PassQueen
a.k.a dumpsqueen.com

Qlik Sense System Administrator Certification Exam - June 2018 Release

Qlik QSSA2018

Version Demo

Total Demo Questions: 11

Total Premium Questions: 115

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Qlik Sense Enterprise Architecture	19
Topic 2, Qlik Sense Enterprise Installation	5
Topic 3, Qlik Sense Enterprise Security	49
Topic 4, Qlik Sense Enterprise Administration	23
Topic 5, Qlik Sense Enterprise Monitoring and Troubleshooting	19
Total	115

QUESTION NO: 1

A system administrator must set up security that does NOT allow certain users to create objects in published apps. The users that should NOT be able to create objects are in an AD group called LimitedUsers.

Which security rule should the administrator use to meet this requirement?

A. Resource filter App_*Action CreateRule Condition: (resource, objectType=charts'' and user group='' LimitedUsers'')Context Both in hub and QMC

B. Resource filter App_*Action CreateRule Condition: (resource, objectType=charts'' and user group='' LimitedUsers'')Context: Only in hub

C. Resource filter App_*Action CreateRule Condition: (resource, objectType=charts'' and user group='' LimitedUsers'')Context: Both in hub and OMC

D. Resource filter App_*Action CreateRule Condition: (resource, objectType=charts'' and user group='' LimitedUsers'')Context: Only in hub

E. Resource filter App.Object_*Action CreateRule Condition: resource.app.published = false or user.group != "LimitedUsers"Context: Only in hub

ANSWER: E

Explanation:

The applicable Create permission must be scoped to app objects and must exclude members of `LimitedUsers` when the app is published. Qlik Sense security rules are permissive: a matching rule grants an action; they do not provide a separate deny action that can override another matching grant. Therefore, the administrator should amend the rule that grants creation of app objects, or ensure no other Create rule grants this access, so its condition allows creation in unpublished apps while allowing creation in published apps only for users outside the restricted AD group. The resource filter `App.Object_*` targets app objects rather than only chart objects, covering the relevant object-creation capability. The Hub is the appropriate context because users create sheets and visualizations in apps through the Qlik Sense hub. The condition `resource.app.published = false or user.group != "LimitedUsers"` preserves normal object creation for unpublished apps and prevents the specified group from receiving Create access in published apps. Qlik recommends carefully reviewing overlapping security rules because access is granted when a rule permits the action. See the Qlik Sense security rules documentation and security-rule expression documentation.

QUESTION NO: 2

A multi-node Qlik Sense site has a dedicated scheduler node. A reload task that uses an ODBC connection fails because the required database driver is installed only on the central node.

Which three actions should the system administrator take? (Choose three.)

A. Install the required 64-bit ODBC driver on the scheduler node

B. Create the required system DSN on the scheduler node

C. Grant the Qlik Sense service account access to the database

D. Install Qlik Sense Desktop on the scheduler node

E. Configure the connection to use the central node local drive

ANSWER: A B C

Explanation:

The scheduler node executes the reload, so it must have the required 64-bit ODBC driver installed. If the connection depends on a system DSN, that DSN must also be created and configured on the scheduler node because system DSNs are local to each Windows server.

The identity used by the Qlik Sense services on the scheduler node must be authorized to access the database. Installing or testing the driver only on the central node does not make it available to a reload that executes on another node. See Qlik Sense data connections documentation.

QUESTION NO: 3

A system administrator has to set up three physical servers and one virtual server for a new Qlik Sense Enterprise environment. Four separate nodes are required.

The physical servers have 32 GB of RAM. The virtual server has 8 GB of RAM.

Which node should be virtualized?

A. Proxy

B. Scheduler/Reload

C. Central

D. Engine

ANSWER: A

Explanation:

Proxy is the appropriate role for the virtual server with 8 GB of RAM. In a four-node Qlik Sense Enterprise deployment, the Central node, Scheduler/Reload node, and Engine node should receive the higher-capacity physical servers because they host the services most dependent on memory and compute resources. The Engine service performs associative calculations and manages in-memory application data for user sessions, while reload operations can consume substantial memory and processor capacity as data is extracted, transformed, and loaded. The Central node coordinates the deployment and hosts core management services, so it should also be placed on a reliable, suitably provisioned server.

The Proxy service primarily accepts client connections and routes authenticated requests to the appropriate Qlik Sense services. Although its capacity must be sized for expected concurrent connections and network throughput, it does not carry the same in-memory analytics or reload-processing workload as the Engine and Scheduler/Reload roles. Consequently, using the lower-memory virtual machine for the Proxy role preserves the three 32 GB physical servers for the more resource-intensive services. This role separation also supports predictable performance and makes future scaling of proxy capacity straightforward. Qlik's deployment-planning guidance discusses sizing infrastructure according to deployed services and workload: Qlik deployment planning. For service-role architecture, see Qlik Sense Enterprise architecture.

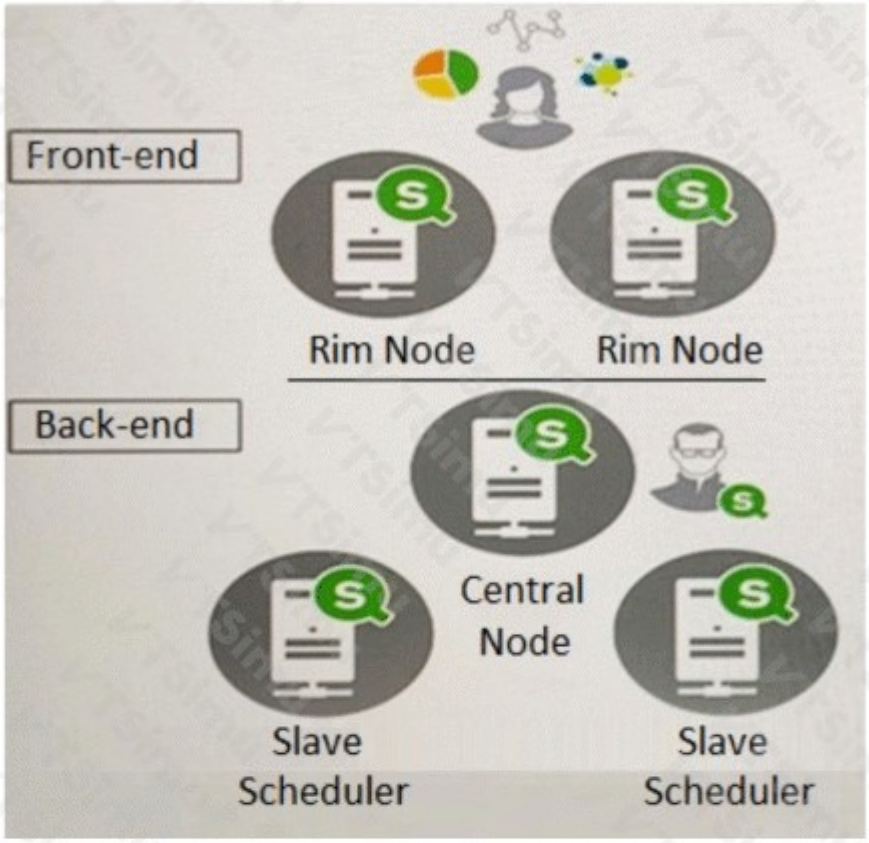
QUESTION NO: 4

A system administrator must design a Qlik Sense server architecture that meets the following requirements:

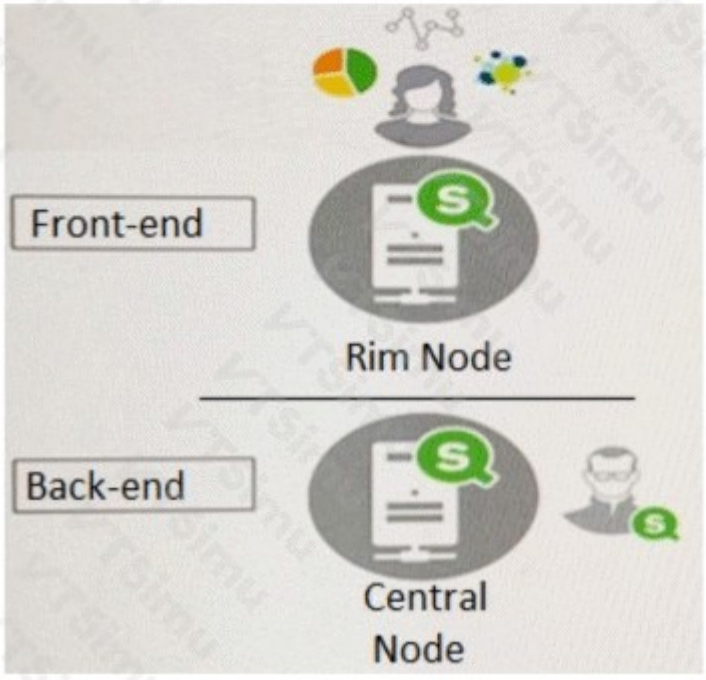
- Approximately 1000 users will be using apps
- Apps are reloaded outside of office hours
- The total size of data in all apps will be approximately 600 million rows
- Apps must be available 24/7

Which architecture meets these requirements in the most cost efficient way?

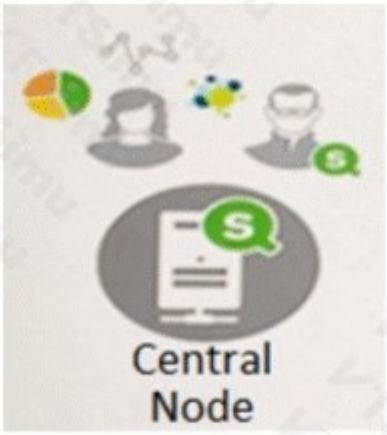
A.


Front-end
Rim Node
Rim Node
Back-end
Central
Node
Slave
Scheduler
Slave
Scheduler

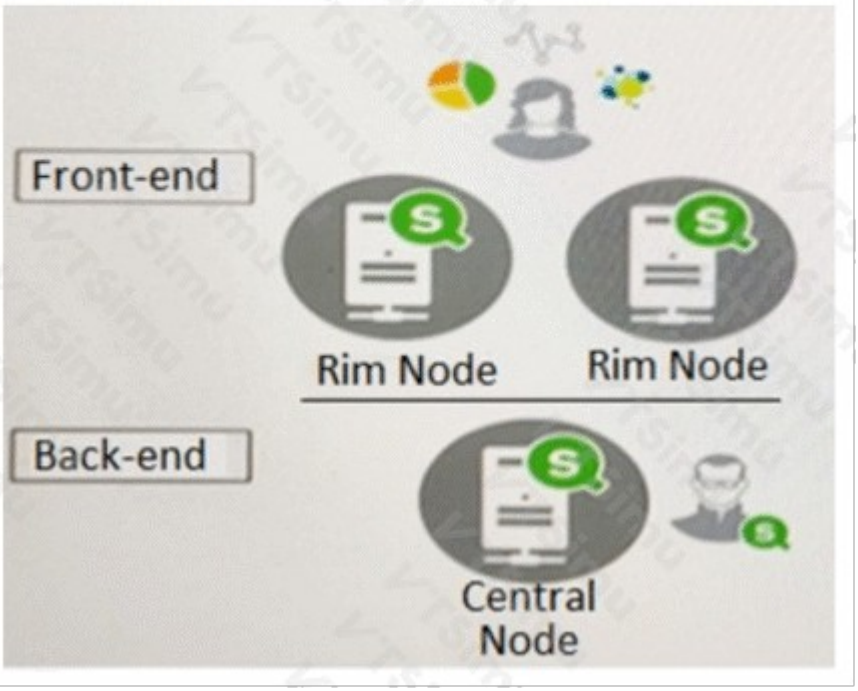
B.


Front-end
Rim Node
Back-end
Central
Node

C.



D.



A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: D

Explanation:

The architecture shown in the selected diagram is appropriate because it separates the workload that must remain continuously available from the resource-intensive reload workload, while avoiding unnecessary infrastructure. With approximately 1,000 users, the environment needs sufficient engine capacity to serve concurrent interactive sessions and sufficient resilience so that app access is not interrupted by scheduled data reloads or a single node becoming unavailable. Reloads occur outside office hours, so dedicated reload capacity can be sized for the batch window rather than duplicated across every user-facing node. This is a cost-efficient design because it targets additional hardware at the two distinct workload types instead of overprovisioning all nodes for both peak user activity and reload processing.

Qlik Sense Enterprise on Windows supports multi-node deployments, where nodes can be assigned roles and workload capabilities to distribute consumption and reload activity. Shared persistence is also central to a multi-node site, allowing services to access the same governed apps and content. This design supports 24/7 app availability by retaining user-serving capacity while scheduled reloads are processed separately. Qlik's deployment guidance and node-management documentation provide the relevant principles for planning capacity, roles, and workload distribution: Qlik Sense deployment planning and Managing Qlik Sense nodes.

QUESTION NO: 5

A system administrator must make sure that only members of the "Dov" Active Directory group have the Work stream and are able to create Qlik Sense apps.

The administrator creates a security rule that only allows member of the "Dov" group to create apps. but other users can still see the Personal Work area and are able to create apps

What is the cause of this issue?

A. The security rules are corrupted

B. The default security rule tor app creation is enabled

C. The Create app functionality is disabled for "Dev" group

D. Security rules do NOT impact the Work stream

ANSWER: B

Explanation:

The default security rule tor app creation is enabled. In Qlik Sense Enterprise on Windows, security rules are permissive: a user receives access when at least one applicable rule grants the requested action. Creating a new rule that grants app-creation rights only to members of the specified Active Directory group does not override another enabled rule that already grants the same Create action to a broader user population. The built-in app-creation rule normally allows authenticated users to create apps in their personal work area, so it continues to authorize users outside that group.

To enforce the intended restriction, the administrator must review the rules applying to the App resource and the Create action, then disable or modify the broad default app-creation rule as appropriate. The replacement rule should explicitly grant app creation to the required directory group and should be tested using the security-rule audit tools before deployment. Qlik's documentation describes how rules are evaluated and how access is granted through applicable security rules: Managing security rules. The documented default rules should also be reviewed before changing access behavior: Default security rules.

QUESTION NO: 6

A Qlik Sense deployment is planned for 200 users initially. Within a year, the number of users will grow to 2000, with over 100 apps. Most of these users will be the organization's firewall. There are plans to eventually allows access to some apps to users outside the firewall.

Which two deployment modes will ensure secure access to Qlik Sense apps to users outside the firewall.

Which two deployment models will ensure secure access to Qlik Sense apps by authorized users outside the firewall? (Select two.)

A. Deploy a reverse proxy in the DMZ and configure it to forward all Qlik Sense traffic to the Qlik Sense servers on the corporate network.

B. Enable all external users to connect to the corporate network via a secure VPN to access Qlik Sense apps.

C. Deploy Qlik Sense in the DMZ and open all required ports to internal and external users.

D. Deploy Qlik Sense in the corporate network, open all required firewall, and allow external users to access apps directly.

E. Configure Qlik Sense in 'off-line mode' for external users and allow then to access apps locally

ANSWER: A B

Explanation:

Deploying a reverse proxy in the DMZ and configuring it to forward Qlik Sense traffic to Qlik Sense servers on the corporate network is a secure perimeter design. The reverse proxy is the only component exposed to internet-facing users, while the

Qlik Sense services, applications, repositories, and data remain protected inside the corporate network. The proxy can terminate TLS, enforce authentication, and route only the required HTTP and WebSocket traffic to the appropriate Qlik Sense virtual proxy. This supports controlled external access without directly exposing Qlik Sense back-end services.

Enabling external users to connect through a secure VPN is also an appropriate secure-access model. A VPN establishes an authenticated, encrypted connection to the corporate network before the user accesses Qlik Sense. After connecting, authorized users can reach Qlik Sense through the same protected internal access path and identity controls used by internal users. This approach is especially suitable when external access is limited to known users such as employees or trusted partners and when the organization already operates VPN access with suitable endpoint and authentication policies.

Qlik's deployment guidance describes the proxy role as the component that handles client connections and routes requests to Qlik Sense services. See Qlik Sense Proxy Service documentation and Qlik Sense deployment planning documentation.

QUESTION NO: 7

A source app is published to the Operations stream. The source app reloads successfully every night, but users of the published app continue to see data from the previous week.

Which two actions should the system administrator take to update the published app? (Choose two.)

A. Reload the source app successfully

B. Replace the published app with the updated source app

C. Reload the published app directly from the hub

D. Create a new stream for every updated version of the app

E. Export the published app and import it as a new source app

ANSWER: A B

Explanation:

A published app is a managed copy of its source app. Reloading the source app updates the data in that source app, but it does not automatically update the published copy that users open in the stream. The administrator must replace the published app with the updated source app after the source app reload has completed successfully.

The Replace operation updates the published app while retaining it as managed content in its stream. Reloading only the source app does not refresh the published copy, and publishing a separate app can create unnecessary duplicate content in the stream. See Publishing apps in Qlik Sense.

QUESTION NO: 8

A system administrator configures a virtual proxy with a session inactivity timeout of 30 minutes.

A user opens an app, closes the browser without logging out, and does not return to Qlik Sense.

What will occur after 30 minutes of inactivity?

A. The user session is terminated and the user must authenticate again

B. The app is automatically unpublished from its stream

C. The Qlik Sense Engine service restarts

D. The user is permanently disabled in the QMC

ANSWER: A

Explanation:

The user session is terminated after the configured inactivity period. The session inactivity timeout is a virtual proxy setting that controls how long an inactive browser session can remain valid. Closing a browser does not necessarily terminate a Qlik Sense session immediately, but the inactivity timeout causes the Proxy service to end the session after the specified interval.

This setting helps release resources associated with abandoned sessions and requires the user to authenticate again when returning after the timeout. See Qlik Sense virtual proxy documentation.

QUESTION NO: 9

A system administrator is installing and configuring a new Qlik Sense deployment. The system administrator completes the following steps: ▪ Makes sure the IT-provisioned server, named Server1, meets the required specifications

- Installs Qlik Sense on Server1
- Tests the installation by opening Qlik Sense from the server desktop shortcut
- Modifies default virtual proxy prefix to “qliksense”
- Creates a new virtual proxy for users with a prefix of “QSE”
- Links the new virtual proxy to the central proxy
- Configures the new virtual proxy to load balance with the central node
- Configures the new virtual proxy host white list with the server name, FQDN, and server IP address

When the system administrator tests the new virtual proxy using the URL, http://Server1/sense/hub, this error message displays:

Error 404 The requested resource cannot be found

What is causing this error?

A. The new central proxy was NOT created

B. The incorrect virtual proxy was used in the test

C. The new virtual proxy is configured incorrectly

D. The central proxy was NOT configured correctly

ANSWER: B

Explanation:

The incorrect virtual proxy was used in the test. A virtual proxy prefix is a required path segment in the URL used to access Qlik Sense through that virtual proxy. In this deployment, the original default virtual proxy prefix was changed from the empty/default path to `qliksense`, and a separate virtual proxy was created with the prefix `QSE`. Therefore, the request `http://Server1/sense/hub` targets a path for a virtual proxy prefix named `sense`, which was not configured. Because Qlik Sense cannot resolve that requested proxy path, the proxy returns a 404 response.

To test the newly created virtual proxy, the administrator should use its configured prefix in the URL, such as `http://Server1/QSE/hub`. To access the modified default virtual proxy, the corresponding path would be `http://Server1/qliksense/hub`. Qlik documentation describes virtual proxy prefixes as the URI path used for access and notes that the prefix forms part of the URL used by clients. See Qlik Sense virtual proxy documentation and Qlik Support article 000009039.

QUESTION NO: 10

A system administrator needs to troubleshoot an issue reported with Qlik Sense. The administrator confirms the following.

* NO hardware issues exist

* NO other process are affecting Qlik Sense

* NO other systems report any issues

* The network team reports optimal performance

The system administrator decides to check the task execution details and token allocations Which two tools should the system administrator use? (Select two)

A. Log Monitor

B. Sessions Monitor

C. Operations Monitor

D. Reloads Monitor

E. License Monitor

ANSWER: D E

Explanation:

Reloads Monitor is the appropriate monitoring application for examining task execution details. It provides administrators with reload-task information such as task status, execution history, duration, start and finish times, and failures. This allows the administrator to investigate whether the reported Qlik Sense issue is connected to scheduled or manually initiated reload activity, including identifying unsuccessful reloads or abnormal execution times. **License Monitor** is the appropriate application for checking token allocations. In Qlik Sense Enterprise deployments using token-based licensing, it provides visibility into license allocation and consumption, helping an administrator determine how tokens have been assigned and whether licensing capacity or allocation patterns could affect access. Together, these monitoring apps directly address the two stated investigation areas: reload-task execution and licensing-token allocation. Qlik documents the supplied monitoring apps as administrative tools for observing operational and license-related usage data. See the Qlik Sense monitoring apps documentation and Qlik's license management documentation.

QUESTION NO: 11

A system administrator needs to troubleshoot an issue reported with Qlik Sense. The administrator confirms the following: ▪ NO hardware issues exist

- NO other processes are affecting Qlik Sense
- NO other systems report any issues
- The network team reports optimal performance

The system administrator decides to check the task execution details and token allocations.

Which two tools should the system administrator use? (Choose two.)

A. Log Monitor

B. Sessions Monitor

C. Operations Monitor

D. Reloads Monitor

E. License Monitor

ANSWER: D E

Explanation:

Reloads Monitor is the appropriate monitoring application for reviewing task execution details. It provides administrators with visibility into reload-task activity and outcomes, allowing them to investigate task status, execution history, duration, failures, queued work, and related reload behavior. This information is central when the reported issue may involve application reload processing rather than infrastructure, network, or external-system performance.

License Monitor is the appropriate application for investigating token allocations. Qlik Sense monitoring apps expose license-consumption information so an administrator can review allocation and usage patterns, identify the users or entities consuming tokens, and assess whether licensing availability or allocation behavior is relevant to the reported issue. Reviewing this data helps distinguish a workload problem from a licensing or access-consumption concern.

These two monitoring apps directly align with the stated investigation: one addresses operational reload-task execution, while the other addresses license-token allocation. Qlik documents the supplied monitoring applications and their administrative purpose in its monitoring-app guidance. See Qlik Sense monitoring apps and Reloads Monitor.