



Splunk

Exam Questions SPLK-3002

Splunk IT Service Intelligence Certified Admin Exam

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

There are two departments using ITSI. Finance and Sales. Analysts in each department should not be allowed to see each other's services. What are the role configuration steps required to accomplish this?

- A. itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_analyst.
- B. itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_team_analyst; itoa_sales_analyst, inherited from itoa_team_analyst.
- C. itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_team_analyst.
- D. itoa_finance_admin, inherited from itoa_team_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_analyst.

Answer: C

Explanation:

C is the correct answer because teams are a feature of ITSI that allow you to restrict access to service content in UI views based on user roles. To create separate teams for finance and sales analysts, you need to create custom roles that inherit from the itoa_analyst role, which has read-only access to ITSI content. For example, you can create itoa_finance_analyst and itoa_sales_analyst roles that inherit from itoa_analyst. Then, you need to create custom teams that include these roles and assign them to the relevant services. For example, you can create a finance team that includes the itoa_finance_analyst role and assign it to the finance services. Similarly, you can create a sales team that includes the itoa_sales_analyst role and assign it to the sales services. This way, analysts in each department can only see their own services and not each other's. References: Create teams in ITSI, Assign teams to services in ITSI

NEW QUESTION 2

Which of the following describes default deep dives?

- A. Are manually generated and can be accessed via the Service Analyzer.
- B. Include all KPIs of all services.
- C. Are auto-generated and can be accessed via the Service Analyzer.
- D. Include health scores of all services.

Answer: C

Explanation:

In Splunk IT Service Intelligence (ITSI), default deep dives are auto-generated and can be accessed via the Service Analyzer. Deep dives are an essential feature of ITSI that provide an in-depth, granular view into the health and performance of services and their associated KPIs. These default deep dives are automatically created for each service, allowing users to quickly drill down into the detailed operational metrics and performance data of their services. By accessing these deep dives through the Service Analyzer, ITSI users can efficiently investigate issues, understand service dependencies, and make informed decisions to maintain optimal service health. The auto-generated nature of these default deep dives simplifies the monitoring and analysis process, providing immediate insights into service performance without the need for manual setup or configuration.

NEW QUESTION 3

Which of the following is a best practice when configuring maintenance windows?

- A. Disable any glass tables that reference a KPI that is part of an open maintenance window.
- B. Develop a strategy for configuring a service's notable event generation when the service's maintenance window is open.
- C. Give the maintenance window a buffer, for example, 15 minutes before and after actual maintenance work.
- D. Change the color of services and entities that are part of an open maintenance window in the service analyzer.

Answer: C

Explanation:

It's a best practice to schedule maintenance windows with a 15- to 30-minute time buffer before and after you start and stop your maintenance work.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW>

A maintenance window is a period of time when a service or entity is undergoing maintenance operations or does not require active monitoring. It is a best practice to schedule maintenance windows with a 15- to 30-minute time buffer before and after you start and stop your maintenance work. This gives the system an opportunity to catch up with the maintenance state and reduces the chances of ITSI generating false positives during maintenance operations. For example, if a server will be shut down for maintenance at 1:00PM and restarted at 5:00PM, the ideal maintenance window is 12:30PM to 5:30PM. The 15- to 30-minute time buffer is a rough estimate based on 15 minutes being the time period over which most KPIs are configured to search data and identify alert triggers. References: Overview of maintenance windows in ITSI

NEW QUESTION 4

Which of the following items describe ITSI Deep Dive capabilities? (Choose all that apply.)

- A. Comparing a service's notable events over a time period.
- B. Visualizing one or more Service KPIs values by time.
- C. Examining and comparing alert levels for KPIs in a service over time.
- D. Comparing swim lane values for a slice of time.

Answer: BCD

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/DeepDives>

A deep dive is a dashboard that allows you to analyze the historical trends and anomalies of your KPIs and metrics in ITSI. A deep dive displays a timeline of events and swim lanes of data that you can customize and filter to investigate issues and perform root cause analysis. Some of the capabilities of deep dives are:

* B. Visualizing one or more service KPIs values by time. This is true because you can add KPI swim lanes to a deep dive to show the values and severity levels of one or more KPIs over time. You can also compare KPIs from different services or entities using service swapping or entity splitting.

* C. Examining and comparing alert levels for KPIs in a service over time. This is true because you can add alert swim lanes to a deep dive to show the alert levels

and counts for one or more KPIs over time. You can also drill down into the alert details and view the notable events associated with each alert.

* D. Comparing swim lane values for a slice of time. This is true because you can use the time range selector to zoom in or out of a specific time range in a deep dive. You can also use the time brush to select a slice of time and compare the swim lane values for that time period.

The other option is not a capability of deep dives because:

A. Comparing a service's notable events over a time period. This is not true because deep dives do not display notable events, which are alerts generated by ITSI based on certain conditions or correlations. Notable events are displayed in other dashboards, such as episode review or glass tables.

References: [Overview of deep dives in ITSI], [Add swim lanes to a deep dive in ITSI]

NEW QUESTION 5

Where are KPI search results stored?

- A. The default index.
- B. KV Store.
- C. Output to a CSV lookup.
- D. The itsi_summary index.

Answer: D

Explanation:

Search results are processed, created, and written to the itsi_summary index via an alert action.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch>

D is the correct answer because KPI search results are stored in the itsi_summary index in ITSI. This index is an events index that stores the results of scheduled KPI searches.

Summary indexing lets you run fast searches over large data sets by spreading out the cost of a computationally expensive report over time. References: Overview of ITSI indexes

NEW QUESTION 6

Which of the following describes a realistic troubleshooting workflow in ITSI?

- A. Correlation Search → Deep Dive → Notable Event
- B. Service Analyzer → Notable Event Review → Deep Dive
- C. Service Analyzer → Aggregation Policy → Deep Dive
- D. Correlation search → KPI → Aggregation Policy

Answer: B

Explanation:

A realistic troubleshooting workflow in ITSI is:

? B. Service Analyzer → Notable Event Review → Deep Dive

This workflow involves using the Service Analyzer dashboard to monitor the health and performance of your services and KPIs, using the Notable Event Review dashboard to investigate and manage the notable events generated by ITSI, and using the Deep Dive dashboard to analyze the historical trends and anomalies of your KPIs and metrics.

The other workflows are not realistic because they involve components that are not part of the troubleshooting process, such as correlation search, aggregation policy, and KPI. These components are used to create and configure the alerts and episodes that ITSI generates, not to investigate and resolve them. References: [Service Analyzer dashboard in ITSI], Overview of Episode Review in ITSI, [Overview of deep dives in ITSI]

NEW QUESTION 7

Which of the following is an advantage of an adaptive time threshold?

- A. Automatically alerting when KPI value patterns change over time.
- B. Automatically adjusting thresholds as normal KPI values change over time.
- C. Automatically adjusting to holiday schedules.
- D. Automatically predicting future degradation of KPI values over time.

Answer: B

Explanation:

An adaptive time threshold in the context of Splunk IT Service Intelligence (ITSI) refers to the capability of dynamically adjusting threshold values for Key Performance Indicators (KPIs) based on historical data trends and patterns. This feature allows thresholds to evolve as the 'normal' behavior of KPIs changes over time, ensuring that alerts remain relevant and reduce the likelihood of false positives or negatives. The advantage of this approach is that it accommodates for natural fluctuations in KPI values that may occur due to changes in business operations, seasonality, or other factors, without requiring manual threshold adjustments. This makes the monitoring system more resilient and responsive to actual conditions, improving the overall effectiveness of IT operations management.

NEW QUESTION 8

Which index will contain useful error messages when troubleshooting ITSI issues?

- A. _introspection
- B. _internal
- C. itsi_summary
- D. itsi_notable_audit

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/TroubleshootRE> The index that will contain useful error messages when troubleshooting ITSI issues is:

* B. _internal. This is true because the _internal index contains logs and metrics generated by Splunk processes, such as splunkd and metrics.log. These logs can

help you diagnose problems with your Splunk environment, including ITSI components and features.

The other indexes will not contain useful error messages because:

* A. _introspection. This is not true because the _introspection index contains data about Splunk resource usage, such as CPU, memory, disk space, and so on.

These data can help you monitor the performance and health of your Splunk environment, but not the error messages.

* C. itsi_summary. This is not true because the itsi_summary index contains summarized data for your KPIs and services, such as health scores, severity levels, threshold values, and so on. These data can help you analyze the trends and anomalies of your IT services, but not the error messages.

* D. itsi_notable_audit. This is not true because the itsi_notable_audit index contains audit data for your notable events and episodes, such as creation time, owner

NEW QUESTION 9

Which step is required to install ITSI on a single Search Head?

- A. Untar the ITSI package in <splunk home>/etc/apps
- B. Run splunk_apply shcluster-bundle
- C. Use the Splunk -> Manage Apps Dashboard to download and install.
- D. All of the above.

Answer: C

Explanation:

To install Splunk IT Service Intelligence (ITSI) on a single Search Head, one of the straightforward methods is to use the Splunk Web interface, specifically the "Manage Apps" dashboard, to download and install ITSI. This method is user-friendly and does not require manual file handling or command-line operations. By navigating to "Manage Apps" in the Splunk Web interface, users can find ITSI in the app repository or upload the ITSI installation package if it has been downloaded previously. From there, the installation process is initiated through the Splunk Web interface, simplifying the setup process. This approach ensures that the installation follows Splunk's standard app installation procedures, helping to avoid common installation errors and ensuring that ITSI is correctly integrated into the Splunk environment.

NEW QUESTION 10

When deploying ITSI on a distributed Splunk installation, which component must be installed on the search head(s)?

- A. SA-ITOA
- B. ITSI app
- C. All ITSI components
- D. SA-ITSI-Licensechecker

Answer: B

Explanation:

Install SA-ITSI-Licensechecker and SA-UserAccess on any license master in a distributed or search head cluster environment. If a search head in your environment is also a license

master, the license master components are installed when you install ITSI on the search heads.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallDD>

When deploying ITSI on a distributed Splunk installation, the component that must be installed on the search head(s) is the ITSI app. The ITSI app contains the main features and functionality of ITSI, such as service creation and management, KPI configuration, glass table creation and editing, episode review, deep dives, and so on. The ITSI app also contains some add-ons that provide additional functionality, such as SA-ITOA (IT Operations Analytics), SA-UserAccess (User Access Management), and SA-Utils (Utility Functions). The ITSI app must be installed on the search head(s) because it handles the search management and presentation functions for ITSI. References: Install IT Service Intelligence in a distributed environment

NEW QUESTION 10

Which of the following services often has KPIs but no entities?

- A. Security Service.
- B. Network Service.
- C. Business Service.
- D. Technical Service.

Answer: C

Explanation:

In the context of Splunk IT Service Intelligence (ITSI), a Business Service often has Key Performance Indicators (KPIs) but might not have directly associated entities. Business Services represent high-level aggregations of organizational functions or processes and are typically measured by KPIs that reflect the performance of underlying technical services or components rather than direct infrastructure entities. For example, a Business Service might monitor overall transaction completion times or customer satisfaction scores, which are abstracted from the specific technical entities that underlie these metrics. This abstraction allows Business Services to provide a business-centric view of IT health and performance, focusing on outcomes rather than specific technical components.

NEW QUESTION 13

When installing ITSI to support a Distributed Search Architecture, which of the following items apply? (Choose all that apply.)

- A. Copy SA-IndexCreation to all indexers.
- B. Copy SA-IndexCreation to the etc/apps directory on the index cluster master node.
- C. Extract installer package into etc/apps directory of the cluster deployer node.
- D. Extract ITSI app package into etc/apps directory of search head.

Answer: A

Explanation:

Copy SA-IndexCreation to \$SPLUNK_HOME/etc/apps/ on all individual indexers in your environment.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallSHC>

A is the correct answer because when installing ITSI to support a distributed search architecture, you need to copy SA-IndexCreation to all indexers. SA-IndexCreation is an app that contains the definitions of the ITSI indexes, such as itsi_summary, itsi_tracked_alerts, itsi_grouped_alerts, etc. You need to copy this

app to all indexers to ensure that they can store and search the ITSI data. B is not a correct answer because you do not need to copy SA-IndexCreation to the etc/apps directory on the index cluster master node. The index cluster master node does not store or search data, it only manages the replication and availability of data across the index cluster peers. C is not a correct answer because you do not need to extract the installer package into etc/apps directory of the cluster deployer node. The cluster deployer node is used to distribute apps and configuration updates to the search head cluster members. You need to extract the installer package into etc/shcluster/apps directory of the cluster deployer node instead. D is not a correct answer because you do not need to extract the ITSI app package into etc/apps directory of search head. You need to extract the ITSI app package into etc/shcluster/apps directory of the cluster deployer node and use the deployer to push the app to all search head cluster members. References: [Install Splunk IT ServiceIntelligence on a search head cluster], [Install Splunk IT Service Intelligence on an indexer cluster]

NEW QUESTION 15

How can Service Now incidents be created automatically when a Multi-KPI alert triggers? (select all that apply)

- A. By creating a custom etc/apps/SA-ITOA/workflow_rule
- B. conf
- C. By linking Entities to Service-Now configuration items.
- D. By creating a notable event aggregation policy with a SNOW incident action.
- E. By editing the associated correlation search and specifying an alert action.

Answer: CD

Explanation:

To automatically create ServiceNow incidents when a Multi-KPI alert triggers in Splunk IT Service Intelligence (ITSI), the following approaches can be used:

* C.By creating a notable event aggregation policy with a ServiceNow (SNOW) incident action:ITSI allows the creation of notable event aggregation policies that can specify actions to be taken when certain conditions are met. One of these actions can be the creation of an incident in ServiceNow, directly linking the alerting mechanism in ITSI with incident management in ServiceNow.

* D.By editing the associated correlation search and specifying an alert action: Correlation searches in ITSI are used to identify patterns or conditions that signify notable events. These searches can be configured to include alert actions, such as creating a ServiceNow incident, whenever the search conditions are met. This direct integration ensures that incidents are automatically generated in ServiceNow, based on the specific criteria defined in the correlation search.

Options A and B are not standard practices for integrating ITSI with ServiceNow for automatic incident creation. The configuration typically involves setting up actionable alert mechanisms within ITSI that are specifically designed to integrate with external systems like ServiceNow.

NEW QUESTION 20

In maintenance mode, which features of KPIs still function?

- A. KPI searches will execute but will be buffered until the maintenance window is over.
- B. KPI searches still run during maintenance mode, but results go to itsi_maintenance_summary index.
- C. New KPIs can be created, but existing KPIs are locked.
- D. KPI calculations and threshold settings can be modified.

Answer: A

Explanation:

It's a best practice to schedule maintenance windows with a 15- to 30-minute time buffer before and after you start and stop your maintenance work. This gives the system an opportunity to catch up with the maintenance state and reduces the chances of ITSI generating false positives during maintenance operations.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW>

A is the correct answer because KPI searches still run during maintenance mode, but the results are buffered until the maintenance window is over. This means that no alerts are triggered during maintenance mode, but once it ends, the buffered results are processed and alerts are generated if necessary. You cannot create new KPIs or modify existing KPIs during maintenance mode. References: [Overview of maintenance windows in ITSI]

NEW QUESTION 23

What are valid considerations when designing an ITSI Service? (Choose all that apply.)

- A. Service access control requirements for ITSI Team Access should be considered, and appropriate teams provisioned prior to creating the ITSI Service.
- B. Entities, entity meta-data, and entity rules should be planned carefully to support the service design and configuration.
- C. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index.
- D. Backfill of a KPI should always be selected so historical data points can be used immediately and alerts based on that data can occur.

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/ImplementPerms>

A, B, and C are correct answers because service access control requirements for ITSI Team Access should be considered before creating the ITSI Service, as different teams may have different permissions and views of the service data. Entities, entity meta-data, and entity rules should also be planned carefully to support the service design and configuration, as they determine how ITSI maps data sources to services and KPIs. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index for faster retrieval and analysis. References: ITSI service design best practices, Overview of ITSI indexes

NEW QUESTION 27

Which deep dive swim lane type does not require writing SPL?

- A. Event lane.
- B. Automatic lane.
- C. Metric lane.
- D. KPI lane.

Answer: D

Explanation:

A KPI lane is a type of deep dive swim lane that does not require writing SPL. You can simply select a service and a KPI from a drop-down list and ITSI will automatically populate the lane with the corresponding data. You can also adjust the threshold settings and time range for the KPI lane. References: [KPI Lanes]

NEW QUESTION 28

Which of the following is a problem requiring correction in ITSI?

- A. Two or more entities with the same service ID.
- B. Two or more entities with the same entity ID.
- C. Two or more entities with the same value in a single alias field.
- D. Two or more entities with the same entity key value in any info field.

Answer: C

Explanation:

In Splunk IT Service Intelligence (ITSI), entities represent infrastructure components, applications, or other elements that are monitored. Each entity is uniquely identified by its entity ID, and entities can be associated with one or more services through the concept of aliases. A problem arises when two or more entities have the same value in a single alias field because aliases are used to match events to entities in ITSI. If multiple entities share the same alias value, ITSI might incorrectly associate data with the wrong entity, leading to inaccurate monitoring and analytics. This scenario requires correction to ensure that each alias uniquely identifies a single entity, thereby maintaining the integrity of the monitoring and analysis process within ITSI. The uniqueness of service IDs, entity IDs, and entity key values in info fields is also important but does not typically present the same level of issue as duplicate values in an alias field.

NEW QUESTION 29

Which of the following describes entities? (Choose all that apply.)

- A. Entities must be IT devices, such as routers and switches, and must be identified by either IP value, host name, or mac address.
- B. An abstract (pseudo/logical) entity can be used to split by for a KPI, although no entity rules or filtering can be used to limit data to a specific service.
- C. Multiple entities can share the same alias value, but must have different role values.
- D. To automatically restrict the KPI to only the entities in a particular service, select ??Filter to Entities in Service??.

Answer: BD

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIfilter>

Entities are IT components that require management to deliver an IT service. Each entity has specific attributes and relationships to other IT processes that uniquely identify it. Entities contain alias fields and informational fields that ITSI associates with indexed events. Some statements that describe entities are:

- * B. An abstract (pseudo/logical) entity can be used to split by for a KPI, although no entity rules or filtering can be used to limit data to a specific service. An abstract entity is an entity that does not represent a physical host or device, but rather a logical grouping of data sources. For example, you can create an abstract entity for each business unit in your organization and use it to split by for a KPI that measures revenue or customer satisfaction. However, you cannot use entity rules or filtering to limit data to a specific service based on abstract entities, because they do not have alias fields that match indexed events.
- * D. To automatically restrict the KPI to only the entities in a particular service, select ??Filter to Entities in Service??. This option allows you to filter the data sources for a KPI by the entities that are assigned to the service. For example, if you have a service for web servers and you want to monitor the CPU load percent for each web server entity, you can select this option to ensure that only the events from those entities are used for the KPI calculation.

References: Overview of entity integrations in ITSI, [Create KPI base searches in ITSI]

NEW QUESTION 32

Which of the following is a characteristic of base searches?

- A. Search expression, entity splitting rules, and thresholds are configured at the base search level.
- B. It is possible to filter to entities assigned to the service for calculating the metrics for the service??s KPIs.
- C. The fewer KPIs that share a common base search, the more efficiency a base search provides, and anomaly detection is more efficient.
- D. The base search will execute whether or not a KPI needs it.

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch>

A base search is a search definition that can be shared across multiple KPIs that use the same data source. Base searches can improve search performance and reduce search load by consolidating multiple similar KPIs. One of the characteristics of base searches is that it is possible to filter to entities assigned to the service for calculating the metrics for the service??s KPIs. This means that you can use entity filtering rules to specify which entities are relevant for each KPI based on the base search results. References: Create KPI base searches in ITSI, [Filter entities for KPIs based on base searches]

NEW QUESTION 34

Which of the following is a recommended best practice for ITSI installation?

- A. ITSI should not be installed on search heads that have Enterprise Security installed.
- B. Before installing ITSI, make sure the Common Information Model (CIM) is installed.
- C. Install the Machine Learning Toolkit app if anomaly detection must be configured.
- D. Install ITSI on one search head in a search head cluster and migrate the configuration bundle to other search heads.

Answer: A

Explanation:

One of the recommended best practices for Splunk IT Service Intelligence (ITSI) installation is to avoid installing ITSI on search heads that already have Splunk Enterprise Security (ES) installed. This recommendation stems from potential resource conflicts and performance issues that can arise when both resource-intensive applications are deployed on the same instance. Both ITSI and ES are complex applications that require significant system resources to function effectively, and running them concurrently on the same search head can lead to degraded performance, conflicts in resource allocation, and potential stability issues. It's generally advised to segregate these applications onto separate Splunk instances to ensure optimal performance and stability for both platforms.

NEW QUESTION 39

Which of the following describes enabling smart mode for an aggregation policy?

- A. Configure → Policies → Smart Mode → Enable, select ??fields??, click ??Save??
- B. Enable grouping in Notable Event Review, select ??Smart Mode??, select ??fields??, and click ??Save??
- C. Edit the aggregation policy, enable smart mode, select fields to analyze, click ??Save??
- D. Edit the notable event view, enable smart mode, select ??fields??, and click ??Save??

Answer: C

Explanation:

- * 1. From the ITSI main menu, click Configuration > Notable Event Aggregation Policies.
- * 2. Select a custom policy or the Default Policy.
- * 3. Under Smart Mode grouping, enable Smart Mode.
- * 4. Click Select fields. A dialog displays the fields found in your notable events from the last 24 hours.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/SmartMode>

C is the correct answer because smart mode is a feature of aggregation policies that allows ITSI to automatically group notable events based on the fields that have the most impact on the event occurrence. You can enable smart mode for an aggregation policy by editing the policy, selecting the smart mode option, and choosing the fields to analyze. You can also specify a minimum number of events to trigger smart mode and a maximum number of groups to create. References: Configure smart mode for aggregation policies in ITSI

NEW QUESTION 42

.....

Relate Links

100% Pass Your SPLK-3002 Exam with Exambible Prep Materials

<https://www.exambible.com/SPLK-3002-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>