KillTest

Mejor calidad. Mejor servicio

Preguntas de práctica

https://www.killtest.es

Actualizaciones gratuitas durante un año

Exam : **NSE6_DLP_AD-26**

Title : Fortinet NSE 6 - FortiDLP 26 Administrator

Version : DEMO

1.An organization has deployed the FortiDLP agent to all corporate Windows laptops. An employee travels to a remote location with no internet connectivity and attempts to transfer a restricted, sensitive document to an unauthorized USB drive.
How will FortiDLP handle this action while the endpoint is offline?
A. The agent will buffer the file transfer event and evaluate the policy only after connectivity to the tenant is restored.
B. The policy is enforced and the transfer is blocked locally because the inspection engine resides on the endpoint.
C. The endpoint defaults to a fail-open state to prevent business disruption during extended network outages.
D. The transfer is permitted temporarily, but an alert is queued and sent to the administrator upon reconnection.
Answer: B
Explanation:
FortiDLP utilizes a robust endpoint-based architecture where the data inspection engine and policy configurations are stored locally on the machine. This ensures that data protection policies are consistently enforced in real-time, preventing unauthorized actions such as USB transfers even when the endpoint is completely offline and unable to communicate with the management console.

2.An administrator is preparing for an unattended mass deployment of the FortiDLP agent across 500 Windows workstations using a centralized endpoint management system.
Which parameter is required during the installation to successfully authenticate and register the agents with the organization's tenant?
A. The tenant identifier string combined with an active operator account password.
B. A static pre-shared key (PSK) that must be manually configured in the local registry.
C. An Active Directory synchronized service account assigned with deployment roles.
D. A valid FortiDLP Agent enrollment token generated for the tenant.
Answer: D
Explanation:
For bulk or automated deployments, Fortinet documentation specifies the use of a FortiDLP Agent enrollment token. This token is generated from the console and securely authenticates the newly installed agent, registering it to the correct tenant without requiring interactive operator credentials.

3.When integrating FortiDLP with Microsoft 365 to provide data protection and visibility for files stored in SharePoint and OneDrive, which method describes the correct architectural approach used by Fortinet?
A. Through API integration requiring admin consent for the FortiDLP enterprise application.
B. By routing all user web traffic through the FortiDLP secure web gateway proxy before reaching Microsoft.
C. By installing a lightweight monitoring agent directly on the Microsoft 365 Exchange and SharePoint servers.
D. By deploying a virtual sensor appliance within the Azure virtual network to intercept all outbound traffic.
Answer: A
Explanation:

FortiDLP integrates with SaaS applications like Microsoft 365 and Google Workspace via API. This requires authorizing the FortiDLP application within the cloud environment (such as granting Admin Consent in Microsoft Entra ID using OAuth2) to allow out-of-band scanning of data at rest and activity monitoring.

4.An enterprise utilizes a non-persistent Virtual Desktop Infrastructure (VDI) environment.
Which step is required during deployment to ensure FortiDLP handles agent identities and licensing correctly across ephemeral instances?
A. Dynamically clear the registry of the FortiDLP device ID upon each user logout via a custom script.
B. Manually delete stale VDI records from the FortiDLP console every 24 hours to free up licenses.
C. Follow the specific Fortinet non-persistent VDI deployment procedure for master image preparation.
D. Isolate the master image from the FortiDLP tenant until the first user login occurs.
Answer: C
Explanation:
FortiDLP supports non-persistent VDI environments by providing specific deployment procedures, including master image preparation steps. Following the official documentation for VDI deployment ensures that new ephemeral instances correctly register with the tenant without improperly exhausting the organization's license count.

5.An organization maintains its users and groups in an on-premises Active Directory environment.
Which FortiDLP component should the administrator use to synchronize these directory users with the FortiDLP tenant?
A. The FortiDLP LDAP Sync Tool.
B. The Microsoft Entra ID directory synchronization module.
C. A custom API script utilizing the SCIM protocol.
D. The native FortiDLP Agent installed on the primary domain controller.
Answer: A
Explanation:
For organizations utilizing on-premises Active Directory or LDAP, Fortinet provides the FortiDLP LDAP Sync Tool. This dedicated utility queries the local directory and securely uploads user and group data to the FortiDLP infrastructure, enabling accurate, directory-based data protection policies.