PassQueen
a.k.a dumpsqueen.com

RSA NetWitness Logs & Network Administrator Exam

RSA 050-11-CARSANWLN01

Version Demo

Total Demo Questions: 9

Total Premium Questions: 99

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An administrator deploys a parser to a Packet Decoder and wants to verify that it produces searchable metadata for the expected traffic. Which items should be validated? (Choose three)

A. Verify that the parser is enabled on the target Packet Decoder

B. Verify that expected traffic passes the capture filter

C. Verify that the generated metadata key is indexed for searching

D. Restart the Broker after parser deployment

E. Create a Respond incident rule

ANSWER: A B C

Explanation:

The parser must be **enabled on the target Packet Decoder**, and the relevant traffic must **pass the configured capture filter** so that the Decoder can process it. The metadata key must also be **configured for indexing on the applicable query path** when analysts need to search for its values in Investigation.

Restarting a Broker does not enable a parser, admit filtered traffic, or create metadata indexes. A Broker federates queries across configured services; it does not perform packet parsing.

See the NetWitness Documentation portal for parser deployment, Packet Decoder configuration, and metadata-indexing procedures.

QUESTION NO: 2

The types of feeds that you can add to RSA NetWitness are:

A. Public feed, private feed

B. Custom feed. Live feed

C. Identity feed, resource feed

D. Custom feed, identity feed

ANSWER: B

Explanation:

Custom feed. Live feed is correct because NetWitness supports both administrator-created custom feeds and feeds obtained through the NetWitness Live service. A custom feed is created or maintained by the organization to supply locally relevant contextual data, such as indicators, asset-related values, user-related values, or other intelligence that should enrich investigation and correlation. NetWitness Live feeds are curated content packages made available through the NetWitness Live service and can be subscribed to and deployed into the environment. After a feed is configured and enabled, NetWitness can use its entries to add context to observed log and network metadata, helping analysts identify notable activity and investigate events with additional intelligence. This distinction is important operationally: custom feeds allow direct control of organization-specific data, while Live feeds provide maintained threat-intelligence and content sources delivered through the platform's content service. RSA's NetWitness documentation and community resources describe NetWitness Live as the mechanism for obtaining deployable content, including feeds, and provide product guidance for administering contextual intelligence. See the NetWitness Community and NetWitness product resources for current documentation and administration materials.

QUESTION NO: 3

To create a feed for all of your event sources, you could:

A. Deploy a feed from Live

B. Export event source data from the Manage Events Sources interface and create a custom feed

C. Create a log parser

D. Export event source data from the Manage Events Sources interface and create an identity feed

ANSWER: B

Explanation:

Export event source data from the Manage Events Sources interface and create a custom feed is correct because the Manage Event Sources view provides the consolidated event-source information needed to build a feed that applies across the environment. Exporting this data produces a reusable source list containing the event-source attributes identified by NetWitness, such as device and parser-related values. That exported content can then be used as the basis for a custom feed, allowing administrators to enrich events consistently with metadata derived from all known event sources.

Custom feeds are intended for administrator-defined lookup data and can be created from a properly formatted file. In this scenario, exporting the existing event-source inventory avoids manually compiling values and ensures the feed is based on the event sources currently managed by the platform. Once the feed is imported and enabled, its lookup keys and metadata can be used during parsing and enrichment so that matching events receive the desired context. This approach aligns with the NetWitness workflow of managing event sources centrally and using feed data for enrichment. See the NetWitness Platform documentation community and the NetWitness documentation portal for platform configuration and feed-management guidance.

QUESTION NO: 4

You configure an email server for notifications for everything except the Reporting Engine in:

A. ADMIN > System > Global Auditing

B. ADMIN > System > Legacy Notifications

C. ADMIN > System > Email

D. ADMIN > System > Global Notifications

ANSWER: C

Explanation:

ADMIN > System > Email is the centralized NetWitness Administration location for defining the SMTP email-server settings used by platform notification services. An administrator configures the mail-server connection details there, including the SMTP host, port, transport security requirements, sender information, and—where required—SMTP authentication. Once the email server is configured, NetWitness services that use the shared notification infrastructure can send operational messages, such as system alerts and appliance-related notifications, through that SMTP service.

The Reporting Engine is intentionally treated separately because reporting has its own delivery and scheduling configuration model. Its email distribution settings are associated with report generation and report scheduling rather than the common system-notification mail configuration. Therefore, when the question concerns configuring the email server for notifications across the NetWitness platform while excluding Reporting Engine reporting, the System Email page is the applicable administrative path.

For current NetWitness product documentation and administrative guidance, consult the NetWitness Documentation portal and the NetWitness Community, which provide version-specific administration and configuration references.

QUESTION NO: 5

If you choose "Stop Rule Processing" in your Application Rule definition, which of the following are action choices? (Choose three)

A. Keep

B. Filter

C. Truncate

D. Index

E. Transient

F. Remove

ANSWER: A B C

Explanation:

When an Application Rule uses the *Stop Rule Processing* action, the available handling choices are **Keep**, **Filter**, and **Truncate**. These choices determine how NetWitness handles the event or session at the point where rule processing is stopped. **Keep** retains the data under the applicable processing outcome, allowing it to remain available for downstream NetWitness processing. **Filter** applies the configured filtering outcome when the rule matches, enabling administrators to control collection and processing of data that meets the rule condition. **Truncate** preserves the applicable session while limiting the data retained, which can be useful when a rule identifies traffic for which full payload retention is unnecessary. Together, these choices provide administrators with practical control over retention and processing behavior directly within an Application Rule, while the Stop Rule Processing setting ensures that subsequent application rules are not evaluated for the matching data. RSA NetWitness documentation for Application Rules describes this action and its available choices; see the RSA NetWitness Application Rules documentation and the NetWitness documentation portal.

QUESTION NO: 6

When adding a locally defined metadata key for a device integration, which practices help preserve the configuration through content updates? (Choose three)

A. Use the device-specific custom index file.

B. Validate the XML before applying the change.

C. Reload or restart the affected service as required.

D. Edit only the vendor-supplied base index file.

E. Configure every new key as IndexAll.

ANSWER: A B C

Explanation:

Administrators should place local definitions in the device-specific `index-<device>-custom.xml` file, validate the XML before applying it, and follow the supported procedure to reload or restart the affected service so the definition is recognized. Directly modifying the vendor-supplied base index file risks losing changes when device content is updated. The metadata key should also be configured with an index level appropriate to the required query behavior. See the NetWitness Documentation portal for version-specific device-parsing and index configuration instructions.

QUESTION NO: 7

What of the following components can be used to set up external authentication for RSA NetWitness?

A. AAoP

B. Broker

C. Spectrum

D. PAM

ANSWER: D

Explanation:

PAM is the component used to configure external authentication for RSA NetWitness. PAM, or Pluggable Authentication Modules, provides a standard framework through which NetWitness services can delegate user authentication to an external identity source rather than relying solely on locally managed credentials. In a supported deployment, administrators configure the applicable PAM service settings and the underlying operating-system PAM stack to communicate with the organization's authentication infrastructure, such as an LDAP-compatible directory. This enables centralized identity management and allows authentication policy to be governed by the external directory and its associated controls.

Because PAM is integrated at the authentication layer, it is the appropriate mechanism when the requirement is to validate NetWitness user logins against an external service. Configuration should follow the NetWitness version-specific administration documentation and the operating system's PAM guidance, including secure transport, certificate validation where applicable, and controlled testing before production rollout. NetWitness documentation is available through the NetWitness Documentation portal. For background on PAM's authentication framework and configuration model, see the Red Hat PAM documentation.

QUESTION NO: 8

Which resource types can be obtained and deployed through NetWitness Live? (Choose three)

A. Parsers

B. Feeds

C. Application rules

D. PAM configuration

ANSWER: A B C

Explanation:

Parsers, **feeds**, and **application rules** are NetWitness Live resource types. Live provides managed content that administrators can subscribe to and deploy to applicable services. For example, parsers can extract metadata from supported traffic or log formats, feeds can match observed values against intelligence content, and application rules can control how matching data is handled.

PAM configuration is not a Live resource. PAM is configured at the operating-system authentication layer when integrating external authentication methods.

See the NetWitness Documentation portal for Live content subscription and deployment procedures.

QUESTION NO: 9

To run a report you need to create which of the following?

A. View

B. Alert

C. Report rule

D. Schedule

ANSWER: C

Explanation:

Report rule is correct because reporting in NetWitness is driven by a rule that defines what data is collected and how the report output is produced. The report rule contains the report logic, including the query or conditions used to select relevant events and the report's configured output details. Once this definition exists, an administrator can execute it to generate a report and can optionally associate it with scheduling so that it runs at recurring intervals. In other words, the report rule is the essential reporting object; it provides the reusable definition that NetWitness needs before there is anything to run. This design lets administrators consistently produce reports based on the same criteria, rather than recreating queries and output settings each time. Scheduling is an optional execution mechanism for an existing report definition, while the report rule is the required foundation for both manual and scheduled report generation. NetWitness product and documentation resources are available from NetWitness Documentation and the NetWitness Platform product page.