



Vendor: Salesforce

Exam Code: Analytics-Admn-201

Exam Name: Salesforce Certified Tableau Server

Administrator

Version: DEMO

QUESTION 1

What Tableau Server authentication method should you configure to use OpenID Connect?

- A. Local Authentication
- B. Kerberos
- C. Active Directory
- D. SAML

Answer: D

Explanation:

Tableau Server supports multiple authentication methods, including Local Authentication, Active Directory, Kerberos, SAML, and OpenID Connect. OpenID Connect (OIDC) is an identity layer built on OAuth 2.0, commonly used for single sign-on (SSO). In Tableau Server, OIDC is implemented as a variant of SAML (Security Assertion Markup Language) authentication because both are SSO protocols managed through the same configuration workflow.

To use OpenID Connect:

Configure Tableau Server for SAML/SSO.

Provide an OIDC-compatible identity provider (IdP) configuration (e.g., Google, Okta).

Set up the IdP metadata and certificates in TSM.

Option D (SAML): Correct. Tableau Server treats OIDC as a subset of its SAML authentication framework, so you configure it under the SAML settings in TSM.

QUESTION 2

A new engineer reports that he is unable to log on to Tableau Services Manager (TSM) from the initial node of a Windows test cluster. Which account credentials should you instruct the engineer to use?

- A. An account with a Creator site role
- B. An account with a Site Administrator role
- C. An account with administrative rights to the computer
- D. An account for the Tableau Server administrator

Answer: C

Explanation:

Tableau Services Manager (TSM) is the administrative tool for managing Tableau Server's configuration, processes, and topology. To log in to TSM (via the web UI at <https://<server>:8850> or CLI), you need:

TSM administrator credentials: These are distinct from site roles and are set during installation or reset via `tsm reset`.

Local administrative rights: On Windows, the account used to access TSM must be in the local Administrators group on the initial node, as TSM interacts with system-level services. In a test cluster, the engineer's inability to log in suggests they lack either the correct TSM credentials or sufficient OS-level permissions. Since the question focuses on a Windows environment and "initial node," the most immediate requirement is local administrative rights to run TSM commands or access the UI.

Option C (An account with administrative rights to the computer): Correct. The engineer must use an account in the local Administrators group on the initial node to authenticate to TSM. After that, they'll need the TSM admin username/password set during installation.

QUESTION 3

If a user already exists as part of a group in Tableau Server, and Active Directory synchronization then applies a minimum site role to the group, what will happen to the existing user's site role?

- A. It will change to the minimum site role only if the minimum site role reduces access
- B. It will change to the minimum site role only if the minimum site role provides more access
- C. It will always change to the minimum site role
- D. It will never change as a result of synchronization

Answer: A

Explanation:

When Tableau Server uses Active Directory (AD) for authentication, group synchronization imports AD groups and assigns a minimum site role (e.g., Viewer, Explorer) to users in that group. This ensures users meet a baseline access level. The behavior for existing users during sync is:

If the user's current site role provides more access than the minimum (e.g., Explorer vs. Viewer), their role remains unchanged.

If the user's current role provides less access than the minimum (e.g., Unlicensed vs. Viewer), their role is upgraded to the minimum.

This preserves higher privileges while enforcing a floor. "Reduces access" means the minimum role is lower than the current role (e.g., Viewer vs. Explorer), in which case the existing role stays.

Option A (It will change to the minimum site role only if the minimum site role reduces access):

Correct. The user's role changes only if the minimum increases access (e.g., Unlicensed to Viewer); otherwise, it stays higher.

QUESTION 4

What command should you run to update the automatically-generated secrets that are created during a Tableau Server installation?

- A. `tsm data-access caching set -r 1`
- B. `tsm licenses refresh`
- C. `tsm security regenerate-internal-tokens`
- D. `tsm security validate-asset-keys`

Answer: C

Explanation:

Tableau Server uses internal secrets (tokens) for secure communication between its processes (e.g., Repository, File Store). These are automatically generated during installation and can be regenerated if compromised or for security maintenance. The command to update these is:

`tsm security regenerate-internal-tokens`: This regenerates the internal security tokens, ensuring all processes use the new tokens after a restart.

Option C (`tsm security regenerate-internal-tokens`): Correct. This is the documented command for updating internal secrets.

QUESTION 5

What are two features of the Tableau Server user-based license? (Choose two.)

- A. A subscription license
- B. Enables distinct user roles
- C. Restricts the number of machine cores you can deploy
- D. A perpetual license

Answer: AB

Explanation:

Tableau Server's user-based licensing model assigns licenses to individual users (Creator, Explorer, Viewer) rather than machines or cores. Key features include:

Subscription license: Licenses are typically subscription-based, renewed annually or monthly, aligning with Tableau's pricing model.

Distinct user roles: It supports three roles (Creator, Explorer, Viewer), each with specific capabilities, enabling granular access control.

Option A (A subscription license): Correct. User-based licenses are subscription-based by default.

Option B (Enables distinct user roles): Correct. The model defines Creator, Explorer, and Viewer roles.

QUESTION 6

You use Tableau Desktop 10.5 and plan to publish a visualization to a Tableau Server that runs version 2020.1. You are assigned the Creator site role, and Publisher permissions for a project. What statement correctly describes what happens when you attempt to publish the visualization?

- A. You will successfully publish the visualization without any errors or warnings
- B. You will see an error message instructing you that you are unable to publish the workbook to a newer version of Tableau Server
- C. You will see a warning message instructing you that embedded .tde extracts will be upgraded to .hyper
- D. You will see a warning message instructing you that the workbook will be upgraded to a new version

Answer: C

Explanation:

Tableau Desktop and Tableau Server have versioning considerations when publishing content, particularly regarding compatibility between older Desktop versions (e.g., 10.5) and newer Server versions (e.g., 2020.1). Let's break this down step-by-step:

Version Context: Tableau Desktop 10.5 was released in 2017 and used the .tde (Tableau Data Extract) format for extracts. Tableau Server 2020.1, released in 2020, introduced the .hyper extract format (starting with version 10.5, but fully standardized later). When publishing from an older Desktop version to a newer Server version, Tableau ensures backward compatibility but may upgrade certain components.

Publishing Process: With a Creator site role and Publisher permissions, you have the rights to publish workbooks to the specified project. Tableau Server accepts workbooks from older Desktop versions (e.g., 10.5) and upgrades them to the current Server version (2020.1) during publishing. This process is seamless for the workbook itself, but extracts require special handling.

Extract Handling: If the workbook contains embedded .tde extracts (stored within the .twb or .twbx file), Tableau Server 2020.1 converts these to .hyper format upon publishing. This conversion is necessary because .hyper replaced .tde as the default extract engine starting in Tableau 10.5 and beyond, offering better performance and scalability. During this process, Tableau Desktop or Server displays a warning to inform the user of the upgrade, as it's a one-way conversion (you can't revert to .tde on the Server).

Option C (Warning: embedded .tde extracts will be upgraded to .hyper): Correct. This is the precise warning displayed when a workbook with .tde extracts is published to a Server version that uses .hyper. It ensures the user is aware of the format change, which might affect extract refresh schedules or performance expectations.

QUESTION 7

Several Tableau Server users published workbooks that have large extracts. After several weeks of use, the users abandoned the workbooks. What should you do to identify the abandoned workbooks?

- A. Use the Stale Content administrative view
- B. Examine the extract files in ProgramData/Tableau/Tableau Server/data/tabsvc/dataengine/extract
- C. Delete all extracts and allow them to be re-generated automatically if they are still in use
- D. View all workbooks, and sort by the Modified date

Answer: A

Explanation:

Abandoned workbooks--those no longer actively used--can clutter Tableau Server and consume resources (e.g., disk space for extracts). Identifying them efficiently requires leveraging built-in administrative tools rather than manual or destructive methods. Let's explore this in depth:

Tableau Server Admin Views: Tableau provides pre-built administrative views to monitor server health, usage, and content. The Stale Content view, accessible under Server > Status > Administrative Views, is specifically designed to identify content (workbooks, data sources) that hasn't been viewed or modified recently. It shows:

Content name, owner, and project.

Last viewed date and last modified date.

View count over a period.

This view uses Repository data to track usage metrics, making it ideal for spotting abandoned workbooks.

Option A (Use the Stale Content administrative view): Correct. This is the most efficient and non-invasive method. You can filter by last viewed date (e.g., >30 days ago) to identify workbooks with large extracts that users have stopped accessing. From there, you can contact owners or delete the content if policy allows. It's a server administrator's go-to tool for content management.

QUESTION 8

Which two statements are advantages of published data sources in comparison to embedded data sources? (Choose two.)

- A. Data is protected so that it is only available in one workbook
- B. Drivers are automatically installed on each client's machine
- C. Centralized data management is easier
- D. Storage space is conserved and resource usage during data refreshes is optimized

Answer: CD

Explanation:

In Tableau, data sources can be embedded (stored within a workbook) or published (stored separately on Tableau Server). Let's define these and analyze the advantages:

Embedded Data Source: The connection details and any extract are bundled in the .twb or .twbx file.

Each workbook manages its own copy.

Published Data Source: The connection or extract is hosted on Tableau Server, reusable across multiple workbooks.

Now, let's evaluate the options:

Option C (Centralized data management is easier): Correct. Published data sources allow:

Single source of truth: One data source can serve multiple workbooks, ensuring consistency.

Unified updates: Refresh schedules, permissions, and metadata (e.g., calculated fields) are managed in one place via the Server UI.

Governance: Administrators can control access and monitor usage centrally. In contrast, embedded data sources require individual updates per workbook, leading to duplication and management overhead.

Option D (Storage space is conserved and resource usage during data refreshes is optimized): Correct. With published data sources:

Storage: A single extract on the Server (e.g., a .hyper file) is shared across workbooks, avoiding redundant copies stored in each embedded workbook.

Refreshes: One refresh job updates the shared extract, reducing CPU and memory usage compared to multiple refreshes for duplicate embedded extracts. Embedded data sources replicate extracts, increasing disk space and refresh load.

QUESTION 9

What two Tableau Services Manager (TSM) processes continue to run when Tableau Server is stopped? (Choose two.)

- A. VizQL Server
- B. License Manager
- C. Backgrounder
- D. Administration Controller

Answer: BD

Explanation:

Tableau Server consists of multiple processes managed by TSM. When you stop Tableau Server (e.g., via `tsm stop`), most application processes halt, but some TSM-specific processes remain active to manage the server's infrastructure. Let's examine each:

TSM Processes: These include the Administration Controller, Administration Agent, and License Manager, which handle configuration, monitoring, and licensing. **Application Processes:** These include VizQL Server, Backgrounder, Data Server, etc., which deliver Tableau's core functionality and stop when the server is stopped.

When `tsm stop` is executed:

The Administration Controller (port 8850) continues running to manage TSM operations (e.g., restarts, status checks).

The License Manager remains active to validate licenses and ensure compliance, even when the server is offline.

Application processes like VizQL Server and Backgrounder shut down, as they're tied to user-facing services.

Option B (License Manager): Correct. It persists to handle licensing tasks, ensuring the server can restart without license issues.

Option D (Administration Controller): Correct. It's the core TSM process, always running to accept commands and manage the server state.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14