Fortinet

NSE6_DLP_AD-26

Fortinet NSE 6 - FortiDLP 26 Administrator

Latest Version: 6.0

Question: 1

An administrator is working with Fortinet support on a single endpoint where the FortiDLP agent intermittently fails a specific operation, and support needs detailed internal diagnostic detail about what the agent is doing when the fault occurs.
Which artifact is the RIGHT one to consult for this fault?

A. The Event Visibility timeline.
B. Performance reports.
C. Debug logs.
D. Audit logs.

Answer: C

Question: 2

An analyst triages a FortiDLP case built from several correlated events. A user who normally handles a handful of records per day is observed, over a short window and outside normal working hours, accessing and moving an unusually large volume of sensitive files toward removable media — a pattern that behavior analytics flags as far outside that user's established baseline.
Which reasoning BEST justifies escalating this case to an incident rather than dismissing it as benign?

A. The volume and timing deviate sharply from the user's behavioral baseline toward an egress path
B. Any access to sensitive files by a non-administrator is automatically an incident regardless of behavior.
C. The case should be dismissed because the user had legitimate access rights to the files.
D. The case should be escalated only after confirming the endpoint agent lost connectivity during the window.

Answer: A

Question: 3

While investigating, an analyst notes that FortiDLP surfaced an anomalous user activity even though no Action blocked it.
What does this illustrate about detection versus enforcement?

A. An event exists only after an enforcement Action has blocked the activity
B. Behavior analytics removes the need for any enforcement Action

C. Detection always blocks the matching activity automatically
D. Detection and visibility surface risky activity even without enforcement

Answer: D

Question: 4

An analyst argues that reviewing only discrete policy-match events gives an incomplete picture of how data moves across the environment, because much risky behavior does not trigger a single clear content match.
Which FortiDLP capability best addresses this by giving analysts visibility into data movement and behavior rather than only individual policy hits?

A. Event Visibility together with behavior analytics
B. Content inspection tuned to additional data patterns
C. Audit log review of administrator changes
D. The LDAP Sync Tool for directory identity sync

Answer: A

Question: 5

Several related events involving the same user and repeated sensitive-data movement are observed over a short period. An analyst wants to triage them together and, if warranted, escalate them for formal investigation.
Which sequence reflects the FortiDLP investigation model?

A. An incident is decomposed into events, each of which becomes its own case
B. Individual events are grouped and triaged into a case
C. Cases are atomic observations that combine into events
D. Each event automatically becomes its own separate incident

Answer: B

Question: 6

While configuring FortiDLP, an administrator distinguishes the objects they manage. They need to identify the managed endpoint that runs the agent and enforces policy locally.
Which FortiDLP object is that?

A. Asset
B. Node

C. Tenant
D. Case

Answer: B

Question: 7

A user downloads a sensitive report, renames it, embeds its contents inside an unrelated document, and later uploads that document to a personal cloud account. Content matching on the final upload finds nothing that obviously looks sensitive.
Which FortiDLP capability is most likely to still connect the upload back to the original sensitive data?

A. Performance reporting measuring the agent's resource impact.
B. LDAP Sync mapping the upload to the user's directory identity.
C. Content inspection matching sensitive patterns in the uploaded file.
D. Data lineage and behavior analytics tracking how the data moved.

Answer: D

Question: 8

During investigations, an administrator wants DLP events and policy scope to map to real user identities and organizational units instead of raw device names.
What is the purpose of the FortiDLP LDAP Sync Tool?

A. It extends DLP enforcement into sanctioned SaaS applications.
B. It provisions the tenant that the console administers.
C. It synchronizes users and groups from the corporate directory.
D. It streams endpoint telemetry from managed nodes up to the tenant.

Answer: C

Question: 9

In FortiDLP terminology, a managed laptop that runs the lightweight agent and streams telemetry to the tenant has a specific name.
What is such a managed endpoint called?

A. The console
B. A node
C. A tenant
D. An endpoint agent

Answer: B

Question: 10

A new administrator is learning the FortiDLP object model.
What does a DLP policy primarily define?

A. Which data is sensitive and what response a risky data movement triggers.
B. The debug-log verbosity level used by the endpoint agent.
C. The physical network topology connecting managed endpoints to the console.
D. The order in which cases escalate into incidents during triage.

Answer: A

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer