rsa.security.authentication.prefetch-service-token	true	boolean	Prefetch service tokens before they expire
rsa.security.authentication.refresh-token-lifetime	30	seconds	The time-to-live on a refresh token.
rsa.security.authentication.remote-enabled	false	boolean	Support remote authentication.
rsa.security.authentication.remote-timeout	30	seconds	The time to wait for a response before failing a remote authentication.
rsa.security.authentication.token-lifetime	8	seconds	The time-to-live on a token.
rsa.security.authentication.trusted-channel-enabled	true	boolean	Support trusted channel authentication.

AuthorizationProperties

Name	Default value	Type	Description
rsa.security.authorization.permission-cache-expiry	15	seconds	This property controls cache expiry interval for the role to permissions mapping.
rsa.security.authorization.permission-cache-size	100	integer	This property controls number of role definitions cached in the service.
rsa.security.authorization.permission-synchronization-retry-interval	1	seconds	This property controls how long to wait before retrying a failed permission synchronization attempt.
rsa.security.authorization.remote-enabled	true	boolean	This property controls if the service must synchronize its permissions to the deployment Security Server.

CertificateAuthorityProperties

Name	Default value	Type	Description
rsa.security.ca.alias	Service CA	string	The alias for the CA keypair.
rsa.security.ca.auto-sign-operational-certificate	false	boolean	Should the service operational certificate be automatically signed by the embedded CA?
rsa.security.ca.certificate-lifetime	1000	seconds	The certificate validity lifetime
rsa.security.ca.issued-time-allowance	10	seconds	The certificate issued time can allow some clock drift.
rsa.security.ca.store-certificates	false	boolean	Should the service store certificates it signs

PkiProperties

Name	Default value	Type	Description
rsa.security.pki.audit-tls-hand-shakes	true	boolean	Enables auditing of TLS handshakes
rsa.security.pki.ciphers	[TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256]	string[]	This property controls the list of SSL cipher suites used by the service.
rsa.security.pki.client-auth		ssl$clientauth	This property controls the SSL client authentication preference.
rsa.security.pki.tls-protocols		string[]	This property controls the TLS protocol versions supported by the applications.

Name	Default value	Type	Description
rsa.security.pki.trust-synchronization-retry-interval	1	seconds	This property controls how long to wait before retrying a deployment trust synchronization attempt.
rsa.security.pki.use-deployment-trust	true	boolean	This property controls if the deployment security-server must be trusted.
rsa.security.pki.use-jvm-trust	false	boolean	This property controls if the JVM trust store should be used to validate peer certificates.
rsa.security.pki.verify-certificates	true	boolean	This property controls whether we must verify server certificates.

ServiceAccountProperties

Name	Default value	Type	Description
rsa.security.serviceaccounts.auth-request-validity	1	seconds	Validity of the auth request
rsa.security.serviceaccounts.max-request-cache-size	10000	integer	Cache hashes of previously authenticated requests to prevent renegotiation attacks
rsa.security.serviceaccounts.min-interval-between-authentications	30	seconds	Minimum interval between authentications to prevent brut-force attacks
rsa.security.serviceaccounts.token-lifetime	1	seconds	The time-to-live for a service account token.

TransportBusProperties

Name	Default value	Type	Description
rsa.transport.bus.advanced		map	A map that holds any other RabbitProperties configuration
rsa.transport.bus.enabled	true	boolean	Defines if Bus is enabled
rsa.transport.bus.host	localhost	string	The connection host
rsa.transport.bus.max-consumers	16	integer	Maximum number of consumers reading the queues
rsa.transport.bus.message-prefetch	1	integer	Number of messages to be handled in a single request
rsa.transport.bus.min-consumers	8	integer	Minimum number of consumers reading the queues
rsa.transport.bus.password		string	The connection password
rsa.transport.bus.port	5672	integer	The connection port
rsa.transport.bus.recovery-interval	15	seconds	The time to wait between attempts to recover a broken RabbitMQ broker connection.
rsa.transport.bus.reply-timeout	15	seconds	The time to wait for replies to arrive before giving up. AMQP is not connection-oriented so the absence of a service on the bus can only be determined by the absence of a reply. This timeout determines how long the framework waits before giving up.
rsa.transport.bus.secure	false	boolean	Use an SSL/TLS connection to the broker
rsa.transport.bus.shutdown-timeout	5	seconds	The time to wait for workers after the container is stopped, and before the connection is forced closed. If any workers are active when the shutdown signal comes they will be allowed to finish processing as long as they can finish within this timeout. Otherwise the connection is closed and messages remain unacked (if the channel is transactional).
rsa.transport.bus.username		string	The connection user
rsa.transport.bus.virtual-host	/rsa/system	string	The connection virtual host

TransportBusSubscriptionProperties

Name	Default value	Type	Description
rsa.transport.bus.subscription.subscribe-retry-interval	5	seconds	The interval to retry declaring the bindings for subscriptions if the exchange is unavailable or missing.

TransportProperties

Name	Default value	Type	Description
rsa.transport.detailed-errors-enabled	false	boolean	A boolean indicating whether the server should return detailed errors that may contain additional implementation details.

TransportHttpProperties

Name	Default value	Type	Description
rsa.transport.http.access-token-headers		string[]	Defines the HTTP headers to check for an access token
rsa.transport.http.basic-auth-enabled	false	boolean	Defines if web security basic authentication should be enabled.
rsa.transport.http.enabled	true	boolean	Defines if HTTP is enabled
rsa.transport.http.keep-alive-timeout	60s	seconds	The number of seconds this Connector will wait for another HTTP request before closing the connection. Setting the value to 0 will indicate no (i.e. infinite) timeout.
rsa.transport.http.max-keep-alive-requests	100	integer	The maximum number of HTTP requests which can be pipelined until the connection is closed by the server. Setting this to -1 will allow an unlimited amount of pipelined or keep-alive HTTP requests.

Name	Default value	Type	Description
rsa.transport.http.port	8080	short	Defines the HTTP port
rsa.transport.http.secure	true	boolean	Defines if HTTPS must be used
rsa.transport.http.session-id-random-algorithm	HMACDRBG	string	This property controls the algorithm to use for the SecureRandom used to generate HTTP session IDs.

License-server Configuration

LicenseProperties

Name	Default value	Type	Description
rsa.license.auto-cleanup-enabled	true	boolean	Whether to enable data retention job
rsa.license.auto-cleanup-interval	24 hours	seconds	Data retention job interval. The job cleans License usage and history data older than `dataRetention` property value
rsa.license.auto-refresh-interval	60 minutes	seconds	Periodic entitlement refresh interval
rsa.license.compliance-cache-expiry	60 minutes	seconds	Compliance will be evaluated and cached for this duration before evaluating again. Set to 0 to disable cache. Maximum cache expiry duration is 6 hours
rsa.license.data-retention-period	365 days	seconds	Days to retain license usage and history data in repository

FneProperties

Name	Default value	Type	Description
rsa.license.fne.base-url	/api/1.0/	string	Base URL path of REST API, all other URLs are appended to baseUrl
rsa.license.fne.capability-request-url	/capability_request/offline	string	URL to generate a new capability request
rsa.license.fne.capability-response-url	/capability_response	string	URL to post a response of capability request
rsa.license.fne.delay-before-proxy-update	2	seconds	Wait time to hold the proxy update job before receiving all the proxy config change notifications.

Name	Default value	Type	Description
rsa.license.fne.feature-page-size	25	integer	Requests to local flexnet server is paginated. This property controls the number of features that FlexnetLS returns in a single request. Defaults to 25.
rsa.license.fne.features-url	/features	string	URL to fetch features, %s is replaced with FNE License Server instance id
rsa.license.fne.fne-restart-timeout	5 minutes	seconds	Maximum time to wait for the FNE server to restart before timing out.
rsa.license.fne.host	localhost	string	Host where FNE License Server is running, defaults to localhost
rsa.license.fne.host-id-url	/hostids/selected	string	URL to fetch Unique identifier of the environment that maps licenses
rsa.license.fne.host-ids-url	/hostids	string	URL to fetch all host identifiers available in the environment
rsa.license.fne.local-config-file	/opt/netwitness/flexnetls/local-configuration.yaml	string	Local Configuration file
rsa.license.fne.max-pages	50	integer	Maximum number of pages to be requested from FlexnetLS features response. This is to prevent requesting infinite number of pages from FlexnetLS because of any reason which may cause end-of-response to not be detected.
rsa.license.fne.port	3333	integer	Port number where FNE License Server accepts REST requests, defaults to 3333
rsa.license.fne.proxy-config-file	/etc/netwitness/flexnetls/proxy.conf	string	Proxy configuration file
rsa.license.fne.sync-url	/capability_request	string	URL to force an online sync from FNE License Server to FNO remote service to fetch Features

Name	Default value	Type	Description
rsa.license.fne.trust-store-path	/var/netwitness/flexnetls	string	Path to the directory which contains FNE server trust store files
rsa.license.fne.use-ssl	false	boolean	Is the REST API secured

Metrics-server Configuration

MetricsProperties

Name	Default value	Type	Description
rsa.metrics.content.content-sync-interval	2 minutes	seconds	Time interval at which content available should be tried to upload to Elastic-Kibana
rsa.metrics.content.elastic-health-check-interval	1 minute	seconds	Time interval at which Elastic and Kibana health should be checked
rsa.metrics.content.metrics-health-check-interval	30 minutes	seconds	Time interval at which metrics collection health for Netwitness services should be checked
rsa.metrics.content.orchestration-sync-interval	30 Seconds	seconds	Interval at which orchestration-server should be queried to get deployment details
rsa.metrics.content.overwrite-index-template	false	boolean	Controls if NW index template need to be overridden
rsa.metrics.content.saved-objects-created	false	boolean	Whether to create saved objects

AlertProcessingProperties

Name	Default value	Type	Description
rsa.metrics.elastic.alert.metrics-interval	900	seconds	Duration (in seconds) after which Alarm metrics is uploaded to elastic
rsa.metrics.elastic.alert.retry-delay	1	seconds	Interval between subsequent retries
rsa.metrics.elastic.alert.wait-time	1	seconds	Wait time post which, first retry attempt on Alert Notification will be done
rsa.metrics.elastic.alert.work-interval	60	seconds	Frequency (in seconds) how often Alerts need to collected from Elastic

ElasticRetentionProperties

Name	Default value	Type	Description
rsa.metrics.elastic.data.retention.alert-retention-threshold	60	seconds	Time duration (in days) for which alerts need to be retained
rsa.metrics.elastic.data.retention.allocated-size	100	bytes	Disk space permissible to be used for Netwitness indexes in Elastic
rsa.metrics.elastic.data.retention.time-retention-frequency	4	seconds	Interval between invocations of the time based retention job
rsa.metrics.elastic.data.retention.time-threshold	30	seconds	Time (in days) for which Additional Telemetry data needs to be retained

ElasticProperties

Name	Default value	Type	Description
rsa.metrics.elastic.host		string	Host Elastic node/cluster is running on
rsa.metrics.elastic.password		string	Password for Elastic
rsa.metrics.elastic.port	9200	integer	Port Elastic node/cluster is running on
rsa.metrics.elastic.secure	true	boolean	Secure to decide protocol for Elastic
rsa.metrics.elastic.username		string	Username to connect Elastic
rsa.metrics.elastic.verify-hostname	false	boolean	Whether to verify Elastic hostname on SSL validation

ElasticClientCertAuthenticatorProperties

Name	Default value	Type	Description
rsa.metrics.elastic.security.authenticator.clientcert.http-enabled	false	boolean	Whether HTTP authentication requests are enabled
rsa.metrics.elastic.security.authenticator.clientcert.order	0	integer	Numerical order of this authentication domain
rsa.metrics.elastic.security.authenticator.clientcert.roles-attribute		string	DN attribute in X509 certificate that identifies role of the subject principal. In NW product suite, username is mapped to a role name in elasticsearch
rsa.metrics.elastic.security.authenticator.clientcert.transport-enabled	false	boolean	Whether authentication enabled at Transport level
rsa.metrics.elastic.security.authenticator.clientcert.username-attribute		string	DN attribute in X509 Certificate that identifies subject principal (username), defaults to 'cn' (Common name)

ElasticJwtAuthenticatorProperties

Name	Default value	Type	Description
rsa.metrics.elastic.security.authenticator.jwt.http-enabled	false	boolean	Whether HTTP authentication requests are enabled
rsa.metrics.elastic.security.authenticator.jwt.jwt-header		string	Authentication backend defines how to validate username or credentials, this is specific to authenticator
rsa.metrics.elastic.security.authenticator.jwt.order	0	integer	Numerical order of this authentication domain
rsa.metrics.elastic.security.authenticator.jwt.roles-key		string	Key name in the JWT claim that contains to user roles
rsa.metrics.elastic.security.authenticator.jwt.signing-key		string	Public key from the issuer certificate that issued JWT token in Base64 format without headers (i.e.without `----BEGIN/END Publi Key----`)
rsa.metrics.elastic.security.authenticator.jwt.subject-key		string	Name of the key in JWT claim that identifies subject principal (user)
rsa.metrics.elastic.security.authenticator.jwt.transport-enabled	false	boolean	Whether authentication enabled at Transport level

ElasticServiceProperties

Name	Default value	Type	Description
rsa.metrics.elastic.service.password		string	Password for nw-service user to be used for metrics collection

KibanaProperties

Name	Default value	Type	Description
rsa.metrics.kibana.base-path		string	
rsa.metrics.kibana.connection-time-out	30	seconds	Time to changes connection timeout
rsa.metrics.kibana.host		string	Host Kibana node/cluster is running on
rsa.metrics.kibana.password		string	Password for kibana
rsa.metrics.kibana.port	0	integer	Port Kibana node/cluster is running on
rsa.metrics.kibana.secure	false	boolean	Secure to decide protocol for Kibana
rsa.metrics.kibana.username		string	Username to connect kibana
rsa.metrics.kibana.verify-hostname	false	boolean	Whether to verify kibana hostname on SSL validation

MetricsRetryProperties

Name	Default value	Type	Description
rsa.metrics.retry.retry-attempts	5	integer	The number of times we retry if a service can be configured with the latest configuration.
rsa.metrics.retry.retry-delay	4min	seconds	The delay between successive retry attempts.

TelemetryProperties

Name	Default value	Type	Description
rsa.telemetry.collect-click-stream-metrics	false	boolean	Controls if the click stream stats are to be collected
rsa.telemetry.config-load-retry-interval	2	seconds	Controls the interval to load the telemetry config

MongoDataRetentionProperties

Name	Default value	Type	Description
rsa.telemetry.mongo.data.retention.additional-data-threshold	7	seconds	Time (in days) for which Additional Telemetry data needs to be retained
rsa.telemetry.mongo.data.retention.disk-allocated-size	50	integer	Size of the data (in GB) that is allowed to be consumed by Telemetry data
rsa.telemetry.mongo.data.retention.mandatory-data-threshold	365	seconds	Time (in days) for which Mandatory Telemetry data needs to be retained
rsa.telemetry.mongo.data.retention.size-retention-frequency	1	seconds	Interval between invocations of the storage size based retention job

Node-infra-server Configuration

AdminNodeTrackerProperties

Name	Default value	Type	Description
rsa.platform.node.admin-node-ip-list-save-path	/etc/netwitness/node-infra-server/admin-node-ip-list.json	string	Path to persist ip list of possible admin nodes
rsa.platform.node.call-home-interval	15	seconds	Call home interval Reaches out to orchestration server at this given interval
rsa.platform.node.chef-status-check-interval	1	seconds	Override wait time between checks for chef status checks
rsa.platform.node.enable-call-home	true	boolean	Enable call home feature
rsa.platform.node.enable-track-admin-hosts	true	boolean	Enable tracking of admin hosts feature
rsa.platform.node.path-for-admin-node-primary-check	/nodeMode	string	Part of the URL path to find information about the admin node being primary or not
rsa.platform.node.primary-admin-host-ip-path	/etc/netwitness/node-infra-server/primary-admin-host-ip	string	Path to save the primary admin host's ip before running chef. Chef / Ohai plugin reads this file.
rsa.platform.node.restart-after-admin-node-ip-change	true	boolean	Restart service after Admin node Ip change
rsa.platform.node.switch-master-run-list	nw-dns-client	string	Chef run list to switch to new master ip
rsa.platform.node.track-admin-hosts-interval	5	seconds	Node mode check interval Reaches out to admin node to verify if it is still the primary

ChefRunProperties

Name	Default value	Type	Description
rsa.platform.node.chefrun.chef-client-command	/usr/bin/chef-client	string	Path to chef client

Name	Default value	Type	Description
rsa.platform.node.chefrun.chef-client-log-level		chefrunproperties$ chefclientloglevel	The log level of chef client
rsa.platform.node.chefrun.chef-config-location	/var/lib/netwitness/config-management/client.rb	string	The location of the Chef solo configuration
rsa.platform.node.chefrun.chef-log-location	/var/log/netwitness/config-management/chef-client.log	string	The location to write the log file for a Chef client execution
rsa.platform.node.chefrun.chef-run-timeout	1	seconds	Timeout for chef run before marking task as failed
rsa.platform.node.chefrun.sudo	true	boolean	Execute command with sudo

No-op-server Configuration

TestProperties

Name	Default value	Type	Description
rsa.noop.test.array-string		string[]	
rsa.noop.test.map-uri		map	
rsa.noop.test.pojo-array		testproppojo[]	
rsa.noop.test.pojo-list		list	
rsa.noop.test.pojo-map		map	
rsa.noop.test.simple-long		long	
rsa.noop.test.simple-pojo		testproppojo	
rsa.noop.test.simple-string		string	
rsa.noop.test.some-interval		seconds	
rsa.noop.test.some-size		bytes	

Orchestration-server Configuration

HostProperties

Name	Default value	Type	Description
rsa.orchestration.engine.host-infra.back-off-interval	15	seconds	Backoff interval in seconds
rsa.orchestration.engine.host-infra.max-backoff-factor	5	integer	Maximum call-home delay factor. Used to exponentially back off for subsequent host refresh failures.

SaltClientProperties

Name	Default value	Type	Description
rsa.orchestration.engine.salt.client.api-uri	https://localhost:8000/run	uri	The URI for the SaltStack API
rsa.orchestration.engine.salt.client.external-authentication	pam	string	The Salt API authentication mechanism
rsa.orchestration.engine.salt.client.host-verification-enabled	true	boolean	The certificate host validation when communicating with the Salt API
rsa.orchestration.engine.salt.client.password		string	The Salt API password
rsa.orchestration.engine.salt.client.retry-interval	5	seconds	The amount of time in between retries
rsa.orchestration.engine.salt.client.retry-timeout	2	seconds	The maximum amount of time to wait during retries of Salt API commands {@link #retryInterval}
rsa.orchestration.engine.salt.client.username		string	The Salt API username

ChefConfigurationProperties

Name	Default value	Type	Description
rsa.orchestration.engine.salt.component.chef-cache-run-list-location	/var/lib/netwitness/config-management/nodes	string	Directory where chef stores the json from the previous chef runs
rsa.orchestration.engine.salt.component.chef-config-location	/var/lib/netwitness/config-management/client.rb	string	The location of the Chef solo configuration
rsa.orchestration.engine.salt.component.chef-log-location	/var/log/netwitness/config-management/chef-solo.log	string	The location to write the log file for a Chef solo execution
rsa.orchestration.engine.salt.component.chef-run-list-location	/etc/netwitness/config-management/node.json	string	The location to write the Chef run list
rsa.orchestration.engine.salt.component.descriptor-location	/etc/netwitness/component-descriptor/descriptor	string	The location of the component descriptor JSON file
rsa.orchestration.engine.salt.component.use-stable-package-versions	true	boolean	When enabled, the RPM version in the component descriptor file will be used. If disabled, the latest RPM version available in the yum repository will be used instead.

ProvisionHostProperties

Name	Default value	Type	Description
rsa.orchestration.engine.salt.task.provision-host.interval	5	seconds	The amount of time in between the availability checks.
rsa.orchestration.engine.salt.task.provision-host.ping-timeout	30	seconds	Timeout for ping
rsa.orchestration.engine.salt.task.provision-host.timeout	1	seconds	The amount of time to wait for the host/minion to connect to the Salt master. The checks will happen at the configured {@link #interval}

DeploymentProperties

Name	Default value	Type	Description
rsa.orchestration.platform.node-mode	active	string	

TaskExecutionProperties

Name	Default value	Type	Description
rsa.orchestration.task.async-keep-alive-time	10	long	maximum time that excess idle threads will wait for new tasks before terminating for async tasks
rsa.orchestration.task.async-keep-alive-time-unit		timeunit	Time unit for above
rsa.orchestration.task.async-pool-size	1	integer	the maximum number of threads to allow for asynchronous executor service
rsa.orchestration.task.cleanup-interval	7	seconds	The interval at which to delete existing Tasks
rsa.orchestration.task.freeze-detection-threshold	15	seconds	Time after which a stuck monitor thread is considered frozen

Name	Default value	Type	Description
rsa.orchestration.task.number-of-threads	5	integer	Number of threads in the pool for the sync execution service
rsa.orchestration.task.retain-task-duration	30	seconds	The amount of time to keep the jobs since its created. After the configured time elapses since the task created, task will be deleted.
rsa.orchestration.task.salt-job-schedule-wait-time	5	seconds	Grace period to wait for a salt job to be scheduled
rsa.orchestration.task.shutdown-timeout	30	seconds	The amount of time to wait, after receiving a shutdown request, for an executing task to finish before interrupting the execution.
rsa.orchestration.task.task-monitor-interval	30	seconds	Interval to check for new tasks and submit them
rsa.orchestration.task.update-interval	15	seconds	Amount of time between status check of currently running asynchronous jobs

Relay-server Configuration

NchanProperties

Name	Default value	Type	Description
rsa.netwitness.relay.agent-subscribe-channel	/agent/subscribe	string	Subscription nchan URL to get the responses published by endpoint-server
rsa.netwitness.relay.connection-timeout	60	seconds	Max time to wait for the connection to be created
rsa.netwitness.relay.max-connections	100	integer	Maximum number of connections allowed to nchan from relay server
rsa.netwitness.relay.nchan-base-url	https://localhost	string	URL of the Nchan service
rsa.netwitness.relay.read-timeout	120	seconds	Max time to wait for the response before throwing error
rsa.netwitness.relay.server-metrics-url	/nchan_stub_ status	string	URL to get the nchan metrics
rsa.netwitness.relay.server-publish-channel	/endpoint_ server/publish	string	Publish nchan URL to forward the requests and endpoint-server will read from there

RelayPkiProperties

Name	Default value	Type	Description
rsa.netwitness.relay.pki.certificate-path	/etc/pki/nw/service/import	string	location of the certificate and private key
rsa.netwitness.relay.pki.initial-delay	5	seconds	Time to wait before reloading the keystore if needed
rsa.netwitness.relay.pki.relay-cert-name	relay-server-cert.chain	string	the file name of the relay-server certificate chain
rsa.netwitness.relay.pki.relay-key-name	relay-server-key.pem	string	the file name of the relay-server private key

Respond-server Configuration

MigrationProperties

Name	Default value	Type	Description
rsa.migration.im-data-path	/opt/rsa/im	string	The location of the 10.x IM service
rsa.migration.max-retries	200	integer	Number of time respond attempts to run the migration in case unable to connect mongo or mongo is down.
rsa.migration.time-to-wait-between-retries	60	seconds	Frequency (in seconds) how often respond try to connect mongo

RespondPrimaryProperties

Name	Default value	Type	Description
rsa.primary.host	true	boolean	Determine whether the current respond service is running on the primary
rsa.primary.mode		respondprimaryproperties$scheduledjobsmode	Mode of current respond server

AlertRuleProperties

Name	Default value	Type	Description
rsa.respond.alertrule.batch-size	1000	long	The number of alerts to be processed by rule in a batch
rsa.respond.alertrule.counter-reset-interval-days	7	integer	How often should rule counters be reset
rsa.respond.alertrule.enabled	true	boolean	Alert rules enabled

Name	Default value	Type	Description
rsa.respond.alertrule.frequency	5	seconds	The frequency of the alert rule job
rsa.respond.alertrule.last-counter-reset-time	0	long	Timestamp for when the rule counters were reset

ArcherIntegrationProperties

Name	Default value	Type	Description
rsa.respond.archer.export.user-domain		string	Archer UserDomain, to be set only when LDAP is enabled on Archer

RespondCacheProperties

Name	Default value	Type	Description
rsa.respond.cache.user-cache-expiry	2	seconds	How often to query security server for the latest user information like their email
rsa.respond.cache.user-cache-size	1000	integer	Total size of the user cache

DataRetentionConfiguration

Name	Default value	Type	Description
rsa.respond.dataretention.enabled	false	boolean	Is the data retention job enabled
rsa.respond.dataretention.execution-hour	0	integer	Hour at which to run the job
rsa.respond.dataretention.frequency	24	seconds	How often should the job to delete old alerts/incidents run
rsa.respond.dataretention.retention-period	90	seconds	How long should alerts/incidents be stored

IndicatorAggregationJobConfig

Name	Default value	Type	Description
rsa.respond.indicatoraggregationrule.schedule-delay	0	long	Delay and frequency of indicator aggregation jobs
rsa.respond.indicatoraggregationrule.schedule-rate	5000	long	
rsa.respond.indicatoraggregationrule.seek-ahead-days	0	integer	How many days ahead should indicator aggregation go from incident window close time.
rsa.respond.indicatoraggregationrule.seek-back-days	1	integer	How many days back should indicator aggregation go from first alert received time when aggregating indicators

IntegrationExportProperties

Name	Default value	Type	Description
rsa.respond.integration.export.archer-exchange-name	incidents.archer	string	
rsa.respond.integration.export.archer-sec-ops-integration-enabled	false	boolean	
rsa.respond.integration.export.breach-integration-enabled	false	boolean	
rsa.respond.integration.export.escalation-settings		map	
rsa.respond.integration.export.export-incident-enabled	true	boolean	
rsa.respond.integration.export.help-desk-integration-enabled	false	boolean	

NormalizationProperties

Name	Default value	Type	Description
rsa.respond.normalization.alerts-queued	100	integer	The number of alerts to queue from rabbit before waiting to consume further The more you increase it, the higher chance of losing alerts if respond goes down during normalization
rsa.respond.normalization.custom-script-filename	custom_ normalize_ alerts.js	string	The name of the main custom JavaScript file used to normalize alerts.
rsa.respond.normalization.indicator-normalization-enabled	true	boolean	Determines whether the legacy and indicator bindings should be created or not
rsa.respond.normalization.max-legacy-consumers	10	integer	The maximum number of consumers that can consume from the legacy alerting exchange.
rsa.respond.normalization.script-directory	scripts	string	The name of the directory, relative to the service home directory, that contains the normalization JavaScript files.
rsa.respond.normalization.script-filename	normalize_ alerts.js	string	The name of the main JavaScript file used to normalize alerts.
rsa.respond.normalization.shutdown-timeout	30	seconds	The maximum amount of time to wait to finish processing alerts that have been received before shutting down the service.
rsa.respond.normalization.thread-count	4	integer	The number of threads to use to normalize and persist alerts.
rsa.respond.normalization.transient-indicator-normalization-enabled	true	boolean	Determines whether the low priority transient alerts binding should be created or not

QueryProperties

Name	Default value	Type	Description
rsa.respond.query.default-batch-size	100	long	Default chunk/batch size to send a stream of items to the client (client may override)
rsa.respond.query.default-query-limit	1000	long	Default number of items to send to the client in response to a single request (client may override)
rsa.respond.query.max-query-limit	5000	long	Max number of items to send to the client in response to a single request

RiskProcessingProperties

Name	Default value	Type	Description
rsa.respond.risk.alert.processing.concurrent-processors	4	integer	Concurrent number of staging that should be done.
rsa.respond.risk.alert.processing.context-limit	1000	integer	Maximum number of alert contexts per rule in a category
rsa.respond.risk.alert.processing.default-files	cmd.exe, powershell.exe, wscript.exe, cscript.exe, rundll32.exe	string	Name of files those are considered to be default OS provided files
rsa.respond.risk.alert.processing.page-size	100	integer	Page size for query while querying for persisted alerts
rsa.respond.risk.alert.processing.persisted-collection-interval	30	seconds	Interval at which alert collection should be queried for persisted alerts
rsa.respond.risk.alert.processing.staging-cleanup-interval	5	seconds	Cleanup interval for processed AlertRule from staging collection

Name	Default value	Type	Description
rsa.respond.risk.alert.processing.staging-fetch-size	5000	integer	Number of AlertRule to be fetched from staging in a single request
rsa.respond.risk.alert.processing.staging-work-interval	10	seconds	Frequency (in seconds) how often staged entries need to fetched for processing
rsa.respond.risk.alert.processing.track-file-name-change	false	boolean	Over time file-name might change for a hash, should that changes be tracked and latest name should be saved
rsa.respond.risk.alert.processing.track-host-name-change	true	boolean	Over time host-name might change for a host, should that changes be tracked and latest name should be saved

RiskCachingProperties

Name	Default value	Type	Description
rsa.respond.risk.caching.expiration-time	60	seconds	Time (in minutes) since last access of entry post which it will expire from cache.
rsa.respond.risk.caching.grouped-cache-expiration-time	5	seconds	Time (in minutes) since last access of entry post which it will expire from grouped cache
rsa.respond.risk.caching.grouped-cache-size	10000	integer	Max number of entries to be stored in the grouped cache
rsa.respond.risk.caching.size	500000	integer	Size of entries to be stored in cache

RiskRetentionProperties

Name	Default value	Type	Description
rsa.respond.risk.data.retention.frequency	1	seconds	Frequency to run the retention job
rsa.respond.risk.data.retention.retention-period	30	seconds	The retention threshold specified (in days)
rsa.respond.risk.data.retention.roll-up-to-day	false	boolean	Controls if the rollup-time needs to be calculate from start of the day when the task is executed.

RespondScheduledJobsProperties

Name	Default value	Type	Description
rsa.respond.scheduled.jobs.aggregation-job-enabled	true	boolean	Determine whether the aggregation job enabled/disabled
rsa.respond.scheduled.jobs.data-retention-job-enabled	true	boolean	Determine whether the data retention job enabled/disabled
rsa.respond.scheduled.jobs.risk-scoring-enabled	true	boolean	Determine whether the risk scoring functionality enabled/disabled

SecurIdIntegrationProperties

Name	Default value	Type	Description
rsa.respond.securid.alert-page-size	100	integer	Alerts are fetched from incidents pagewise. This property controls the maximum number of alerts to be fetched per page
rsa.respond.securid.alert-scan-json-paths	$.events[*]..	list	List of JSONPaths to scan the given userMetas in an alert. By default, it has just one JSONPath enough to read all direct occurrences of the given userMeta values from source and destination metas in all events in an alert.

Name	Default value	Type	Description
rsa.respond.securid.incident-processing-threads	3	integer	Number of threads to process the incident update events
rsa.respond.securid.max-incident-queue-size	100	integer	Maximum size of the queue used to hold the incident change events for processing.
rsa.respond.securid.secur-id-list-update-task-interval	15 minutes	seconds	Interval of the periodic task which updates the high-risk users' list in the SecurId cloud
rsa.respond.securid.secur-id-request-batch-size	100	integer	Maximum number of users to be sent in a single request to SecurId cloud.
rsa.respond.securid.user-meta	email_ address	string	The "respond specific" meta in an alert that identifies the user to be added to SecurID high-risk users' list Defaults to email_ address

Security-server Configuration

MigrationProperties

Name	Default value	Type	Description
rsa.migration.enable	true	boolean	Flag to be used in case of unit and integration tests for disabling migration check on first boot.
rsa.migration.ui-data-path	/backup/var/lib/netwitness/uax	string	The location of 10.x SA UI data

PasswordPolicyProperties

Name	Default value	Type	Description
rsa.security.account.password-policy.cannot-include-id	false	boolean	Can the password include the account identifier in it?
rsa.security.account.password-policy.min-chars	8	integer	The minimum number of characters the password must have.
rsa.security.account.password-policy.min-lower-chars	0	integer	The minimum number of lower-case characters the password must have.
rsa.security.account.password-policy.min-non-latin-chars	0	integer	The minimum number of non-latin characters a password must have
rsa.security.account.password-policy.min-numeric-chars	0	integer	The minimum number of numeric characters the password must have.
rsa.security.account.password-policy.min-special-chars	0	integer	The minimum number of special characters the password must have.
rsa.security.account.password-policy.min-upper-chars	0	integer	The minimum number of upper-case characters the password must have.
rsa.security.account.password-policy.passwords-expire-after	30	seconds	The maximum time an account password is valid before it must be changed.
rsa.security.account.password-policy.special-chars	~!@#$%^&*_-+=`$|(){}[]:;'"<>,.?/	string	The characters that are considered "special"

PkiAuthenticationProperties

Name	Default value	Type	Description
rsa.security.authentication.pki.enabled	false	boolean	This property controls if the PKI authentication feature is enabled
rsa.security.authentication.pki.retry-interval	1	seconds	This property controls how long to wait before retrying an initialization task.

AuthenticationPolicyProperties

Name	Default value	Type	Description
rsa.security.authentication.policy.account-lockout	20	seconds	Account lockout interval
rsa.security.authentication.policy.auto-create-external-users	true	boolean	Automatically create user profiles for external accounts
rsa.security.authentication.policy.case-sensitive	true	boolean	Case sensitivity of account identifiers
rsa.security.authentication.policy.max-successive-failures-before-lockout	5	integer	Accounts are locked after successive failures
rsa.security.authentication.policy.must-have-a-role	true	boolean	Require role mapping for external users

DeploymentProperties

Name	Default value	Type	Description
rsa.security.deployment.bootstrap-retry-interval	30	seconds	The amount of time to wait before retrying a failed bootstrap attempt.

SamlUserAccountProperties

Name	Default value	Type	Description
rsa.security.saml.account.user-account-type		accounttype	Account type of the users authenticated by SAML

Source-server Configuration

FeatureProperties

Name	Default value	Type	Description
rsa.features.file-policy-feature	true	boolean	rsa.usm feature toggle to control if creating File policies are supported
rsa.features.view-sources-feature	false	boolean	rsa.usm feature toggle to control if creating File policies are supported

UsmProperties

Name	Default value	Type	Description
rsa.usm.cache-duration	24	seconds	Time it takes for the cache that stores data to expire
rsa.usm.content-initialization-enabled	true	boolean	Enable content initialization task
rsa.usm.content-sync-interval	1	seconds	The interval between content sync tasks.
rsa.usm.database-initialization-enabled	true	boolean	Enable database initialization task
rsa.usm.page-size	1000	integer	Default page size for paged response
rsa.usm.policy-ip-to-uuid-migration-enabled	true	boolean	Enable policy ip to uuid migration
rsa.usm.source-count-sync-interval	10	seconds	The interval between source count sync tasks.