SailPoint

Identity-Security-Administrator

SailPoint Certified Identity Security Administrator

Latest Version: 6.0

Question: 1

An Administrator needs to monitor the health of Virtual Appliances (VA) and make sure the appropriate actions are taken if an alert message appears.
Is the following action appropriate in order to accomplish this task?
Proposed Solution / Statement:

If the VA status badge text shows "Connected", no action is required for the admin on this VA, move onto the next one in the cluster.
Does this proposed solution meet the requirement / solve the scenario?

A. Yes
B. No

Answer: A

Explanation:
This action is valid. In Identity Security Cloud, the health state of an individual Virtual Appliance is exposed through VA status and alert indicators. A VA displaying a Connected status is operating normally and maintaining communication with the SailPoint tenant. Therefore, when an administrator reviews the appliances in a VA cluster and encounters a VA whose status is Connected, no remediation is required for that particular appliance.
The administrator should continue reviewing the remaining VAs because cluster health depends on the operational state of all participating appliances. Other statuses can require intervention. For example, an inactive or disconnected appliance can indicate network, configuration, certificate, or service-related problems. Warning and error indicators should be investigated to determine whether restart, connectivity troubleshooting, configuration correction, or escalation is required.
Consequently, treating a Connected VA as healthy and proceeding to inspect the next appliance is the correct operational response.
Study Guide Virtual Appliances — Monitoring Virtual Appliance Health, VA Status and Alert Messages.
==========

Question: 2

Below is a search command in Identity Security Cloud.
Does the description accurately match the outcome of the search command?

Proposed Solution / Statement:

attributes.location:"sao paulo"
will return all identities that have the phrase "Sao Paulo" listed as their location.
Does this proposed solution meet the requirement / solve the scenario?

A. Yes
B. No

Answer: A

Explanation:
The proposed description is correct. Identity Security Cloud Search supports field-specific queries that allow administrators to search identity attributes directly. The expression attributes.location restricts the search to the location identity attribute rather than searching across all indexed identity fields.
The quotation marks around "sao paulo" indicate that the search engine should evaluate the value as a phrase. This means the query is intended to identify identities whose location attribute contains the phrase Sao Paulo rather than independently searching for the words sao and paulo in unrelated positions.
Field qualification is important when administrators need precise search results. Without the attributes.location prefix, a general search could potentially return matches from other searchable attributes or indexed properties. Combining the specific identity attribute with a quoted phrase produces a more targeted search result.
Therefore, the query accurately retrieves identities whose location information matches the Sao Paulo phrase.
Study Guide Platform — Identity Security Cloud Search, Building Search Queries, Identity Attribute Searches.
==========

Question: 3

Below is a search command in Identity Security Cloud.
Does the description accurately match the outcome of the search command?
Proposed Solution / Statement:

accountCount:[1 to 4
will search for identities that have 1, 2, 3, or 4 accounts.
Does this proposed solution meet the requirement / solve the scenario?

A. Yes
B. No

Answer: B

Explanation:
The proposed statement is incorrect because the displayed search syntax is malformed. To search for identities whose account count falls within an inclusive numerical range, Identity Security Cloud uses range-query syntax with properly matched square brackets.
The correct expression is:
accountCount:[1 TO 4]
Square brackets indicate that both endpoints are included. Therefore, a correctly formatted query would return identities with account counts of 1, 2, 3, or 4. The displayed expression, however, is missing the closing square bracket and does not follow the documented range syntax correctly.
The accountCount field represents the number of accounts associated with an identity across connected sources. Range searches are useful when administrators need to identify identities with unusually low or high account ownership, investigate orphaned access patterns, or perform access-analysis activities.
Because the specific proposed command is syntactically incomplete, it cannot reliably be treated as the documented query that returns identities with one through four accounts.
Study Guide Platform — Search Query Syntax, Range Queries, Identity Search Fields.
==========

Question: 4

Is the following statement regarding the concept of federated identities true?
Proposed Solution / Statement:

An identity provider offers specific services or applications to users after verifying their identity.
Does this proposed solution meet the requirement / solve the scenario?

A. Yes
B. No

Answer: B

Explanation:
The statement is incorrect because it confuses the responsibilities of an Identity Provider with those of a Service Provider. In a federated authentication architecture, the Identity Provider, commonly called the IdP, is responsible for authenticating the user and issuing trusted identity or authentication information.
The Service Provider is the system, application, or service that the user is attempting to access. It relies on the authentication assertion provided by the IdP and determines whether the authenticated user can access the requested resource.
For example, when Identity Security Cloud is configured to use SAML federation, an external IdP can authenticate the user. The IdP then sends a signed SAML assertion to Identity Security Cloud. Identity Security Cloud acts as the Service Provider and provides the application functionality after accepting the trusted authentication information.

Therefore, the component that offers the application or service is generally the Service Provider, not the Identity Provider. The IdP establishes identity and provides authentication assertions.
Study Guide Access Management — Federated Authentication, Identity Providers, Service Providers, SAML Authentication.
==========

Question: 5

Is the following statement regarding the concept of federated identities true?
Proposed Solution / Statement:

An identity provider (IdP) is a trusted entity that authenticates users and provides identity information to service providers.
Does this proposed solution meet the requirement / solve the scenario?

A. Yes
B. No

Answer: A

Explanation:
The statement accurately describes the function of an Identity Provider in a federated authentication architecture. An IdP authenticates users and provides trusted identity or authentication information to a Service Provider. This enables the Service Provider to rely on an established trust relationship instead of independently validating the user's primary credentials.
In a SAML-based implementation, the Identity Provider authenticates the user and generates a signed SAML assertion. The assertion contains information that allows the Service Provider to determine that the user's authentication has been successfully completed. Depending on configuration, additional identity attributes can also be included.
Identity Security Cloud can operate as a SAML Service Provider and rely on an organization's external Identity Provider for user authentication. This allows enterprises to centralize authentication and integrate SailPoint access with existing single sign-on infrastructure.
The critical concepts are trust, centralized authentication, and secure transfer of authentication assertions between the IdP and Service Provider. The proposed statement correctly identifies each of these fundamental IdP responsibilities.
Study Guide Access Management — Federated Identity, Identity Providers, SAML Authentication, Service Provider Integration.
==========

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer