

Tableau Certified Architect

Tableau TCA-C01

Version Demo

Total Demo Questions: 15

Total Premium Questions: 152

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Design	54
Topic 2, Installation and Configuration	20
Topic 3, Security	33
Topic 4, Monitoring and Maintenance	21
Topic 5, Troubleshooting	24
Total	152

QUESTION NO: 1

In the context of Tableau Cloud, what is a key benefit of implementing automated user provisioning using SCIM?

- A. Eliminating the need for any user authentication mechanisms in Tableau Cloud
- B. Reducing the administrative overhead associated with manual user account management and improving security
- C. Allowing users to bypass organizational identity verification processes for quicker access to Tableau Cloud
- D. Integrating SCIM solely for tracking user activity and not for managing user accounts

ANSWER: B

Explanation:

Reducing the administrative overhead associated with manual user account management and improving security is a key benefit of SCIM provisioning in Tableau Cloud. System for Cross-domain Identity Management (SCIM) lets an identity provider automate the creation, update, and removal of Tableau Cloud user accounts based on changes managed centrally in the organization's identity system. This avoids repetitive administrative work, helps keep names, email addresses, and account status current, and provides a more dependable process as the organization grows.

Security improves because access can be adjusted or revoked promptly when a person changes roles or leaves the organization. Automated deprovisioning reduces the chance that inactive accounts retain access to Tableau Cloud content, while centralized provisioning supports consistent application of organizational identity and access-management practices. Tableau Cloud supports SCIM in conjunction with single sign-on configurations, allowing identity lifecycle information to flow from the organization's identity provider into the Tableau Cloud site. Tableau recommends planning user authentication and provisioning together so that users, groups, and site roles are administered appropriately. See Tableau's [SCIM provisioning documentation](#) and its [SAML configuration documentation](#) for implementation details.

QUESTION NO: 2

A multinational corporation with various branches worldwide needs to integrate its Tableau Server with its existing corporate identity management system. What is the most appropriate identity store and authentication configuration?

- A. Local authentication for each branch to maintain independent user management
- B. Active Directory with single sign-on (SSO) to integrate with the existing corporate identity management system
- C. Separate identity stores for each region, disregarding the existing corporate identity management system
- D. Manual username and password setup for each user on the Tableau Server

ANSWER: B

Explanation:

Active Directory with single sign-on (SSO) to integrate with the existing corporate identity management system is the appropriate configuration because it allows Tableau Server to use the organization's established directory as its authoritative source for users and groups. In a multinational environment, centralizing identity management in Active Directory supports consistent account lifecycle processes, including provisioning, group-based access administration, password policies, and timely removal of access when employees change roles or leave the company. Tableau Server can be configured to synchronize users and groups from Active Directory, enabling administrators to assign site roles and permissions through existing directory groups rather than managing individual accounts separately in Tableau.

Single sign-on further improves the user experience and security posture by allowing authenticated corporate users to access Tableau Server without repeatedly entering separate Tableau credentials. With an appropriate SSO implementation, Tableau Server relies on the organization's trusted authentication flow while continuing to apply Tableau authorization controls, such as project, workbook, view, and data-source permissions. This approach is especially suitable for globally distributed branches because it aligns Tableau access with the corporation's existing identity governance model and provides a unified, scalable administrative model. Tableau documents Active Directory as an external identity store option and supports SSO-related authentication approaches for enterprise deployments. See [Tableau Server Identity Store](#) and [Tableau Server SAML Authentication](#).

QUESTION NO: 3

When configuring SAML (Security Assertion Markup Language) for authentication in Tableau Server, which of the following steps is essential for successful integration?

- A. Enabling automatic user provisioning within the SAML provider to create Tableau Server accounts
- B. Configuring Tableau Server to redirect all HTTP requests to HTTPS for secure communication
- C. Obtaining and installing an SSL certificate specifically for the SAML provider
- D. Importing the SAML provider's metadata into Tableau Server for proper identity provider configuration

ANSWER: D

Explanation:

Importing the SAML provider's metadata into Tableau Server for proper identity provider configuration is the essential integration step because Tableau Server must have the identity provider's SAML configuration details to establish a trusted SAML relationship. Identity provider metadata is an XML document that supplies values Tableau Server needs for the exchange, including the identity provider entity ID, single sign-on endpoint, and signing certificate information. By importing this metadata during SAML setup, an administrator configures Tableau Server to recognize assertions issued by the trusted identity provider and to validate their signatures. This establishes the technical trust required before users can authenticate through the external provider. Tableau Server's SAML configuration workflow supports importing identity provider metadata directly, which reduces transcription errors and ensures endpoint and certificate details are populated from the provider's published configuration. Administrators must also ensure that the identity provider is configured with Tableau Server's service-provider details, such as its assertion consumer service URL and entity ID, so that authentication responses are delivered to the correct Tableau Server endpoint. Tableau's configuration guidance is available in the [Tableau Server SAML documentation](#), and general SAML metadata concepts are described by [OASIS SAML Metadata](#).

QUESTION NO: 4

A Tableau Cloud site uses Tableau Bridge to refresh extracts from a private-network database. Refreshes fail intermittently after the organization introduced a network policy that places Bridge client machines into sleep mode overnight. What is the most appropriate remediation?

- A. Run Bridge clients on always-on managed machines and prevent sleep during refresh windows
- B. Change permissions on the affected Tableau Cloud workbooks
- C. Require analysts to upload refreshed extracts manually each morning
- D. Install Tableau Bridge on each analyst's laptop

ANSWER: A

Explanation:

Running the Bridge clients on always-on managed machines and preventing sleep during scheduled refresh windows is the correct remediation. Tableau Bridge must be running and able to reach both Tableau Cloud and the private-network data source when an assigned refresh is due. A client that is asleep or unavailable cannot execute the refresh task.

Changing workbook permissions does not restore network connectivity. Manual extract uploads remove the managed refresh capability, and installing Bridge on analysts' laptops would reduce reliability rather than provide an operationally supported service.

QUESTION NO: 5

When configuring a coordination ensemble for a Tableau Server cluster, what is the primary purpose of the ensemble?

- A. To store user data and content such as workbooks and data sources
- B. To balance the load among different nodes in the cluster
- C. To manage the election process for the active repository and synchronize cluster configurations
- D. To encrypt data transferred between nodes in the cluster

ANSWER: C

Explanation:

To manage the election process for the active repository and synchronize cluster configurations is correct because the Coordination Service supplies the distributed coordination foundation required by a highly available Tableau Server deployment. Tableau Server uses this service to keep essential cluster state and configuration information available across nodes and to coordinate activities that require a single authoritative decision. A key high-availability responsibility is supporting repository failover: when the active repository becomes unavailable, the cluster can use coordinated state to select and promote an eligible passive repository. The ensemble also helps Tableau Server components maintain a consistent view of the cluster, which is necessary for reliable service operation as nodes communicate and recover from failures. For fault tolerance, Tableau recommends an odd-numbered Coordination Service ensemble, typically three instances, so the service can maintain quorum if an instance fails. This makes the ensemble a core control-plane component for cluster consistency and repository availability rather than a workload-processing component. Tableau's documentation describes the Coordination Service as the mechanism used to coordinate processes and maintain configuration data in distributed deployments, including high-availability configurations. See [Configure a Coordination Service ensemble](#) and [Tableau Server high availability](#).

QUESTION NO: 6

If a performance recording indicates that query response times from external databases are the primary bottleneck in Tableau Server, what should be the first course of action?

- A. Upgrading the external database servers for faster processing
- B. Reviewing and optimizing the database queries used in Tableau workbooks for efficiency
- C. Implementing caching mechanisms in Tableau Server to reduce the reliance on database queries
- D. Restricting the size of data extracts to lessen the load on the external databases

ANSWER: B

Explanation:

Reviewing and optimizing the database queries used in Tableau workbooks for efficiency is the appropriate first action because the performance recording has isolated time spent waiting for the external database as the dominant source of latency. Tableau Server sends queries to the underlying data source based on workbook design, calculations, filters, joins, relationships, and the amount and granularity of data requested. Examining the affected workbook queries and their database execution plans allows an administrator and database team to identify opportunities such as reducing unnecessary fields or rows, improving filters, simplifying calculations, ensuring appropriate indexes exist, and correcting inefficient joins or custom SQL. This evidence-based approach targets the measured bottleneck directly before broader capacity or architectural changes are considered. Tableau performance recordings are intended to help identify which activities consume time during workbook interaction, including query execution, so the remediation can be focused on the component responsible for the delay. Tableau also recommends optimizing workbooks and data-source interactions as part of systematic performance troubleshooting. See Tableau's guidance on [creating and interpreting performance recordings](#) and its [Tableau Server performance tuning guidance](#).

QUESTION NO: 7

In a multi-node Tableau Server environment, you are experiencing intermittent database connectivity issues. What should be the first step in troubleshooting this problem?

- A. Increasing the number of worker nodes in the Tableau Server environment to enhance overall connectivity
- B. Checking the network configuration and firewalls between the Tableau Server nodes and the database server for any connectivity barriers
- C. Upgrading the database server's hardware to improve its ability to handle connections
- D. Changing the database server to a different platform that is known for more stable connectivity

ANSWER: B

Explanation:

Checking the network configuration and firewalls between the Tableau Server nodes and the database server for any connectivity barriers is the appropriate first step because intermittent database connectivity usually indicates a communication-path issue that must be isolated before changing capacity or infrastructure. In a multi-node deployment, every relevant Tableau Server node that runs processes connecting to the database must be able to consistently resolve the database hostname and reach the database listener on its required port. Review firewall rules, routing, DNS resolution, network timeouts, load balancers or proxies where applicable, and any packet loss or latency occurring between nodes and the database host. Testing connectivity from each affected node helps identify whether the condition is node-specific or shared across the environment. Tableau's troubleshooting guidance also emphasizes checking connectivity and validating the data connection when investigating database connection errors. Establishing a stable network path first provides the evidence needed to determine whether further investigation should focus on database availability, credentials, drivers, or Tableau Server processes. See Tableau's [data source troubleshooting documentation](#) and its [Tableau Server processes overview](#).

QUESTION NO: 8

An organization has tested restoration of a Tableau Server backup on replacement infrastructure. The restored content is present, but several custom server settings are absent. What should be added to the disaster recovery runbook?

- A. Add a separate export and secure retention process for Tableau Server configuration and required external dependencies.
- B. Increase the frequency of extract refreshes after the backup has been restored.
- C. Store all Tableau Server backups on the replacement server to reduce restoration time.
- D. Recreate missing configuration manually from administrator memory after each recovery event.

ANSWER: A

Explanation:

The runbook should include exporting and securely retaining the Tableau Server configuration separately from the Tableau Server backup. A backup protects Tableau Server data such as repository and file-store content, but a complete recovery design must also preserve the configuration needed to recreate the intended server behavior. Maintaining configuration exports, certificates, identity-provider details, and documented external dependencies allows replacement infrastructure to be configured consistently before or during restoration. Re-running extract refreshes does not restore missing server settings.

QUESTION NO: 9

During the installation of Tableau Server on a Windows system, you encounter a permissions error. What should be your initial action to address this issue?

- A. Disabling User Account Control (UAC) on the Windows system
- B. Checking and adjusting the security permissions of the Tableau Server installation directory
- C. Granting administrator privileges to all user accounts on the Windows system

D. Reinstalling the Windows operating system to reset system permissions

ANSWER: B

Explanation:

Checking and adjusting the security permissions of the Tableau Server installation directory is the appropriate initial action because a permissions error commonly means that the account running the installer cannot create, modify, or access required files and folders. Tableau Server installation requires appropriate Windows administrative rights and access to the locations used by the installation process. Confirm that the installer is being run by an authorized local administrator and that the intended installation location grants the required access to that account. If a non-default installation path is used, its inherited and explicit NTFS permissions should also be reviewed carefully before proceeding. Addressing the directory-level access issue directly follows the principle of least privilege: it restores only the access necessary for installation rather than making broad, system-wide security changes. Tableau's installation guidance identifies Windows administrative requirements and describes the prerequisites that must be met before installing Tableau Server. Reviewing the relevant setup requirements and validating directory access before retrying the installation provides a targeted, supportable resolution path. See Tableau's [Tableau Server installation requirements](#) and [Windows installation guidance](#).

QUESTION NO: 10

A large retail company with a high volume of daily Tableau users requires a configuration that optimizes query performance and user experience. Which configuration setting should be prioritized?

- A. Decrease the "vizqlserver.session.expiry.timeout" value to reduce session timeouts
- B. Increase the "backgrounder.querylimit" value to allow more concurrent queries
- C. Reduce the "cache.server.timeout" value to lower the caching time
- D. Increase the "vizqlserver.querylimit" value to allow more concurrent queries

ANSWER: D

Explanation:

Increase the "vizqlserver.querylimit" value to allow more concurrent queries is the appropriate priority when a Tableau Server deployment must support substantial interactive demand. VizQL Server is the Tableau Server process responsible for rendering views and managing the interactive requests generated as users open, filter, and explore workbooks. The query limit controls the number of queries a VizQL Server process can run concurrently. Where monitoring demonstrates that this limit is constraining otherwise healthy VizQL capacity, increasing it can reduce queuing for interactive requests and help maintain a responsive user experience during periods of high usage. This setting should be sized deliberately: the server must have sufficient CPU, memory, database capacity, and data-source capacity to process the additional concurrent query load effectively. It is therefore best used alongside workload monitoring and capacity testing, rather than as an unconditional increase. Tableau documents VizQL Server configuration settings, including query-concurrency controls, in its [TSM configuration reference](#). For broader sizing, process topology, and performance planning guidance, consult Tableau's [Performance and Scalability documentation](#).

QUESTION NO: 11

For a large-scale Tableau Server deployment, what is the most effective strategy for collecting and analyzing server process metrics to maintain optimal performance?

- A. Focusing solely on the analysis of CPU and memory usage metrics during peak hours
- B. Implementing a comprehensive monitoring tool that tracks a range of metrics, including C. CPU, memory, disk I/O, and network activity, across different times
- C. Manually checking server performance metrics at the end of each day
- D. Relying on user feedback to determine when to check specific server process metrics

ANSWER: B

Explanation:

Implementing a comprehensive monitoring tool that tracks CPU, memory, disk I/O, and network activity across different times is the most effective approach because Tableau Server performance depends on the interaction of several processes, services, and underlying infrastructure resources. Collecting data continuously rather than at isolated moments establishes a baseline for normal behavior and makes it possible to recognize trends, recurring workload patterns, and resource saturation before they become user-facing incidents. This broad view is especially important in large deployments, where workload spikes can affect background processing, interactive views, extracts, repository activity, and network-dependent communication differently. Tableau Server provides administrative views that expose server activity and performance information, while external enterprise monitoring can correlate Tableau process behavior with operating-system and infrastructure metrics. Combining these sources supports proactive capacity planning, targeted troubleshooting, and validation that tuning changes have the intended effect. Tableau recommends using its built-in administrative views to understand server usage and performance: [Tableau Server Administrative Views](#). For guidance on monitoring Tableau Server health and performance, see [Tableau Server Performance](#).

QUESTION NO: 12

When configuring Tableau Server on Linux to interact with an external email server for notifications, you encounter issues with email delivery. What is the first thing you should check to resolve this issue?

- A. The email content and formatting settings in Tableau Server
- B. The SMTP configuration settings in Tableau Server, including server address and port
- C. Upgrading the email server to a version that is compatible with Tableau Server
- D. Changing the Tableau Server's operating system to one that is more compatible with the email server

ANSWER: B

Explanation:

The SMTP configuration settings in Tableau Server, including server address and port, should be checked first because Tableau Server sends notification emails through the SMTP service defined in Tableau Server Manager (TSM). Successful delivery depends on Tableau Server being able to reach the configured SMTP host on the specified port and use settings that the mail server accepts. Confirm the SMTP server's fully qualified host name or IP address, port, encryption method, authentication account and password where required, and the configured sender address. These values must align with the external mail server's connection and relay policies. After updating SMTP configuration through TSM, apply the pending changes so that Tableau Server services use the new settings. Tableau also provides commands to test SMTP connectivity, allowing an administrator to validate communication from the Tableau Server environment before investigating more specialized mail-server behavior. This makes SMTP configuration and connectivity the appropriate starting point for troubleshooting notification delivery. See Tableau's [Configure SMTP Setup](#) documentation and its [Tableau Services Manager reference](#) for the relevant configuration workflow and commands.

QUESTION NO: 13

A Tableau Server deployment has acceptable Backgrounder throughput, but interactive users experience slow rendering during peak business hours. Monitoring shows sustained CPU saturation on the nodes hosting VizQL Server processes, while other nodes have available capacity. Which change is most appropriate?

- A. Add Backgrounder processes to the nodes with saturated CPU
- B. Add VizQL Server capacity on nodes with available resources
- C. Move all Tableau Server processes to the initial node
- D. Reduce the number of repository instances in the deployment

ANSWER: B

Explanation:

Adding VizQL Server capacity on nodes with available resources is the most appropriate change because the evidence identifies interactive rendering capacity, rather than background processing, as the constrained workload. VizQL Server processes handle interactive view requests, calculations, and rendering. Increasing their capacity and ensuring that the load balancer can route requests to the additional nodes addresses the measured bottleneck.

Adding Backgrounder processes would not resolve interactive rendering saturation, and increasing processes indiscriminately on already saturated nodes could worsen resource contention. The topology should be validated after the change by reviewing response times, CPU utilization, and VizQL workload distribution.

QUESTION NO: 14

In developing a load testing strategy for Tableau Server, what aspect is important to include to ensure comprehensive testing?

- A. Testing the server with a single, high-usage dashboard to see its performance under stress
- B. Simulating a variety of user activities, such as viewing dashboards, publishing workbooks, and refreshing extracts
- C. Exclusively testing the data source connection speeds to determine the overall server performance
- D. Running the tests only with administrative users to evaluate the server's response to privileged activities

ANSWER: B

Explanation:

Simulating a variety of user activities, such as viewing dashboards, publishing workbooks, and refreshing extracts, is essential because a meaningful Tableau Server load test must represent the mix of work performed in the actual deployment. Different activities exercise different Tableau Server processes and resources: interactive dashboard viewing can create concurrent VizQL rendering and query demand; publishing can use background and repository-related resources; and extract refreshes create Backgrounder workload while also placing demand on data sources and disk I/O. Including representative user roles, content complexity, concurrency levels, schedules, and realistic think times helps establish whether the environment can meet expected performance and capacity requirements under normal and peak usage. Tableau's performance-testing guidance recommends defining representative workloads based on how users interact with the server, then measuring behavior as load is increased. This approach provides evidence for capacity planning and configuration decisions because it evaluates the whole operational workload rather than one isolated operation. See Tableau's [Performance and scalability guidance](#) and its [Tableau Server processes reference](#) for how interactive views, background jobs, and other activities use server resources.

QUESTION NO: 15

A deployment pipeline must publish approved workbook versions to Tableau Server without storing an administrator password in source-control files. The automation must use a supported, revocable identity that can be limited to the required publishing activities. Which approach is most appropriate?

- A. Use a dedicated automation identity with a securely stored personal access token
- B. Embed a Site Administrator password in the publishing script
- C. Require an administrator to complete browser authentication for every deployment
- D. Use a shared operating-system account as the Tableau Server API credential

ANSWER: A

Explanation:

Using a dedicated automation identity with a securely stored personal access token is the most appropriate approach. Personal access tokens provide a supported way for scripts to authenticate to Tableau Server without embedding an account password. The token can be stored in an enterprise secret-management system, associated with a dedicated account, and revoked or rotated when required.

Using a site administrator's password in a script creates unnecessary exposure and ties automation to a personal credential. Interactive browser sign-in cannot support unattended publishing, and a shared local operating-system account does not provide Tableau Server API authentication.