Vendor: SailPoint

Exam Code: SailPoint-Certified-IdentityNow-Engineer

Exam Name: SailPoint Certified IdentityNow Engineer

Version: DEMO

QUESTION 1
Is this statement true about the purpose of a tenant?

Solution: A non-production tenant is for demonstrating functionality.

A. Yes
B. No

Answer: A
Explanation:
A non-production tenant is commonly used for demonstrating functionality, as well as for testing and development purposes. In a SailPoint IdentityNow environment, non-production tenants provide a sandbox environment where customers and engineers can safely explore the system, simulate use cases, and demonstrate functionality without impacting the live production environment.

Key Reference from SailPoint Documentation:

Non-Production Tenant Usage: SailPoint recommends non-production tenants for testing, demonstrating functionality, and conducting proofs of concept, ensuring that the production environment remains unaffected.

QUESTION 2
Is this statement true about the purpose of a tenant?

Solution: All customers are allowed a maximum of one non-production tenant.

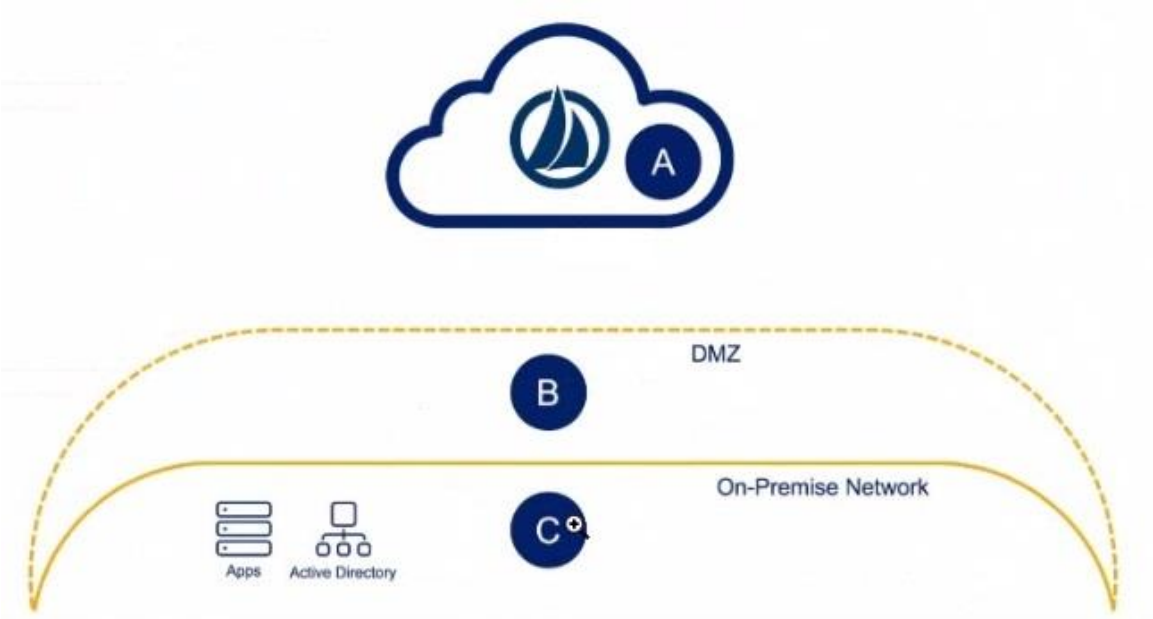
A. Yes
B. No

Answer: B
Explanation:
Not all customers are restricted to a maximum of one non-production tenant. The number of non-production tenants that a customer can have depends on their specific licensing agreement with SailPoint. Some customers may be allowed multiple non-production tenants for various purposes like testing, development, and staging.

Key Reference from SailPoint Documentation:

Tenant Provisioning Guidelines: SailPoint provides flexibility in the number of non-production tenants based on customer agreements, allowing for multiple environments when needed.

QUESTION 3
Exhibit.



Solution: An engineer has one small production data center with an Active Directory, a database server, and two cloud applications to which they need to connect. Where would the virtual appliances (VAs) reside In this scenario?

Solution: B

A. Yes
B. No

Answer: B
Explanation:
In this scenario, the Virtual Appliances (VAs) should not reside in the DMZ (B), which is typically used for hosting services that need to be exposed to both internal and external networks, like web servers or email gateways. However, VAs require more direct and secure access to internal resources like Active Directory and databases. The VA needs to reside where it has secure and reliable connectivity to internal resources like Active Directory and database servers, which would be in the internal network.

Key Reference from SailPoint Documentation:

VA Placement Guidance: Virtual Appliances are placed within the internal network, where they can securely connect to Active Directory, databases, and other internal applications for synchronization and provisioning tasks.

QUESTION 4
Is the following statement accurate regarding Separation of Duties (SoD)?

Solution: An SoD policy can define mitigating controls.

A. Yes
B. No

Answer: A
Explanation:
Yes, an SoD policy can define mitigating controls. Mitigating controls are measures put in place to reduce the risk of having conflicting duties. For example, if it's not possible to completely segregate duties due to resource constraints or other business factors, mitigating controls such as enhanced auditing, periodic reviews, or dual approvals can be defined to manage the risk. SailPoint IdentityNow allows for the creation of SoD policies that include such mitigating controls to ensure compliance with security and governance requirements.

Key Reference from SailPoint Documentation:

Mitigating Controls in SoD Policies: SailPoint supports the definition of mitigating controls within SoD policies to manage and reduce risks when full separation of duties cannot be achieved.

QUESTION 5
An IdentityNow engineer has the following problem:

An identity is listed under Identities with Errors.

Is this one of the steps that should be taken to troubleshoot the issue?

Solution: Check for missing lastname, email, or uid attributes.

A. Yes
B. No

Answer: A
Explanation:
Yes, checking for missing critical attributes like lastname, email, or uid is a valid step when troubleshooting an identity listed under "Identities with Errors" in SailPoint IdentityNow. These attributes are often required for proper identity processing, synchronization, and provisioning. If any of these attributes are missing or incorrectly configured, it could result in errors, preventing the identity from being fully processed by the system.

Key Reference from SailPoint Documentation:

Identity Attributes and Error Handling: SailPoint IdentityNow requires certain core identity attributes (such as lastname, email, uid) to be present and correctly populated. Missing or invalid values for these attributes can lead to errors and prevent identity synchronization or provisioning.

QUESTION 6
Does this correctly describe Manager Correlation?

Solution: Linking the manager of a given identity based on the value of an account or identify attribute

A. Yes
B. No

Answer: A
Explanation:
Yes, this correctly describes Manager Correlation in SailPoint IdentityNow. Manager Correlation

is the process of linking the manager of a given identity based on the value of an attribute in an account or identity profile, such as an employee's manager attribute. This allows the system to automatically identify and associate the correct manager for an identity, which can be important for tasks like access approvals and certification reviews.

Key Reference from SailPoint Documentation:

Manager Correlation Process: Manager correlation involves linking an identity to its manager based on specific attributes in the identity or account, such as the managerId or similar fields.

QUESTION 7
Does this correctly describe Manager Correlation?

Solution: an approval process by which identifies assigned as manager must periodically review and approve all access assigned to their employees.

A. Yes
B. No

Answer: B
Explanation:
No, this statement describes Manager Certification rather than Manager Correlation. Manager Certification refers to an approval process in which managers are required to periodically review and approve the access rights of their direct reports. This is a governance feature used to ensure that employees only have the access they need, and it helps managers validate their team's access periodically. Manager Correlation, on the other hand, is about linking identities to their managers based on attributes.

Key Reference from SailPoint Documentation:

Manager Certification vs. Manager Correlation: While Manager Certification involves periodic review and approval of access by managers, Manager Correlation is strictly about linking identities to their respective managers based on defined attributes.

QUESTION 8
Is this statement true about deploying and configuring IdentityNow's virtual appliance (VA)?

Solution: When using the AWS deployment option, the identityNow engineer needs to convert the VA image in order to deploy it.

A. Yes
B. No

Answer: B
Explanation:
No, when deploying the Virtual Appliance (VA) using the AWS deployment option, the IdentityNow engineer does not need to convert the VA image. SailPoint provides an AWS-compatible Amazon Machine Image (AMI) that can be directly used to deploy the VA in AWS without any additional conversion steps. The AMI is shared with the customer's AWS account, allowing for a streamlined deployment process.

Key Reference from SailPoint Documentation:

VA Deployment in AWS: SailPoint provides a ready-to-use AMI for AWS deployments, and no image conversion is necessary for this deployment method.

QUESTION 9
Is this statement true about deploying and configuring IdentityNow's virtual appliance (VA)?

Solution: When deploying the VA in Azure, the identityNow engineer will need to utilize the Azure command 璉ine interface(CLI) to deploy the VA image.

A. Yes
B. No

Answer: B
Explanation:
No, when deploying the Virtual Appliance (VA) in Azure, the IdentityNow engineer does not necessarily need to use the Azure CLI to deploy the VA image. While using the Azure CLI is one option, SailPoint provides multiple ways to deploy the VA in Azure, including using the Azure portal or ARM (Azure Resource Manager) templates. The process does not mandate using the CLI specifically.

Key Reference from SailPoint Documentation:

Azure VA Deployment Methods: SailPoint supports multiple methods for deploying the VA in Azure, including through the Azure portal or ARM templates, without requiring the CLI.

QUESTION 10
An IdentityNow engineer has set up an access profile for an application. The access profile allows for users to request access, and for a user's manager to approve or deny access.

After a recent staff meeting, management has expressed that they want to remove any approval requirements for this application.

Is management's request possible in IdentityNow. and. if so. are these the recommended steps the engineer should take to meet their new requirement?

Solution: It is possible. Delete the access profile.

A. Yes
B. No

Answer: B
Explanation:
No, deleting the access profile is not the correct way to meet the requirement of removing approval for access requests. The access profile defines the entitlements and permissions that users can request for an application. Deleting it would remove the entire ability to request access, rather than just removing the approval workflow. The correct step would be to modify the approval settings in the access profile (as explained in Question 44), not to delete it.

Key Reference from SailPoint Documentation:

Access Profile Management: Modifying approval settings in the access profile is the appropriate

step to meet management's new requirement, not deleting the profile itself.

QUESTION 11
Is the following true about custom connectors in IdentityNow?

Solution: Custom connector configurations can have account correlation settings defined.

A. Yes
B. No

Answer: A
Explanation:
Yes, custom connector configurations in SailPoint IdentityNow can have account correlation settings defined. Account correlation is used to link accounts from different sources to the correct identity in IdentityNow. When configuring a custom connector, it is possible to define how accounts from the connected system are correlated to existing identities based on attributes like usernames or other unique identifiers.

Key Reference from SailPoint Documentation:

Custom Connector Configuration: SailPoint allows for the definition of account correlation settings in custom connectors to ensure proper linking of external accounts to internal identities.

QUESTION 12
Is the following true about custom connectors in IdentityNow?

Solution: Custom connector are developed and compiled inside identityNow.

A. Yes
B. No

Answer: B
Explanation:
No, custom connectors are not developed and compiled inside IdentityNow. Custom connectors are typically developed outside of the IdentityNow platform using a development environment and then tested and packaged before being uploaded to the platform. These connectors can be developed using tools provided by SailPoint, but the actual development process occurs externally, not directly within the IdentityNow environment.

Key Reference from SailPoint Documentation:

Custom Connector Development: Custom connectors are developed outside of the IdentityNow platform and then integrated into it for use.

Thank You for Trying Our Product

Braindump2go 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.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14