DUMPSBOSS.

Splunk Cloud Certified Admin

Splunk SPLK-1005

Version Demo

Total Demo Questions: 10

Total Premium Questions: 103

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Splunk Cloud Overview	2
Topic 2, Data Management	74
Topic 3, User Management	13
Topic 4, Splunk Cloud Administration	10
Topic 5, Monitoring and Troubleshooting	4
Total	103

QUESTION NO: 1

In case of a Change Request, which of the following should submit a support case for Splunk Support?

A. The party requesting the change.

B. Certified Splunk Cloud administrator.

C. Splunk infrastructure owner.

D. Any person with the appropriate entitlement

ANSWER: D

Explanation:

Any person with the appropriate entitlement is correct because the ability to open and manage a Splunk Support case is governed by the customer's support access and entitlement configuration, rather than by a particular job title or technical responsibility. A change request must be submitted through Splunk's established support process by someone authorized to use the organization's support entitlement. This ensures that Splunk can validate the request against the entitled customer account, communicate with an approved contact, and track the request through the applicable support workflow. In practice, an organization may grant this access to a Splunk Cloud administrator, an infrastructure owner, or another designated employee, but none of those titles alone is the deciding requirement. The key condition is that the individual has the appropriate entitlement and access to submit a case on behalf of the customer. Splunk's support resources describe how customers engage Support and manage cases, while Splunk Cloud service information defines the service and support framework for Cloud customers. See Splunk Support and the Splunk Cloud Service Details.

QUESTION NO: 2

Which of the following are default Splunk Cloud user roles?

A. must_delete, power, sc_admin

B. power, user, admin

C. apps, power, sc_admin

D. can delete, users, admin

ANSWER: B

Explanation:

power, user, admin is correct because these are standard default roles supplied with Splunk Cloud Platform. The **user** role provides the baseline capabilities needed for ordinary users to search data and use Splunk Web within the indexes, search limits, and knowledge-object permissions assigned to that role. The **power** role builds on ordinary user access for people who need additional search and knowledge-object capabilities, such as creating and sharing certain reports or other objects. The **admin** role is the standard administrative role and provides broad permissions for managing Splunk configuration, users, roles, knowledge objects, and other platform settings permitted in the Splunk Cloud environment. These built-in roles provide a practical starting point for role-based access control; administrators can then assign users to appropriate roles and create custom roles when organizational requirements call for more specific privileges. Splunk documents its default roles and their capabilities in the platform security documentation. See About users and roles in Splunk Cloud Platform and Add and edit roles in Splunk Cloud Platform.

QUESTION NO: 3

Which of the following app installation scenarios can be achieved without involving Splunk Support?

A. Deploy premium apps.

B. Install apps via the Request Install button.

C. Install apps via self-service.

D. Install apps that have not gone through the vetting process.

ANSWER: C

Explanation:

Install apps via self-service is correct because Splunk Cloud Platform provides a self-service installation workflow for eligible apps. A Splunk Cloud administrator can use Splunk Web to browse or upload an app package and complete installation without opening a Splunk Support case, provided that the app meets the requirements for self-service installation. This workflow is intended for apps that are compatible with Splunk Cloud and do not require Splunk-managed deployment actions, special entitlement handling, or additional security review. Administrators should confirm that an app is supported for their Splunk Cloud experience and that they have the required administrative permissions before installing it. After installation, the administrator can configure the app and assign its permissions within Splunk Cloud as appropriate. Self-service installation therefore enables a qualified administrator to deploy eligible apps directly, rather than relying on the support-assisted app-installation process. Splunk documents the available installation paths and the requirements for installing apps in Splunk Cloud in its Install apps in Splunk Cloud Platform guidance. Additional information about app availability and app details is available through Splunkbase.

QUESTION NO: 4

Which of the following is a valid method to test if a forwarder can successfully send data to Splunk Cloud?

A. Search the _audit index to confirm whether the forwarder ID was registered.

B. Use oneshot from the CLI on the forwarders, then check to see if those logs show up in the Splunk Cloud environment.

C. On Splunk Cloud UI, click Add Data and upload a test file, then search to see if the logs show up.

D. Ping the inputssl.example.splunkcloud.com to see if it returns the ping.

ANSWER: B

Explanation:

Use oneshot from the CLI on the forwarders, then check to see if those logs show up in the Splunk Cloud environment. This is a valid end-to-end functional test because it causes a known, finite test file to be ingested by the forwarder and forwarded through its configured output to the Splunk Cloud deployment. After submitting the file, an administrator can run a search in Splunk Cloud for distinctive text from the test file, the expected source, host, or sourcetype. Finding those events confirms more than basic network reachability: it demonstrates that the forwarder can read the input, establish and use its configured forwarding connection, transmit the event data, and make the resulting events searchable in the target environment. A small test file with a unique marker or timestamp is especially useful because it makes verification unambiguous and avoids confusing test events with existing production data. The oneshot command is documented as a command-line method for adding a file as a one-time input, and Splunk also documents command-line tools for checking and managing forwarder output configuration. See Monitor files and directories using the CLI and Use forwarding commands.

QUESTION NO: 5

Which of the following lists all parameters supported by the acceptFrom argument?

A. IPv4, IPv6, CIDRs, DNS names, Wildcards

B. IPv4, IPv6, CIDRs, DNS names

C. CIDRs, DNS names, Wildcards

D. IPv4. CIDRs, DNS names. Wildcards

ANSWER: A

Explanation:

IPv4, IPv6, CIDRs, DNS names, Wildcards is correct. The `acceptFrom` setting controls the source hosts that a Splunk TCP or Splunk-to-Splunk receiving input permits to establish a connection. Its accepted source specifications accommodate individual IPv4 and IPv6 addresses, network ranges expressed with CIDR notation, and hostnames resolved through DNS. This lets an administrator define an allow list at the appropriate level of precision, from a single forwarder to an entire approved network.

Wildcard support is also part of the accepted matching capability. It is useful when defining a permitted group of source addresses where a literal IP address or a single CIDR range is not the desired expression. The setting can contain a comma-separated set of supported source specifications, allowing a receiving instance to accept connections from multiple approved address families, networks, and named hosts. A secure implementation should still make the allow list as specific as operationally practical and validate it with the organization's forwarder topology. Splunk documents `acceptFrom` in the `inputs.conf` specification for receiving inputs. See the official inputs.conf specification and Splunk's guidance on enabling a receiver.

QUESTION NO: 6

Consider the following configurations:

```
$SPLUNK_HOME/etc/apps/unix/local/inputs.conf

[monitor:///var/log/secure.log]
sourcetype = access_combined
index = security

$SPLUNK_HOME/etc/apps/search/local/inputs.conf

[monitor:///var/log/secure.log]
host = logsvr1
sourcetype = linux_secure
```

What is the value of the sourcetype property for this stanza based on Splunk ' s configuration file precedence?

A. NULL, or unset, due to configuration conflict

B. access_combined

C. linux_secure

D. linux_secure, access_combined

ANSWER: B

Explanation:

The effective value is **access_combined**. Both settings are in an app's `local` directory, so they are at the same general precedence tier. When Splunk encounters conflicting settings at that tier, it applies app-directory precedence using lexical ordering of the app directory names. The `unix` app directory sorts after the `search` app directory, so the setting in `$SPLUNK_HOME/etc/apps/unix/local/inputs.conf` has precedence over the corresponding setting in `$SPLUNK_HOME/etc/apps/search/local/inputs.conf`. Therefore, for the shared input stanza, Splunk uses `sourcetype = access_combined`.

This illustrates that configuration precedence is evaluated not just by whether a file is in `default` or `local`, but also by the relative precedence of application directories when equivalent configuration layers define the same attribute. An administrator can verify the final merged configuration, including the source file that supplied each setting, with the `splunk btool inputs list --debug` command. Splunk documents configuration locations and precedence at Where to find the configuration files and provides details on inspecting merged configuration through Use btool to troubleshoot configurations.

QUESTION NO: 7

A monitor has been created in inputs. con: for a directory that contains a mix of file types.

How would a Cloud Admin fine-tune assigned sourcetypes for different files in the directory during the input phase?

A. On the Indexer parsing the data, leave sourcetype as automatic for the directory monitor. Then create a props.conf that assigns a specific sourcetype by source stanza.

B. On the forwarder collecting the data, leave sourcetype as automatic for the directory monitor. Then create a props. conf that assigns a specific sourcetype by source stanza.

C. On the Indexer parsing the data, set multiple sourcetype_source attributes for the directory monitor collecting the files. Then create a props, com that filters out unwanted files.

D. On the forwarder collecting the data, set multiple 3ourcotype_sourcÂ« attributes for the directory monitor collecting the files. Then create a props. conf that filters out unwanted files.

ANSWER: B

Explanation:

On the forwarder collecting the data, leave sourcetype as automatic for the directory monitor. Then create a props.conf that assigns a specific sourcetype by source stanza. This approach allows one monitored directory to collect files normally while applying distinct sourcetype assignments according to each file's source path or filename pattern. In Splunk, a `[source::...]` stanza in `props.conf` can match the source value generated for an input and set the appropriate `sourcetype`. This is useful when files with different formats reside under the same monitored directory, because the selected sourcetype drives the parsing and field-extraction behavior appropriate to each format.

The configuration must be available on the data-collection forwarder so the source-based sourcetype assignment is made during input processing, before the events proceed through the indexing pipeline. The directory monitor itself can therefore remain automatic rather than forcing every file collected under that path into one common sourcetype. Splunk documents source-based sourcetype assignment in its Assign sourcetypes guidance and describes how props.conf stanzas configure event processing behavior.

QUESTION NO: 8

Which of the following are features of a managed Splunk Cloud environment?

A. Availability of premium apps, no IP address whitelisting or blacklisting, deployed in US East AWS region.

B. 20GB daily maximum data ingestion, no SSO integration, no availability of premium apps.

C. Availability of premium apps, SSO integration, IP address whitelisting and blacklisting.

D. Availability of premium apps, SSO integration, maximum concurrent search limit of 20.

ANSWER: C

Explanation:

Availability of premium apps, SSO integration, IP address whitelisting and blacklisting is correct. A managed Splunk Cloud Platform deployment is operated by Splunk, while customers retain the ability to use supported Splunk applications and configure important identity and access controls. Premium Splunk applications, including offerings such as Splunk Enterprise Security and Splunk IT Service Intelligence where licensed and supported for the deployment, can be used with Splunk Cloud Platform. This lets organizations extend the managed service with advanced security, observability, and operational workflows without administering the underlying Splunk infrastructure themselves.

Splunk Cloud Platform also supports single sign-on through SAML integration. An organization can connect its identity provider so that users authenticate with centrally managed enterprise identities, helping align Splunk access with established authentication and lifecycle processes. Network-based access restrictions are also available for Splunk Cloud environments. IP allow-list and deny-list controls provide an additional layer of protection by limiting access according to source IP

addresses or ranges, complementing Splunk roles and SSO-based authentication. Together, premium-app support, SSO, and IP address filtering accurately describe managed Splunk Cloud capabilities. See Splunk's SSO administration documentation and its IP allow-list configuration documentation.

QUESTION NO: 9

Which of the following tasks is the responsibility of a Splunk Cloud administrator?

A. Configuring deployer

B. Configuring cluster master

C. Configuring indexers

D. Configuring indexes

ANSWER: D

Explanation:

Configuring indexes is a Splunk Cloud administrator responsibility because indexes are the logical data stores that control how incoming data is organized, retained, and made available for search. Administrators can create and manage indexes in Splunk Cloud, subject to their role capabilities and the service entitlements of their Cloud stack. Index configuration includes choices such as an index name, data retention period, and storage-related settings exposed through Splunk Web or configuration workflows. These choices are important for meeting an organization's data lifecycle, search access, and compliance requirements.

In Splunk Cloud Platform, Splunk operates and maintains the underlying managed infrastructure. A customer administrator therefore manages the logical configuration available within the Cloud service rather than the underlying indexer topology. Splunk's documentation describes index management as an administrative activity and provides procedures for creating and managing indexes. See the Splunk Cloud documentation on setting up multiple indexes and the documentation for managing indexes.

QUESTION NO: 10

Which of the following stanzas would enable a TCP input on port 1025, allowing traffic from all IP addresses except 10.5.5.1?

A)

B)

C)

D)

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: B

Explanation:

The correct configuration is the stanza represented by **Option B**: `[tcp://1025]` followed by `acceptFrom = !10.5.5.1`. In `inputs.conf`, a `tcp://` stanza defines a raw TCP input, and the port number in the stanza name determines the listening port. Therefore, `[tcp://1025]` instructs the Splunk instance to listen for incoming TCP data on port 1025.

The `acceptFrom` attribute controls which source addresses are permitted to establish connections to that input. Prefixing an address with an exclamation mark creates an exclusion. With `acceptFrom = !10.5.5.1`, the input accepts connections from the default population of source IP addresses while specifically denying connections whose source address is `10.5.5.1`. This setting is useful when a single host must be prevented from sending data without creating an extensive allowlist for every other possible source.

Splunk documents TCP input stanzas and the `acceptFrom` setting in the inputs.conf specification. Additional guidance on configuring data inputs is available in the Getting data into Splunk documentation.