Saviynt.SCAIP.v2026-09-07.q20

□□□□:	SCAIP
□□□□:	Saviynt Certified Advanced IGA Professional (Level 200)
□□□:	Saviynt
□□ □□ □□□:	20
□□:	v2026-09-07
# □□ □:	111
# □□ □□□:	200
https://www.krdump.com/Saviynt.SCAIP.v2026-09-07.q20.html	

NEW QUESTION: 1
□□ □□ □□□□ Workday□ □□□□ □□, Workday□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□ □□□ □□□□□. □□ ID □□□□ □□□ □ □□□ □□ □□ □□ □□□ □□ □□□□□ □□□□ □□□.
□□ □□ □□□□, EIC□ □□□□ □□ □□ □□□□ □□□ □□□□□ □□□□ □ □□□□?
A. USERUPDATEJSON□ □□□□ □□□ □□□□□ □□□□□.
B. MODIFYUSERDATAJSON□ □□□□ □□□ □□□□□ □□□□□.
C. IMPORTUSERJSON□ □□□□ □□□ □□□□□ □□□□□.
D. □ □□ □ □□ □□ □□□□ □□
Answer: (SHOW ANSWER)
Saviynt EIC□□□ Workday□ □□ □□□ □□ □□□□ □□□□ □□□ □ ID □□□ □ □ □ □□□□ □□□□ □□, □□ IMPORTUSERJSON□ □□□□ □□□□□. □ JSON □□□ □□□ □□□□ □□□ □□□□, □□ □□□□, Saviynt ID □□□□ □□ □□□□ □□□□□.
□□□ □□ □□□□ □□ □□□ □□□ □□□□ □□□ □□ □□□□□ □□□□ □□ IMPORTUSERJSON □□ □□ □□□ □□□□□ □□□□□. □□ □□ □□□□ □□□ □ Saviynt□ □□□□ □□ □□□□ □□□□ □□ □□, □□ □□ □□ □□□ □□□ □ □ □□ □□□ □□ □□□ □ □□□□.
□□ A(USERUPDATEJSON)□ B(MODIFYUSERDATAJSON)□ □□□□ □ □□□□ □ □ □□□□□ □□ □□□ □□□ □□□□, □□ □ □□ □□□□ □□□□ □□□□. □ □□ □□□ ID □□□□ □□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□ □ □□□.
OptionDis□ Saviynt□ □□□ □□ □□□ □□ IMPORTUSERJSON□□ □□□ □□□□ □ □□□□□ □□□□ □□□ □□□□ □□□□.
□□□ IMPORTUSERJSON□□ □□□ □□□□□ □□□□ □□ □□□□ □ ID □□□ □□□□ □□ □□□□ □□□□ □□ □□□□□.

NEW QUESTION: 2
EIC □□ ID □□□□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□? (□□ □□)
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A,C (LEAVE A REPLY)
Saviynt EIC□ □□ ID □□(DIM)□□ □□□ □□□ □□□□ □□ ID□ □□□□□ □□ □□ □□ □□□ □□□□□ □□□□□. □□□□ □ □□ □□ □□ □□□ □□□□ □ □□ □□□ □□□□, □ □ □□□ □□ □□ □□□ □□□ □□□□.
□□□□ □□(A)□ □□ □□□ □□□□□□ □□□□□. □□, □, □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□ □ □ □□□□ □□□ □□□□ □□□□ □ □ □□□□ □□□□ □□□□□. □□ □□ □□ □□□ □□□ □□□□ □□ □□□ □ □ □□□ □□ □ □□□□.
□□ □□(C)□ □□□ ID, □□ ID □□ □□ □□ □□□□ □□□ □□□ □□ □□□ □ □□ □□□□ □□ □□□□ □□□ □□□□□. □ □□□ □□ □□□□ □□ □□□□ □□ □□ □□□ □ □□ □□□□ □□□ □ □□□□.
□□ B(ID □□)□ DIM □□ □□□□ □□ □□ □□ □□□ □□□, □□ D(□□ □□)□ □□□ □□□□□ □□ □ □□□ □□□ □□□□.
□□□ □□□ □□ □□□ □□ □□□□, □ □ □□□ □□ □□□□ □□□□ □□ ID □ □□ □□□□□.

NEW QUESTION: 3
REST □□□□□ acctEntMappings□ □□□□ □ □□□ □□□□□ □□□□□? (□□ □□)
A. □□□□□
B. idPath
C. □□□
D. □□ ID
Answer: A,B,C (LEAVE A REPLY)
Saviynt REST □□□ □□□□ acctEntMapping□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□□ □□□ □□□□ □ □□□□□. □ □□□ □□, □□ □□ □□□ □□ □□□ □□□ □□□ □□□ □ □□ □□□□□.
acctEntMappings□ □□□□ □ □□□ □□□□□□ listPath, idPath □ keyField□ □□ □□□. listPath(□□ A)□ API □□ □□□ □□ □□□ □□ JSON □□□ □□□□□. □ □ □□ Saviynt□ □□ □□□□ □□□ □□ □□ □□□□ □□□ □ □□□□. idPath(□ □ B)□ □□ □□ □ □ □□□ □□ □□ □□□□ □□□□ □□□ □□ □ □□□ □□□

□□. keyField(□□ C)□ □□□ □□□ □□ □□□□ □ □□□□ □□□ □□ □□□□ □□□□□ □□□□□.
OptionD(accountID)□ acctEntMappings □□□□ □□□ □□□□□ □□□□. □□ □□ □□ □□ □□□□ □□□□□, acctEntMappings□ □□□ □□□ □ accountID □□ keyField□ □□□□□.
□□□ Saviynt REST □□□ □□ □□□ □□ acctEntMappings□ □□□ □□□ □□□ □□ listPath, idPath □ keyField□□□.

NEW QUESTION: 4
The EIC Administrator observed that all accounts were disabled in Saviynt due to incorrect configuration in the target application. What controls can be implemented in Saviynt to avoid such scenarios?
A. Use the accEntThresholdValue attribute in the STATUS_THRESHOLD_CONFIG connection parameter
B. It is not possible to set a limit
C. Set the limit in the external config file
D. Use the accountThresholdValue attribute in the STATUS_THRESHOLD_CONFIG connection parameter
Answer: (SHOW ANSWER)
In Saviynt EIC, mass unintended changes-such as all accounts being disabled due to incorrect target application configuration-can be prevented usingthreshold-based controls. These controls are defined using theSTATUS_THRESHOLD_CONFIGconnection parameter, which acts as a safeguard during reconciliation and provisioning processes.
The correct attribute in this scenario isaccountThresholdValue (Option D). This parameter allows administrators to define a threshold limit for account status changes (such as disablement). If the number or percentage of accounts being disabled exceeds the defined threshold, Saviynt can stop or flag the operation, preventing large-scale unintended impact.
OptionA (accEntThresholdValue)is used for entitlement-level thresholds, not account status changes.
OptionBis incorrect because Saviynt does provide this safeguard mechanism. OptionCis also incorrect since such controls are not managed externally but are part of Saviynt's connector configuration.
By usingaccountThresholdValuewithin STATUS_THRESHOLD_CONFIG, organizations can implement strong governance and prevent bulk account disablement due to misconfigurations or data issues during account import or reconciliation.

NEW QUESTION: 5
Saviynt App for ServiceNow□ □□□□ ServiceNow□ □□□ □ □□ □□□ □□ □□□ □□ □□□□□□?
A. □□□□

B. ServiceNow
C. □□□ □□ Saviynt □□ ServiceNow
D. □ □□ □ □□ □□ □□□□ □□
Answer: C (LEAVE A REPLY)
Saviynt □□ ServiceNow□□□ □□□□ Saviynt-ServiceNow □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □□□□□. □□□ □□ C□ □□□ □□□□□.
Saviynt□ ServiceNow□ □□□ □□ □□□ □□□□□. □ □□□□□ ServiceNow□ □ □□□□ □□ □□□ □□□ □□, Saviynt□ □□(□□□□□, □□ □ □□□ □□)□ □ □□□□.
□ □□ □□□□□ ServiceNow□ □□□□, API □ □□□ □□□ □□□ □□□□□□□ □□ □□ □□ □□□ □□□ □ □□□□.
For example, if the integration is configured such that ServiceNow creates a request and passes it to Saviynt, thenSaviynt performs fulfillment. Alternatively, if certain fulfillment logic or orchestration is handled within ServiceNow workflows or ITSM processes, thenServiceNow may drive parts of the fulfillment process.
This flexibility allows organizations to align the integration with their operational model, whether centralized in Saviynt or distributed with ServiceNow. Therefore, fulfillment is not restricted to a single system and is determined byconfiguration and architectural design choices.

NEW QUESTION: 6
To authenticate Saviynt REST API calls, what must be generated before invoking protected APIs?
A. SMTP token
B. OAuth access token
C. Transport package
D. Dataset key
Answer: B (LEAVE A REPLY)
The correct answer is B. OAuth access token . Saviynt documentation states that to integrate Saviynt APIs with Saviynt Identity Cloud, an OAuth access token must be generated to authenticate API calls. This is a foundational concept for the API section of Level 200 because even when using Postman or another client, the request must be authenticated before protected endpoints can be called successfully. Saviynt also documents that its APIs are RESTful APIs used to configure and access various platform features, so token-based authentication is central to practical API usage.
The other options are unrelated to Saviynt REST API authentication. SMTP token is not a Saviynt API authentication model, Transport package is used for moving supported configurations between environments, and Dataset key is not the documented authentication requirement for API access. Saviynt's API reference guide further describes version-specific collections, supported methods, requests, and responses, which is exactly why Postman-based testing in certification labs usually starts with authentication setup

first. In practical terms, if the OAuth token is missing or invalid, the request will fail even if the endpoint URL and payload are correct. That is why OAuth access token generation is the correct answer.

NEW QUESTION: 7
□□ □ □□ □□ □□□□□? (□□ □□)
A. □□ □□□ □□□□□ □□□□□ □□□□□ □□□ □□□ □ □□ □□□ □□ □ □□ □□□□ □□□ □□ □□□ □□□□□.
B. □□ □□□□□ □□□ □□□□ 60%□ □□, 100% □□□□ □□□ □□□□ □□□ □ □□□□ □□□□□.
C. □□ ID □□ □□□ □□□ SAV □□□ □□ □□□ □□ □□□ □□□ □□□□ □□ □.
D. □□ ID □□□ □□□ □□□ □□□ □ □□□ □□□ □□□□ □□□ □ □□□□.
Answer: A,C (LEAVE A REPLY)
A□ □□□ □□ □□□ Saviynt□ □□ □□□ □□□ □□□ □□ □□□ □□□□ □□ □ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□□. □□□ □□□ □□□□ □ □ □□□ □□□□□ □□□ □□□□□□□ □□□□ □□ □□ □□ □□(RBAC) □□□ □□□□ □□ □□□ □□□ □□ □□□ □□ □ □□□□.
□□ B□ □□ □□□□□ □□□ □□□(□: 60%)□ □□□□ □□ □□□□ □□ 60%□ □ □□□□ □□□ □□ □□□ □□□□□ □□□□ 100%□ □□□□□ □□□ □□□ □ □□□□□□□□. □ □□□ □□□ □□ □□□□ □□ □□□ □□ □□□□ □□□□.
C□ □□□ □□□□. □□ ID □□(DIM) □□□ □□ □□□ SAV □□ □□□ □□ □□□ □□. □□□□ □□□□ □□□□□ □□ ID□ □□ □□□ □ □□□ SAV □□ □□□ □ □□ □□□ □□□□ □□□.
DIM□ □□□ □□□□ □□□ □□□ □□ □□□ □□ □ □□□ □□□□ □□□ □ □ □□□, D□□ □□□ □□□□□. □□ □□□□ □□□□ □□□□.
□□□ □□□ A□ C□□□.

NEW QUESTION: 8
SMTP □□□□ □□□□ □□□ □□ □□□ □□□□□? (□□ □□)
A. NTLM
B. OAuth
C. □ □□ □ □□ □□ □□□□ □□
D. □□
Answer: A,B,D (LEAVE A REPLY)
Saviynt EIC□□ SMTP □□□ □□□ □□, □□, □□ □ □□□ □□□ □□ □□□□□ □□ □□□ □□□ □□□□□ □ □□□□□. □□ □□□□ □□□ □□□ □□ Saviynt □ □□ □□ □□□□□ □□□□□. □□□ □□ □□□ NTLM, OAuth □ Basic□□, □□ □ □□ A, B □ D□ □□□□□.

□□ □□(□□ D)□ □□□ □□□ □□□□□ □□□□ SMTP □□□ □□□□ □□□□ □□□□□. □□ □□□□□ □□ □□□ □□ □□□□ □□□□□ □□ □□□□ □□ □□□ □□□□ □□□□.
NTLM(□□ A)□ □□□□□ Microsoft □□ □□(□: Exchange □□)□□ □□□□ Windows □□ □□□ □□□ □□ □□□ □□□□ □□ □□□□ □ □□ □□□ □□□ □□.
OAuth(□□ B)□ □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□ □□□ □□ □□□ □□ □□□□□□□□. □□□□□ Microsoft 365 □□ Google Workspace□ □□ □ □□□ □□ □□□ □□□□□ □□□□□.
OptionC□ Saviynt□ □□□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□□.
□□□ Saviynt□□ □□□□ SMTP □□ □□□ NTLM, OAuth □ Basic□□□.

NEW QUESTION: 9
□□ □ REST □□□□ ImportAccountEntJSON□□ □□□□ □□ □□□□□ □□□□ □?
A. accountOwnerParams
B. □□ □□□□
C. accountParams
D. entOwnerParams
Answer: D (LEAVE A REPLY)
Saviynt EIC REST □□□ □□□□ ImportAccountEntJSON□ □□ □□□□□ □□ □ □ □ □□□□ □□□□(□□□□) □□□ □□□□ □ □□□□□. □ JSON □□□□ □□, □□ □ □□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□□□ □□□□ □□□□.
accountParams(□□ C)□ □□□ □□□□□□ □□ □□, □□ □ □□□□ □□ □□ □ □ □□□ □□□□ □ □□□□□. entitlementParams(□□ B) □□ □□□ □□□□□□ □□ □□□(□□, □□, □□)□ □□□□ □□□□ □□□ □□□□□.
accountOwnerParams(□□ A)□ □□ □□□ □□□ □□□□ □ □□□□ □ □□ □□□ □□□□□, □□ □□ □□□ □□□□ □□□□ □ □□□ □□□.
□□□, `entOwnerParams`(□□ D)□ `ImportAccountEntJSON` □□□□ □□□ □□□□ □ □□□□. □□ □□□(□□□□ □□)□ □□ □□□ □□ □□□ Saviynt REST □□□ □□□□ "entOwnerParams"□ □□□□ □□□□. Saviynt□ □□□ □□□□ □□ □□ □ □□□, □□□ □□□□ □□□ □□□□□ □□□□□ □□□□ □□□□.
□□□ □□ D□ □□□□□. □□ ImportAccountEntJSON □□□□□□ □□□□ □□ □ □ □□□□□ □□□□ □□□□□.

NEW QUESTION: 10
EIC is configured to create tickets in ServiceNow for requests for disconnected applications. The end user selects 3 different entitlements for a disconnected application and submits the request. How will EIC process this request?

A. If the "Enable Multi Entitlement Request" option is selected, then three tickets will be created in ServiceNow; otherwise, only one ticket will be created
B. Not a valid scenario because EIC does not support multiple entitlement requests when ServiceNow is integrated as the ticketing system
C. EIC will create three separate tickets in ServiceNow, one for each of the three entitlements
D. EIC will combine all three entitlements and create one ticket in ServiceNow
Answer: A (LEAVE A REPLY)
In Saviynt EIC when integrated with ServiceNow as aticketing system (ITSM)for disconnected applications, ticket creation behavior depends on the configuration setting"Enable Multi Entitlement Request." If this option is enabled, Saviynt treats each entitlement independently and createsseparate tickets in ServiceNow for each entitlementselected in the request. Therefore, if a user selects three entitlements,three individual ticketswill be generated, allowing granular tracking and fulfillment of each entitlement.
□□ □□□ □□□□ □□□ Saviynt□ □□ □□□ □□ □□ □□□□□ □□□□ □□ □ □□ □□□ □□□ □□□ ServiceNow □□□ □□□□□. □ □□□ □□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.
□□ B□ Saviynt□ ServiceNow □□□ □□ □□ □□ □□□ □□□□ □□□□□ □□ □□ □□□□. □□ C□ □□□ □□ □□□□ □□□ □□□□□ □□□□□□. □□ D □□ □□□ □□□□ □□ □□ □□ □□□□.
□□□ □□□ A□□□. A□ □□□ □□□ □□ □□□ □□□□ □□□□□.

NEW QUESTION: 11
EIC □□□□ □□□□ □ □□□□□ □□□ SAV □□□ □□ □□□□ □□□□□ □□ □. □□ □□□ □ □□ □□□ □□□□□? (□□ □□)
A. □□□ □□ □□
B. □□□ □□□□□ □□□□ □□□□ □□ SQL □□□ □□□□□.
C. SQL □□□ □□□□ □□□□ □□□□ □□□ □□□□ □□ □□□□ '□□□ □□ □□□ □□□' □□□□ □□□□□.
D. SQL □□□ □□□□ □□ □□□ □□□□ □□□□ □□□ CSV/Excel □□□ □□□ □□.
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which of the following EIC modules support configuration of active workflow? (Choose 3 options)
A. Security System
B. Endpoint
C. Global Configuration
D. Entitlement Type

Answer: A,B,D (LEAVE A REPLY)

In Saviynt EIC, workflows are a core component used to control approval processes for access requests, provisioning, and other identity lifecycle events. These workflows can be configured at multiple levels depending on the scope and granularity required.

Security System (A)supports workflow configuration to define approval processes at the application level.

This allows organizations to enforce consistent approval logic for all endpoints associated with that system.

Endpoint (B)also supports workflow configuration, enabling more granular control where different endpoints within the same security system may require distinct approval processes. This is particularly useful in complex environments with varied access control requirements.

Entitlement Type (D)supports workflows to manage approvals specific to entitlement categories (such as roles, groups, or permissions), ensuring appropriate governance at a finer level.

Global Configuration (C), while important for system-wide settings, is not typically used to directly assign active workflows to access requests. Instead, workflows are selected and applied within modules like Security System, Endpoint, and Entitlement Type.

Thus, the correct modules supporting active workflow configuration areSecurity System, Endpoint, and Entitlement Type.

NEW QUESTION: 13

Which of these is NOT a valid campaign type in EIC?

A. User Manager Campaign

B. SAV Role Campaign

C. Application Owner Meta Data Campaign

D. Organization Owner Campaign

Answer: C (LEAVE A REPLY)

In Saviynt EIC,Campaigns (Certifications)are used to review and validate user access, ensuring compliance and governance. Saviynt provides several predefined campaign types based on different ownership and responsibility models.

User Manager Campaign (A)is a valid campaign type where managers review and certify access of their direct reports. This is one of the most commonly used certification types.

SAV Role Campaign (B)is also valid and focuses on reviewing access related to SAV roles, allowing role owners or administrators to validate role assignments.

Organization Owner Campaign (D)is another valid campaign type, typically used when organizational hierarchy or ownership structures are leveraged for certification responsibilities.

Option C (Application Owner Meta Data Campaign) isnot a valid standard campaign typein Saviynt. While application owner-based campaigns do exist (e.g., Entitlement Owner or Application Owner campaigns),

"Meta Data Campaign" is not a recognized or supported campaign category in Saviynt EIC.
Thus, the correct answer isC, as it does not correspond to any valid campaign type in Saviynt.

NEW QUESTION: 14
Which HTTP method or methods is used to generate an Authorization Token for Saviynt EIC API?
A. PUT
B. GET
C. POST
D. GIVE
Answer: (SHOW ANSWER)
In Saviynt EIC, generating anAuthorization Tokenfor API access is performed using theHTTP POST method.
This is aligned with standard REST API authentication practices, where sensitive information such as credentials (username, password, client ID, or client secret) is securely transmitted in the request body rather than in the URL.
Saviynt provides API endpoints (such as/ECM/api/login) that require aPOST requestcontaining authentication details in JSON format. Upon successful authentication, the system returns asession token or authorization token, which is then used in subsequent API calls (typically passed in headers likeAuthorizationortoken).
Option A (PUT) and Option B (GET) are not suitable for authentication token generation. GET exposes parameters in the URL and is not secure for credential transmission, while PUT is typically used for updating resources. Option D (GIVE) is not a valid HTTP method.
Therefore, POST is the correct and secure method used in Saviynt APIs forauthentication and token generation, ensuring compliance with RESTful and security best practices.

NEW QUESTION: 15
What are the different features available under Role Intelligence? (Multi-Select)
A. Role Governance
B. Entitlement Discovery
C. Role Mining
D. Role-Access Mismatches
Answer: (SHOW ANSWER)
In Saviynt EIC,Role Intelligenceis a key component of Identity Governance that focuses on analyzing, optimizing, and managing roles effectively. It provides multiple features that help organizations improve role design and maintain compliance.
Role Governance (A)is a core feature that ensures roles are properly defined, reviewed, and certified. It helps maintain accountability and ensures that roles align with business policies.

Entitlement Discovery (B)enables identification and analysis of entitlements across applications, helping administrators understand what access exists and how it can be grouped into meaningful roles. This is essential for building accurate and efficient role models.
Role Mining (C)is one of the most important capabilities, allowing organizations to analyze user access patterns and automatically suggest roles based on common entitlement combinations. This improves role engineering and reduces manual effort.
Option D (Role-Access Mismatches) is not considered a standard feature under Role Intelligence; it is more aligned with analytics or audit findings rather than a core Role Intelligence function.
Therefore, the correct answers areA, B, and C, which represent the foundational features of Role Intelligence in Saviynt.

NEW QUESTION: 16
□□ □□ □ EIC□□ □□□ ID□ □□□ □ □□ □□□ □□□□□?
A. □□□ □□□□ □
B. □□ ID □□ □□□ □□□□
C. □□□ > ID □□□□ □□ □□□ □□□□ □
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
Saviynt EIC□□ □□ ID □□(DIM)□ ID □□ □□ □□□ □□ □□ ID□ □□□□ □□ □□□□□ □□□□□ □□ D(□□ □□ □□)□ □□□□□.
□□, HR □□□□ □□ □□□ □□ □□□□ □□□□ □□□ □ □□□ □□□□(□□ A) □□ □□ ID□ □□□ □ □□□□. Saviynt□ □□ □□□ □□□□ □□□ □□ □□□ □ □□□ □□□□□ □□□ □ □□□□. □□, □□ ID □□ □□(□□ B)□ □□□□ □ □□ □□□ □ □□□□. □ □□ □□□ □□□□ □□ □□ ID□ □□□□ □□□, □□□ □□ □□ □□ ID□ □□ □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□□.
□□ □□□□ □□□ □□□ □□□ □ ID □□□(□□ C)□□ □□ □□□□ □□□ □□ □□□ □□□ □ □□□□. □□□□□ □□ □□□ □□□ □□ □□ ID□ □□□□ □□ Saviynt□ □□□□ □□ □□□ □□□ □ □□□□.
□□□ □□□ □□ □□□ □□ □□□ □ □□ □□□ □□ □□□ □□ □□□□ □□ □ □□□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□ □ □□□ □□□.

NEW QUESTION: 17
EIC□□ □□□ □□□ □□ □□□ □□□ □□□□□? (□□ □□)
A. □□□□□ -> □□□ □□ □□ □□□ □□□ □□
B. □□□ □□ □□ □ □□□□ □□
C. As defined in Global Configurations - > Account Name Rule
D. As defined in Connection - > Create Account JSON
Answer: (SHOW ANSWER)
In Saviynt EIC, theservice account name generationis controlled through configuration-driven mechanisms to ensure consistency, automation, and compliance with naming standards.
Option A is correct because administrators can define naming conventions at theEndpoint level using the Service Account Name Rule. This allows dynamic generation of account names based on attributes such as application name, environment, or other identifiers, ensuring standardized naming across systems.
Option D is also correct since in many connector-based integrations, theCreate Account JSONconfiguration plays a role in provisioning. The account name can be derived or constructed within this JSON payload based on defined mappings and logic, especially for REST or custom connectors.
Option B is incorrect because service account creation in Saviynt is typically controlled and standardized; manual entry of account names is generally restricted or governed to avoid inconsistencies. Option C is incorrect because Global Configurations do not directly define service account naming rules in standard implementations.
Thus, the correct answers areEndpoint-based naming rules and Connection-level JSON configuration, ensuring automated and consistent service account naming.

NEW QUESTION: 18
□□ □□□□□(□□ □□)□□ □□□ □ □□ □□□ □□□ □□□□□?
A. □□ □□
B. □□ □□□
C. □□ □□
D. □□+□□ □□ □□□
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 19
The Helpdesk has set a new password for the user who called in for password reset assistance. Choose the correct configuration to share the password with the calling user
A. System automatically shares the password
B. Configure an email template in Change Password Notification configurations
C. Configure an email template in the Reset Password notification under password policy
D. Setup User Update Rule and configure an email template
Answer: C (LEAVE A REPLY)

In Saviynt EIC, password management includes configurable notification mechanisms to securely communicate password changes or resets to users. When aHelpdesk performs a password reset, the appropriate configuration to notify the user is through theReset Password notification under Password Policy.
Option C is correct because Saviynt provides a dedicatedReset Password notification templatewithin password policy configurations. This ensures that whenever a password is reset (either by user self-service or by Helpdesk), the system triggers the configured email template to notify the user. This template can include secure messaging and instructions related to the new password or next steps.
Option A is incorrect because the system does not automatically share passwords without proper configuration. Option B applies tochange password scenarios initiated by users, not Helpdesk resets. Option D is not recommended, as User Update Rules are not designed specifically for password notification workflows.
Thus, configuring theReset Password notification under password policyis the correct and secure approach.

NEW QUESTION: 20
□□□ □□□ □□ □□ □□ □□□(□□□□ □□□□□□□□□ □)□ □□□□ □ □ □ □□□□ □□ □□□ □□□□□?
A. □□□ □□□□ □□
B. □□ □□
C. □□ □□
D. SAV □□
Answer: B (LEAVE A REPLY)
□□□ B. □□ □□□□□. Saviynt □□□□ □□ □□□ □□ □□ □□□ □□ □□□ □ □□□ □□□□□ □□ □□□ □□□ □□□□ □, □ □□□□ □□□□□□ □□□□□ □□□□ □□□□. □□ □□ 200 □□ □□□ □□ □ □□ □□□□ □□ □□□ □□□ □ □□□□□. □□ □□□ □□ □□, □□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□ □□□ □ □□□ □□□ □□ □□□□□ □□ □□ □□□□ □□□ □□ □□□ □□□□□.
□□ □□□□ □ □□ □□□ □□□□ □□□□. □□□ □□□□ □□□ □□□□□ □ □□ □□□□ □□□ □ □□□ □□□ □ □□□□ □□□□□□ □□□□ □□□ □ □ □□, □□□□□ □□ □□ □□□ □□ □□ □□□□□□ □□ □□□ □□□□ □□□ □. □□ □□□ □□ □□□ □□□ □□ □□ □ □□ □□ □□ □□ □□□ □□□□□.
SAV □□□ □□ □□□□□□ □□□ □□□□□□ □□ Saviynt □□ □□□ □□ □□ □ □□□□□. □□ Saviynt □□□□□ □□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□□□□□ □ □□□ □□□□ □□□, □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□□□□□ □□□□□□.

SCAIP □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ SCAIP □□! DumpTop □ □□ **SCAIP** □□ □□□ □□□□□□, DumpTop SCAIP □□ □□□ □ □□□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop SCAIP □□□ □□□□□. https://www.dumptop.com/Saviynt/SCAIP-dump.html (**62** Q&As Dumps, **30%OFF Special Discount: KrDump**)