## 1. What is the primary purpose of the Power BI Admin Portal?

a) Creating data models
b) Managing tenant settings and usage metrics
c) Building dashboards
d) Configuring visuals

**Answer: b) Managing tenant settings and usage metrics**
**Explanation:** The Power BI Admin Portal allows administrators to configure tenant settings, monitor usage, and manage capacities.

---

## 2. Which feature enables Power BI administrators to restrict users from publishing content to specific regions?

a) Sensitivity labels
b) Data loss prevention (DLP) policies
c) Tenant settings
d) Usage metrics

**Answer: c) Tenant settings**
**Explanation:** Tenant settings control who can publish, share, or manage content within specific geographic regions.

---

## 3. What is a primary advantage of row-level security (RLS) in Power BI?

a) It improves dashboard performance.
b) It restricts access to data based on user roles.
c) It allows users to create custom visuals.
d) It automates data refreshes.

**Answer: b) It restricts access to data based on user roles.**
**Explanation:** RLS ensures that users only see the data they are authorized to view by applying filters based on their roles.

---

## 4. How can you enforce data protection within Power BI reports?

a) Use RLS and sensitivity labels.
b) Apply filters at the report level.
c) Configure tenant-level settings.
d) Use bookmarks.

**Answer: a) Use RLS and sensitivity labels.**
**Explanation:** RLS limits data visibility by role, and sensitivity labels classify and protect sensitive data.

---

## 5. What is the significance of sensitivity labels in Power BI?

a) They apply data transformations.
b) They classify and enforce data protection policies.
c) They automate refresh schedules.
d) They create dynamic dashboards.

**Answer: b) They classify and enforce data protection policies.**
**Explanation:** Sensitivity labels ensure that sensitive data is protected and classified according to organizational policies.

---

## 6. Which Power BI feature allows integration with Microsoft Information Protection?

a) Sensitivity labels
b) RLS
c) DLP policies
d) Usage metrics

**Answer: a) Sensitivity labels**
**Explanation:** Sensitivity labels are part of Microsoft Information Protection and ensure consistent data classification across services.

---

## 7. What is a primary purpose of Data Loss Prevention (DLP) policies in Power BI?

a) Preventing unauthorized data refreshes
b) Protecting sensitive data during sharing and export
c) Improving report performance
d) Optimizing capacity utilization

**Answer: b) Protecting sensitive data during sharing and export**
**Explanation:** DLP policies monitor and restrict sensitive data sharing, helping prevent data breaches.

---

## 8. How does Power BI handle user authentication?

a) By storing passwords in the Power BI service
b) Through integration with Azure Active Directory
c) By enabling multi-factor authentication within Power BI
d) By using external tokens only

**Answer: b) Through integration with Azure Active Directory**
**Explanation:** Power BI uses Azure Active Directory for secure user authentication and single sign-on (SSO).

---

## 9. What is the purpose of setting up a "capacity" in Power BI?

a) To improve data refresh speeds
b) To allocate dedicated resources for performance optimization
c) To control dashboard sharing
d) To restrict export options

**Answer: b) To allocate dedicated resources for performance optimization**
**Explanation:** Capacity in Power BI Premium provides dedicated resources for enhanced performance and scalability.

---

## 10. What happens when you assign a workspace to a Power BI Premium capacity?

a) It disables RLS.
b) It provides dedicated resources for that workspace.
c) It converts reports into paginated reports.
d) It automatically encrypts all data.

**Answer: b) It provides dedicated resources for that workspace.**
**Explanation:** Assigning a workspace to Premium capacity ensures that its operations use dedicated resources, improving performance.

---

## 11. Which encryption method does Power BI use to protect data at rest?

a) Symmetric key encryption only
b) Azure Storage encryption
c) Transport Layer Security (TLS)
d) Azure-managed encryption with keys

**Answer: d) Azure-managed encryption with keys**
**Explanation:** Power BI uses Azure encryption with managed keys to protect data at rest.

---

## 12. What is the role of audit logs in Power BI?

a) Managing RLS
b) Tracking user and activity logs for compliance
c) Configuring tenant settings
d) Optimizing report visuals

**Answer: b) Tracking user and activity logs for compliance**
**Explanation:** Audit logs help administrators track user actions, providing transparency and compliance insights.

---

## 13. Which setting controls whether users can share reports outside the organization?

a) Usage metrics
b) Tenant settings
c) Capacity allocation
d) Dataflows

**Answer: b) Tenant settings**
**Explanation:** Tenant settings allow administrators to enable or disable external sharing of reports.

---

## 14. Which tool helps analyze and troubleshoot slow-performing Power BI reports?

a) Usage metrics
b) Performance Analyzer
c) Data Gateway
d) RLS Testing Tool

**Answer: b) Performance Analyzer**
**Explanation:** The Performance Analyzer identifies bottlenecks by measuring visual load times and query execution.

---

## 15. How does row-level security (RLS) differ in Power BI Pro vs. Premium?

a) RLS is only available in Premium.
b) RLS in Pro supports more complex filters.
c) RLS works the same in both but Premium supports larger datasets.
d) RLS requires additional licensing in Pro.

**Answer: c) RLS works the same in both but Premium supports larger datasets.**
**Explanation:** The functionality of RLS is consistent, but Premium supports more significant dataset sizes for broader applications.

---

## 16. How can administrators monitor the refresh history of a Power BI dataset?

a) In the Data Gateway settings
b) Using the Admin Portal's Refresh History
c) From the Dataset Settings in the workspace
d) Through Power BI Audit Logs

**Answer: c) From the Dataset Settings in the workspace**
**Explanation:** Refresh history is available in the workspace's dataset settings, showing detailed logs of each refresh attempt.

---

## 17. What is the function of the Power BI Gateway?

a) To manage sensitivity labels
b) To connect on-premises data sources with the Power BI Service
c) To create paginated reports
d) To assign Premium capacity

**Answer: b) To connect on-premises data sources with the Power BI Service**
**Explanation:** Power BI Gateways securely connect on-premises data to Power BI for report generation and analysis.

---

## 18. What is "Single Sign-On (SSO)" in the context of Power BI Gateways?

a) A method for encrypting connections
b) A user authentication method that uses Azure Active Directory credentials
c) A setting to enable row-level security
d) A feature for sharing dashboards externally

**Answer: b) A user authentication method that uses Azure Active Directory credentials**
**Explanation:** SSO ensures seamless user authentication using their Azure AD credentials for Power BI Gateways.

---

## 19. What is the purpose of enabling "Export Data" in tenant settings?

a) To allow users to download entire datasets.
b) To control whether users can export data from visuals.
c) To restrict external sharing of dashboards.
d) To manage encryption settings.

**Answer: b) To control whether users can export data from visuals.**
**Explanation:** The "Export Data" setting allows administrators to specify if users can export data from reports or dashboards into external formats like Excel or CSV.

---

## 20. How does Power BI support GDPR compliance?

a) By encrypting all data at rest
b) By allowing users to configure data retention policies
c) By integrating data classification and audit logs
d) By restricting report access only to admins

**Answer: c) By integrating data classification and audit logs**
**Explanation:** Power BI supports GDPR compliance by providing tools like sensitivity labels, audit logs, and tenant-level settings to manage and monitor sensitive data.

---

## 21. What does the "Secure embed" option in Power BI do?

a) Ensures data is encrypted during sharing.
b) Enables embedding reports within applications for authenticated users.
c) Applies row-level security to all embedded visuals.
d) Configures dashboards for mobile view.

**Answer: b) Enables embedding reports within applications for authenticated users.**
**Explanation:** Secure embedding ensures that only authenticated users can view embedded reports, enhancing security.

---

## 22. How can you restrict dataset access in Power BI based on user identity?

a) By using dynamic row-level security (RLS).
b) By disabling sharing features.
c) By limiting workspace roles to Viewer only.
d) By applying data loss prevention policies.

**Answer: a) By using dynamic row-level security (RLS).**
**Explanation:** Dynamic RLS uses DAX expressions to filter data based on user identity, providing granular control over dataset access.

---

## 23. Which type of Power BI users can modify workspace settings?

a) Viewers
b) Contributors
c) Members and Admins
d) All users with a Pro license

**Answer: c) Members and Admins**
**Explanation:** Only Members and Admins of a workspace have permissions to modify workspace settings, ensuring secure management.

---

## 24. What happens when a Power BI user leaves an organization?

a) Their dashboards are deleted.
b) Ownership of their content can be reassigned by admins.
c) All reports are archived automatically.
d) Their datasets are locked.

**Answer: b) Ownership of their content can be reassigned by admins.**
**Explanation:** Power BI admins can reassign ownership of dashboards, reports, and workspaces when a user leaves the organization.

---

## 25. Which of the following is NOT a capability of Power BI audit logs?

a) Monitoring report sharing
b) Tracking dashboard views
c) Encrypting sensitive data
d) Recording data export events

**Answer: c) Encrypting sensitive data**
**Explanation:** Audit logs are designed to track user actions like sharing, viewing, and exporting but do not handle encryption.

---

## 26. What is the default data storage limit for Power BI Pro users?

a) 1 GB per user
b) 10 GB per user

c) 100 GB per workspace
d) Unlimited

**Answer: b) 10 GB per user**
**Explanation:** Power BI Pro users are allocated 10 GB of storage for their data and reports.

---

## 27. What is the purpose of "Data Protection Insights" in Power BI?

a) To visualize sensitive data metrics across an organization
b) To configure tenant settings
c) To automatically refresh datasets
d) To enhance dashboard interactivity

**Answer: a) To visualize sensitive data metrics across an organization**
**Explanation:** Data Protection Insights provide admins with a summary of sensitivity labels and data protection policies applied in Power BI.

---

## 28. Which Power BI feature ensures that only selected users can edit a shared report?

a) RLS
b) Workspace roles
c) Sensitivity labels
d) Data gateways

**Answer: b) Workspace roles**
**Explanation:** Workspace roles (Viewer, Contributor, Member, Admin) define user permissions for reports, ensuring that only authorized users can make changes.

---

## 29. How can you prevent accidental sharing of sensitive Power BI reports?

a) Disable the "Share" feature in tenant settings.
b) Use sensitivity labels and restrict external sharing.
c) Apply dynamic RLS to all visuals.
d) Block access to the Power BI Service.

**Answer: b) Use sensitivity labels and restrict external sharing.**
**Explanation:** Sensitivity labels and external sharing restrictions ensure that sensitive content is not shared accidentally.

---

## 30. What is the recommended way to enforce data refresh security for on-premises data?

a) Use RLS.
b) Configure an on-premises data gateway.
c) Enable audit logs.
d) Apply dynamic DAX expressions.

**Answer: b) Configure an on-premises data gateway.**
**Explanation:** The on-premises data gateway securely connects on-premises data to the Power BI Service for scheduled and manual refreshes.

---

## 31. Which role in Power BI allows users to manage Premium capacity settings?

a) Capacity Admin
b) Workspace Member
c) Tenant Admin
d) Power BI Developer

**Answer: a) Capacity Admin**
**Explanation:** Capacity Admins are responsible for configuring and managing Premium capacity to ensure optimal performance.

---

## 32. What is the maximum dataset size for Power BI Premium users?

a) 1 GB
b) 10 GB
c) 100 GB
d) Unlimited

**Answer: c) 100 GB**
**Explanation:** Premium capacities allow for dataset sizes up to 100 GB, significantly larger than the Pro limit.

---

## 33. How does Power BI ensure secure sharing of reports with external users?

a) By creating guest accounts in Azure AD
b) By applying DLP policies automatically
c) By using direct sharing links only
d) By enforcing row-level security on all reports

**Answer: a) By creating guest accounts in Azure AD**
**Explanation:** External users are authenticated via Azure AD guest accounts to ensure secure access.

---

## 34. How can Power BI admins enforce MFA (multi-factor authentication)?

a) By enabling it in tenant settings
b) By configuring Azure AD Conditional Access policies
c) By enabling "Secure Embed"
d) By applying RLS to all datasets

**Answer: b) By configuring Azure AD Conditional Access policies**
**Explanation:** Azure AD Conditional Access policies enforce MFA for Power BI to enhance security.

---

## 35. What feature allows monitoring of Premium capacity performance?

a) Capacity metrics app
b) Admin Portal dashboard
c) Performance Analyzer
d) Workspace Usage Logs

**Answer: a) Capacity metrics app**
**Explanation:** The Capacity Metrics app provides detailed insights into Premium capacity utilization and performance.

---

## 36. What is the main purpose of data lineage in Power BI?

a) To visualize relationships between datasets, reports, and dashboards
b) To apply row-level security across datasets
c) To track data refresh history
d) To enhance report performance

**Answer: a) To visualize relationships between datasets, reports, and dashboards**
**Explanation:** Data lineage in Power BI provides a clear visual representation of how datasets, reports, and dashboards are interconnected, helping with impact analysis and data management.

---

## 37. Which feature can prevent unauthorized report edits in a shared workspace?

a) Audit logs
b) Sensitivity labels
c) Assigning Viewer role
d) Data Loss Prevention (DLP)

**Answer: c) Assigning Viewer role**
**Explanation:** Assigning the Viewer role ensures users can view reports and dashboards but cannot edit or modify them.

---

## 38. What happens if a dataset exceeds the 1 GB memory limit in a shared capacity?

a) The dataset is split automatically.
b) The dataset cannot be refreshed.
c) The dataset is moved to Premium capacity.
d) The dataset refresh fails.

**Answer: d) The dataset refresh fails.**
**Explanation:** In shared capacities, datasets exceeding the 1 GB memory limit cannot be refreshed successfully.

---

## 39. How can you revoke access to a shared Power BI report?

a) Delete the report
b) Change the report's workspace role
c) Remove the user from sharing permissions
d) Assign a sensitivity label

**Answer: c) Remove the user from sharing permissions**
**Explanation:** Revoking a user's sharing permissions directly removes their access to the report or dashboard.

---

## 40. What is the role of Azure Private Link in Power BI?

a) To create secure report embedding
b) To enable row-level security
c) To secure data traffic by connecting Power BI Service to data sources via private IPs
d) To optimize dataset performance

**Answer: c) To secure data traffic by connecting Power BI Service to data sources via private IPs**
**Explanation:** Azure Private Link secures data traffic by ensuring that connections between Power BI and data sources happen over private networks, avoiding public internet exposure.

---

## 41. Which of the following is NOT a Power BI Workspace role?

a) Viewer
b) Contributor
c) Supervisor
d) Admin

**Answer: c) Supervisor**
**Explanation:** Power BI supports roles like Viewer, Contributor, Member, and Admin, but "Supervisor" is not a valid role.

---

## 42. What does a Power BI service principal enable?

a) Automatic dataset refresh
b) Application-level access to Power BI resources
c) Direct email sharing of reports
d) Row-level security configuration

**Answer: b) Application-level access to Power BI resources**
**Explanation:** A service principal allows applications to access Power BI resources securely, often used in automation and integration scenarios.

---

## 43. What is the main function of Power BI Admin APIs?

a) To manage RLS dynamically
b) To allow developers to automate administrative tasks in Power BI
c) To create custom visuals
d) To refresh datasets manually

**Answer: b) To allow developers to automate administrative tasks in Power BI**
**Explanation:** Power BI Admin APIs provide programmatic access to admin functionalities, such as monitoring usage and managing tenant settings.

---

## 44. What is the purpose of the “Disable Export to Excel” setting in tenant settings?

a) To reduce memory usage in shared capacity
b) To prevent unauthorized data sharing outside Power BI
c) To improve report performance
d) To enforce DLP policies automatically

**Answer: b) To prevent unauthorized data sharing outside Power BI**
**Explanation:** Disabling "Export to Excel" limits the ability of users to extract and share data outside of the Power BI environment, enhancing security.

---

## 45. Which Power BI feature helps identify data exposure risks when users export content?

a) Sensitivity labels
b) RLS
c) Usage metrics
d) Data lineage

**Answer: a) Sensitivity labels**
**Explanation:** Sensitivity labels classify data and apply protection policies, including tracking or restricting data export activities.

---

## 46. What is the purpose of Power BI's "Paginated Reports"?

a) To provide detailed, printable reports optimized for specific formats like PDF
b) To automatically refresh data in real-time
c) To create interactive dashboards
d) To visualize datasets exceeding 1 GB

**Answer: a) To provide detailed, printable reports optimized for specific formats like PDF**
**Explanation:** Paginated Reports are designed for pixel-perfect formatting, often used for financial or operational reports.

---

## 47. What does enabling "Capacity overload notifications" do in Power BI?

a) It sends alerts to users if data refreshes fail.
b) It notifies Capacity Admins when Premium capacity reaches resource limits.
c) It restricts user activity during peak hours.
d) It optimizes capacity utilization automatically.

**Answer: b) It notifies Capacity Admins when Premium capacity reaches resource limits.**
**Explanation:** Capacity overload notifications help Capacity Admins manage and allocate resources efficiently in Power BI Premium.

---

## 48. Which of the following actions is NOT logged in Power BI audit logs?

a) Sharing a report
b) Viewing a dashboard
c) Changing a workspace role
d) Renaming a Power BI desktop file

**Answer: d) Renaming a Power BI desktop file**
**Explanation:** Audit logs capture actions within the Power BI service, such as sharing and viewing, but do not track file-level changes outside the service.

---

## 49. What is the purpose of the “Admin Monitoring Workspace” in Power BI?

a) To configure tenant-level settings
b) To create RLS roles dynamically
c) To visualize and analyze tenant usage metrics
d) To automate sensitivity label assignments

**Answer: c) To visualize and analyze tenant usage metrics**
**Explanation:** The Admin Monitoring Workspace provides a centralized dashboard for analyzing tenant usage and activity logs.

---

## 50. How does Power BI ensure secure sharing of reports via email subscriptions?

a) By embedding sensitivity labels into the email content
b) By sending only a snapshot of the report without data export capabilities
c) By encrypting the email attachments with passwords
d) By requiring Pro licenses for recipients

**Answer: b) By sending only a snapshot of the report without data export capabilities**
**Explanation:** Email subscriptions in Power BI send snapshots of reports to recipients, ensuring no interactive or sensitive data is shared directly.