NOKIA

NOKIA
Fixed
Networks
Certification

Practice exam questions for Nokia Altiplano Access Controller Administration exam (4A0-F11)

The following questions will test your knowledge and help prepare you for the Nokia Altiplano Access Controller Administration written exam. Compare your responses with the Answer Key at the end of the document.

1. Which of the following is NOT a default user in the system realm?
   a. aopentsdbuser
   b. adminuser
   c. admin
   d. sysuser

2. Which of the following applications is used to upload blueprint zip files to the Access Controller?
   a. Network views
   b. Inventory manager
   c. System administration
   d. IBN provisioning

3. Which of the following statements about CAPS is FALSE?
   a. Device capabilities ensure that the intent type logic is independent of the hardware type and release number.
   b. Caps-definition zip files are included with device extensions.
   c. The capabilities of the device can be viewed from a capabilities.html file.
   d. The existence of device capabilities is indicated with the “CAPS” label in Altiplano.

4. Which of the following Altiplano installation methods is a standard procedure that requires an understanding of the Altiplano topology?
   a. Guided installation
   b. Helm chart installation
   c. Guided installation-Altiplano Bundled VM
   d. Guided installation-offline

5. Which of the following statements about the Altiplano Virtualization Platform variant (AVP) is TRUE?
   a. It manages NETCONF-based devices only.
   b. It uses the Access Controller like an Element Management System.
   c. It provides abstraction and automation capabilities in addition to Network Virtualizer capabilities.
   d. It has the option to manage only NETCONF-based, only SNMP-based, or both types of devices.

6. Which of the following statements about the Altiplano Access Controller is FALSE?
   a. Altiplano has an open modular cloud-native microservices-based architecture.
   b. Altiplano acts as the single domain controller for the entire fixed-access network.
   c. AC, NV, and ISAM are the three main layers of the Altiplano Access Controller.
   d. Altiplano provides unified access management and integrated network automation.

7. Which of the following is NOT a characteristic of Monolithic architecture?
   a. Small components
   b. Slow to start
   c. Difficult to test
   d. Difficult to scale

8. Which of the following statements about the microservices of the Altiplano Access Controller is FALSE?
   a. The AlarmIS bridge reads all Kafka alarm notifications.
   b. The health calculator constructs alarm events.
   c. The KPI engine builds operator-defined KPI metrics.
   d. The NC inventory collector performs network slicing.

9. Which of the following statements about OpenTSDB is TRUE?
   a. It is an open-source identity and access management system.
   b. It consists of query metrics and filters based on timestamps.
   c. It is used as a message broker to provide messaging capabilities.
   d. It consists of configuration and state information related to the Access Controller.

10. Which of the following statements about the device manager of the Altiplano Access Controller is FALSE?
    a. A device manager is used to manage a specific type of multi-vendor multi-technology devices.
    b. The Access Controller uses a manager directory service (MDS) to identify managers of the access network devices.
    c. The Nokia Access Management System (AMS) is the element management system for NETCONF-based devices.
    d. The Network Virtualizer, NSP, and AMS are the three types of device managers for the Altiplano Access Controller.

11. Which of the following statements about the logging infrastructure of Altiplano is FALSE?
    a. The log-appender driver for Altiplano is Prometheus.
    b. FluentD forwards the logs into the IndexSearch (OpenSearch) database.
    c. IndexSearch (OpenSearch) dashboards can be used for data analysis.
    d. Telemetry metrics are handled by OpenTSDB and Prometheus.

12. Which of the following is a log level in Altiplano?
    a. Error
    b. Fault
    c. Defect
    d. Alert

13. Which of the following statements about log sensitivity is FALSE?
    a. Protocol loggers mask sensitive/private data based on YANG extensions.
    b. To mask the fields marked with “is-sensitive”, the sensitive-includes-actual-value needs to be set to false first.
    c. An IP address is annotated as “is-sensitive” data in the YANG model.
    d. Passwords are annotated as “is-sensitive” data in the YANG model.

14. Which of the following micro-services is used to store telemetry metrics of Altiplano applications?
    a. OpenTSDB
    b. IndexSearch (OpenSearch)
    c. Grafana
    d. MariaDB

15. Which of the following metrics can be collected by the TCollector?
    a. License metrics
    b. Kafka connection metrics
    c. RESTCONF metrics
    d. Container metrics

16. Which of the following is a metric collected by FluentD?
    a. NBI/SBI NETCONF metrics
    b. Host disk metrics
    c. MariaDB metrics
    d. IndexSearch metrics

17. Which of the following statements about the Grafana installation is FALSE?
    a. Grafana is installed automatically in the helm-installation method.
    b. When using the Ansible method, the Grafana admin role is configured in the installation menu under ‘Infrastructure’.
    c. The Grafana installation script comes with the Altiplano-solution helm charts.
    d. The Grafana installation script can be used to install or uninstall Grafana dashboards.

18. Which of the following statements about syslog in Altiplano is TRUE?
    a. It can be used for system management and security auditing.
    b. The devices can be configured to send its syslog messages to Grafana.
    c. It involves collecting data for system resources such as CPU usage, disk usage, memory usage, and so on.
    d. It stores state information, alarms, and performance management information.

19. Which of the following can be used to access Altiplano logs using IndexSearch dashboards?
    a. Log exporter
    b. Discover
    c. Device syslog
    d. System load profile

20. Which of the following statements best describes a permission in Keycloak?
    a. It controls access to a resource based on specific policies.
    b. It provides complete isolation between different sets of users.
    c. It allows you to manage a set of users, roles and applications.
    d. Each permission has a unique identifier that can represent a single or set of resources.

21. Which of the following statements best describes a user in Keycloak?
    a. It represents individuals who need protection and for which access control policies are defined.
    b. It represents an individual who can authenticate and interact with applications and services managed by Keycloak.
    c. It is an individual who can request Keycloak to authenticate a client.
    d. It is an individual who wants to use Keycloak to secure it and provide a single sign-on solution.

22. Which of the following statements about roles in Keycloak in FALSE?
    a. Roles can be assigned to users to determine what actions they are allowed to perform and which resources they can access.
    b. Client roles are global roles within a realm and can be assigned to users across the entire realm.
    c. Roles are often used in conjunction with other authorization mechanisms such as policies and permissions.
    d. A user with the admin role might have full access to all features, while a user with the viewer role can only view content.

23. Which of the following is NOT a security and hardening recommendation from Nokia?
    a. Install new software packages on the operating system once they are available
    b. Modify the default remote management password
    c. Disable USB ports
    d. Change the user's default passwords

24. Which of the following protocols is used to secure Kafka communications using SSL?
    a. SSH
    b. HTTPS
    c. TCP
    d. SFTP

25. Which of the following protocols is used for the communication between WebDAV and access devices?
    a. TCP
    b. SSH
    c. HTTPS
    d. SFTP

26. Which of the following statements about certificate generation using the self-sign method is FALSE?
    a. Altiplano pod certificates are signed and issued by its own self-signed CA.
    b. Nokia recommends configuring a self-signed certificate option with CA signed certificates for the ingress controller.
    c. Nokia recommends configuring a self-signed certificate option with CA signed certificates for the WebDAV file server.
    d. Altiplano supports self-signed certificate generation only for internal pods.

27. Which of the following statements about Altiplano certificate updates is FALSE?
    a. After Altiplano has been installed, CA certificates can be re-generated and updated.
    b. After Altiplano has been installed, pod certificates can be re-generated and updated.
    c. Updated certificates are saved and packaged in a zip file.
    d. Certificates are re-generated based on the chosen option such as self-signed CA.

28. Which of the following statements about the purpose of Altiplano licenses is FALSE?
    a. Altiplano uses licenses for authentication and encryption of its TLS and HTTPS communication.
    b. A valid Altiplano core license is required to use the Altiplano access controller applications.
    c. The license allows the use of Access Controller features depending on the product variants specified in the license.
    d. The license supports a specified maximum number of subscribers corresponding to different port types.

29. Which of the following commands can be used to verify if all pods are 'running' post-restoration?
    a. kubectl get pods
    b. kubectl get sts
    c. kubectl scale
    d. kubectl exec

30. Which of the following commands can be used to check the status of a selective restore?
    a. kubectl get sts <task-id>
    b. altiplano-restore.sh –i <task-id>
    c. kubectl exec -it <task-id>
    d. kubectl scale <task-id>

31. Which of the following statements about geo-redundancy in Altiplano is FALSE?
    a. The geo-redundant installation consists of an active site and a standby site.
    b. After completing a geo-redundant switchover, the geo-redundant state should be 'healthy'.
    c. A geo-redundant switchover is an automatic process.
    d. During a geo-redundant switchover, only one Altiplano site should remain active at a time.

32. Which of the following statements about Kubernetes deployments used in the Altiplano application is TRUE?
    a. It is a resource to implement a stateless application.
    b. ReplicaSets can define and manage deployments.
    c. It ensures that a specified number of pod replicas are running at a given time.
    d. If using a data persistency pod, replicas will be using different volumes.

33. Which of the following statements about geo-redundancy in Altiplano is TRUE?
    a. It provides resiliency against catastrophic events and natural disasters that might cause a loss of a data center.
    b. It means that microservices can be deployed and replicated between different worker nodes in a Kubernetes cluster.
    c. It means that services will continue to run in case of virtual machine failure within a data center.
    d. The level of geo-redundancy is defined by "n+x" where "x" is the allowable level of failure.

34. Which of the following statements about on-demand backup is TRUE?
    a. It has the option to backup either the complete release or a specific component.
    b. The backup time is 01:00 AM GMT by default.
    c. It is recommended to perform the on-demand backup for a specific component.
    d. While performing an on-demand backup, multiple cron jobs cannot run in parallel.

35. Which of the following statements about the trial license is FALSE?
    a. It is valid only for a limited time.
    b. It should not be used in a commercial or production environment.
    c. It is also known as the evaluation license.
    d. License rights are determined by different RTUs as per end-user license agreements.

36. Which of the following statements about license states is FALSE?
    a. A license card that indicates the license state is displayed on the license management page.
    b. Green indicates that the license is valid and active.
    c. Yellow indicates that the license components are invalid.
    d. Red indicates that the license is expired.

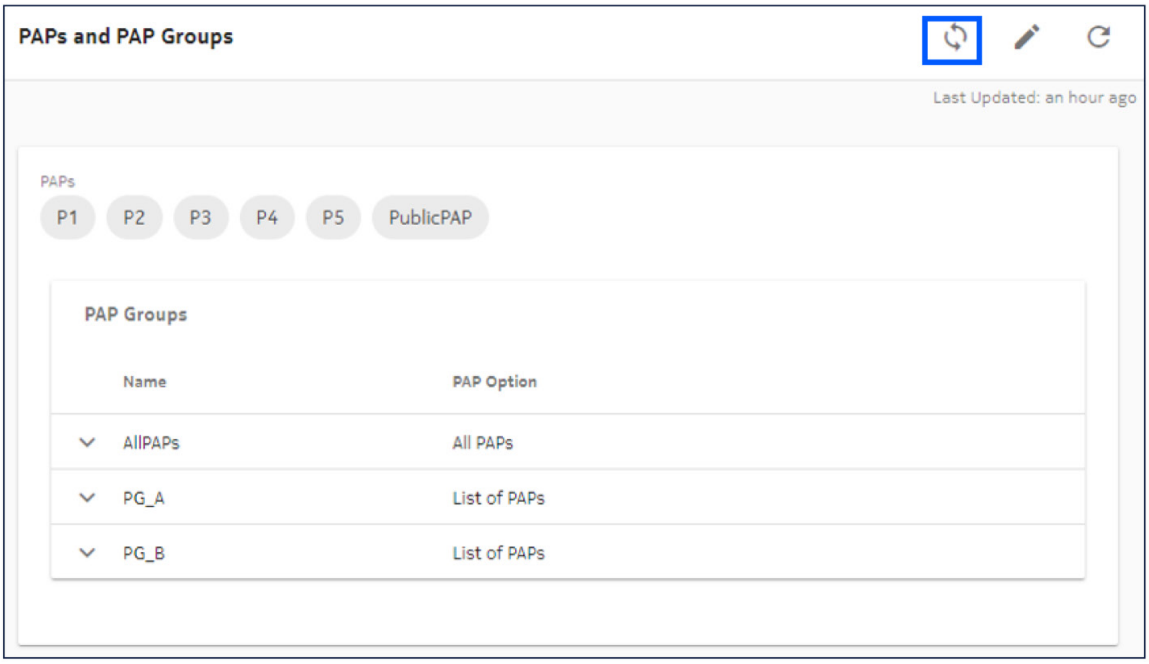
37. Which of the following statements about the function of the Manager Directory Service (MDS) is FALSE?
    a. It receives notifications whenever there is a change in the device manager to devices mapping.
    b. It pushes device configuration when the device becomes reachable.
    c. It periodically synchronizes with device managers to retrieve their managed devices information.
    d. It is required to always keep a device manager to devices mapping up to date.

38. Which of the following statements about device manager synchronization is FALSE?
    a. It retrieves the full device list from the device manager.
    b. It performs an alarm sync of the device manager.
    c. It pushes all the applicable device extensions to the device manager.
    d. It is recommended to trigger this operation periodically to make sure the network is always sync-up.

39. According to the exhibit, which PAP belongs to both the PAP groups PG_A and PG_B?

    a. P1
    b. P2
    c. P3
    d. P4

40. According to the exhibit, which button is highlighted?



a. Edit PAP information
b. Refresh PAP information
c. Synchronization of PAP information with Keycloak
d. Reset PAP information to the default configuration

Answer Key

1. B	11. A	21. B	31. C
2. C	12. A	22. B	32. A
3. B	13. D	23. A	33. A
4. B	14. A	24. C	34. A
5. A	15. D	25. C	35. D
6. C	16. A	26. D	36. C
7. A	17. A	27. C	37. B
8. D	18. A	28. A	38. D
9. B	19. B	29. A	39. B
10. C	20. A	30. B	40. C

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing.

From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in digital health, we are shaping the future of technology to transform the human experience. networks.nokia.com

Nokia Oyj
Karaportti 3
FI-02610 Espoo, Finland
Tel. +358 (0) 10 44 88 000

Document code:CID214164EN (January) CID214508