Free Questions for S90.20 by go4braindumps

Shared by Spencer on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

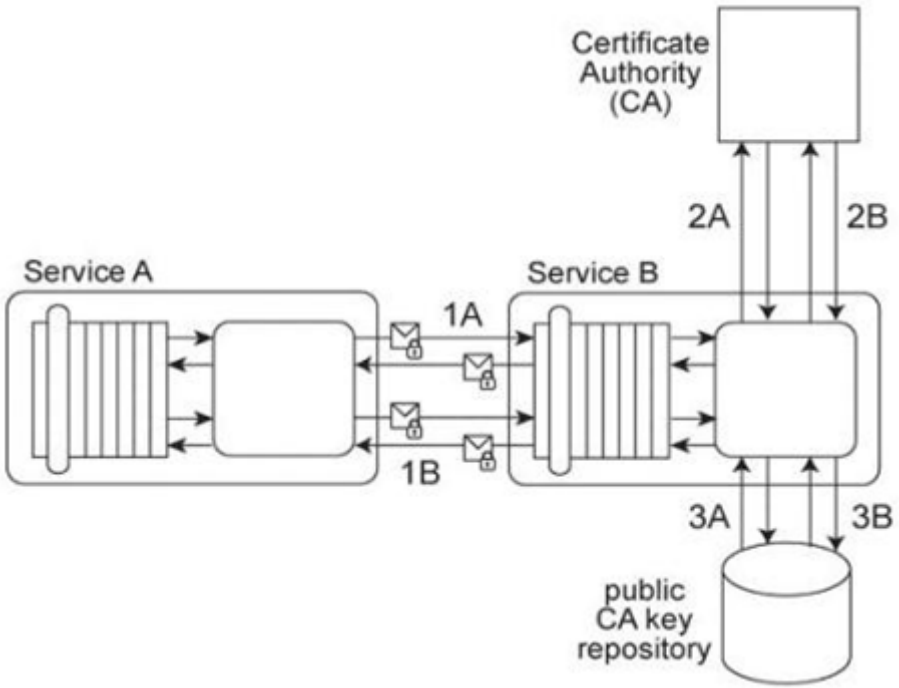
Question 1

Question Type: MultipleChoice

Service A exchanges messages with Service B multiple times during the same runtime service activity. Communication between Services A and B has been secured using transport-layer security. With each service request message sent to Service B (1A .IB), Service A includes an X.509 certificate, signed by an external Certificate Authority (CA). Service B validates the certificate by retrieving the public key of the CA (2A .2B) and verifying the digital signature of the X.509 certificate. Service B then performs a certificate revocation check against a separate external CA repository (3A, 3B). No intermediary service agents reside between Service A and Service B .Service B has recently suffered from poor runtime performance plus it has been the victim of an access-oriented attack. As a result, its security architecture must be changed to fulfill the following new requirements:

1. The performance of security-related processing carried out by Service B when communicating with Service A must be improved.

2. All request messages sent from Service A to Service B must be screened to ensure that they do not contain malicious content. Which of the following statements describes a solution that fulfills these requirements?



Options:

A- Eliminate the need to retrieve the public key from the Certificate Authority and to verify the certificate revocation information by extending the service contract of Service B to accept certificates only from pre-registered Certificate Authorities. This form of pre-registration ensures that Service B has the public key of the corresponding Certificate Authority.

B- Add a service agent to screen messages sent from Service A to Service B .The service agent can reject any message containing malicious content so that only verified messages are passed through to Service B .Instead of using X.509 certificates, use WS-Secure Conversation sessions. Service A can request a Security Context Token (SCT) from a Security Token Service and use the derived keys

from the session key to secure communication with Service B .Service B retrieves the session key from the Security Token Service.

C- Apply the Trusted Subsystem pattern by introducing a new utility service between Service A and Service B .When Service A sends request messages, the utility service verifies the provided credentials and creates a customized security profile for Service A .The security profile contains authentication and access control statements that are then inherited by all subsequent request messages issued by Service A .As a result, performance is improved because Service A does not need to resubmit any additional credentials during subsequent message exchanged as part of the same runtime service activity. Furthermore, the utility service performs message screening logic to filter out malicious content.

D- Apply the Trusted Subsystem pattern to by introducing a new utility service. Because Service B is required to limit the use of external resources. Service A must ensure that no other services can request processing from Service B in order to prevent malicious content from infiltrating messages. This is achieved by creating a dedicated replica of Service B to be used by the utility service only. Upon receiving the request message and the accompanying security credentials from Service A .the utility service verifies the authentication information and the validity of the X.509 signature. If the authentication information is correct, then the utility service replicates the code of Service B, performs the necessary processing, and returns the response to Service A .

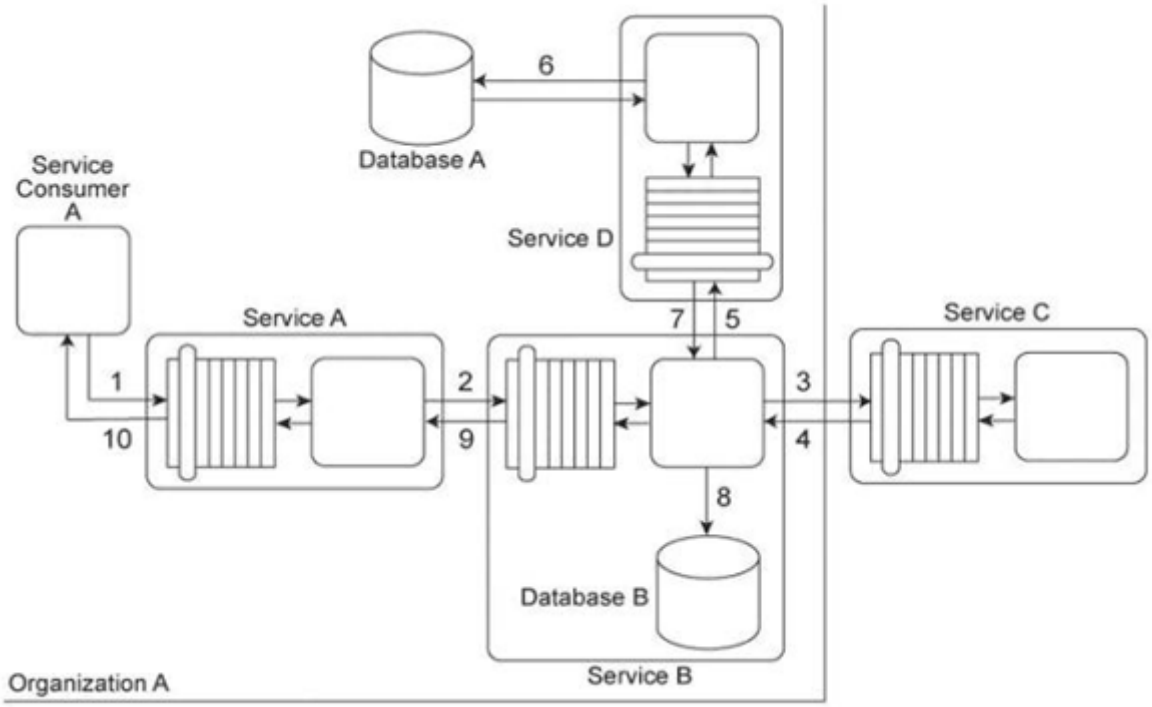
Answer:

B

Question 2

Question Type: MultipleChoice

Service Consumer A sends a request message to Service A (1), after which Service A sends a request message to Service B (2). Service B forwards the message to have its contents calculated by Service C (3). After receiving the results of the calculations via a response message from Service C (4), Service B then requests additional data by sending a request message to Service D (5). Service D retrieves the necessary data from Database A (6), formats it into an XML document, and sends the response message containing the XML-formatted data to Service B (7). Service B appends this XML document with the calculation results received from Service C, and then records the entire contents of the XML document into Database B (8). Finally, Service B sends a response message to Service A (9) and Service A sends a response message to Service Consumer A (10). Services A, B and D are agnostic services that belong to Organization A and are also being reused in other service compositions. Service C is a publicly accessible calculation service that resides outside of the organizational boundary. Database A is a shared database used by other systems within Organization A and Database B is dedicated to exclusive access by Service B .Service B has recently been experiencing a large increase in the volume of incoming request messages. It has been determined that most of these request messages were auto-generated and not legitimate. As a result, there is a strong suspicion that the request messages originated from an attacker attempting to carry out denial-of-service attacks on Service B .Additionally, several of the response messages that have been sent to Service A from Service B contained URI references to external XML schemas that would need to be downloaded in order to parse the message data. It has been confirmed that these external URI references originated with data sent to Service B by Service C .The XML parser currently being used by Service A is configured to download any required XML schemas by default. This configuration cannot be changed. What steps can be taken to improve the service composition architecture in order to avoid future denial-of-service attacks against Service B and to further protect Service A from data access-oriented attacks?



Options:

A- Apply the Data Origin Authentication pattern so that Service B can verify that request messages that claim to have been sent by Service A actually did originate from Service A .Apply-the Message Screening pattern to add logic to Service A so that it can verify that external URIs in response messages from Service B refer to trusted sources.

B- Apply the Service Perimeter Guard pattern to establish a perimeter service between Service B and Service C .Apply the-Brokered Authentication pattern by turning the perimeter service into an authentication broker that is capable of ensuring that only legitimate response messages are being sent to Service C from Service B Further apply the Data Origin Authentication pattern to enable the

perimeter service to verify that messages that claim to have been sent by Service C actually originated from Service C .Apply the Message Screening pattern to add logic to the perimeter service to also verify that URIs in request messages are validated against a list of permitted URIs from where XML schema downloads have been pre-approved.

C- Apply the Service Perimeter Guard pattern and the Message Screening pattern together to establish a service perimeter guard that can filter response messages from Service C before they reach Services A and B .The filtering rules are based on the IP address of Service C .If a request message originates from an IP address not listed as one of the IP addresses associated with Service C .then the response message is rejected.

D- Apply the Direct Authentication pattern so that Service C is required to provide security credentials, such as Username tokens, with any response messages it sends to Service B .Furthermore, add logic to Service A so that it can validate security credentials passed to it via response messages from Service B .by using an identity store that is shared by Services A and B .

Answer:

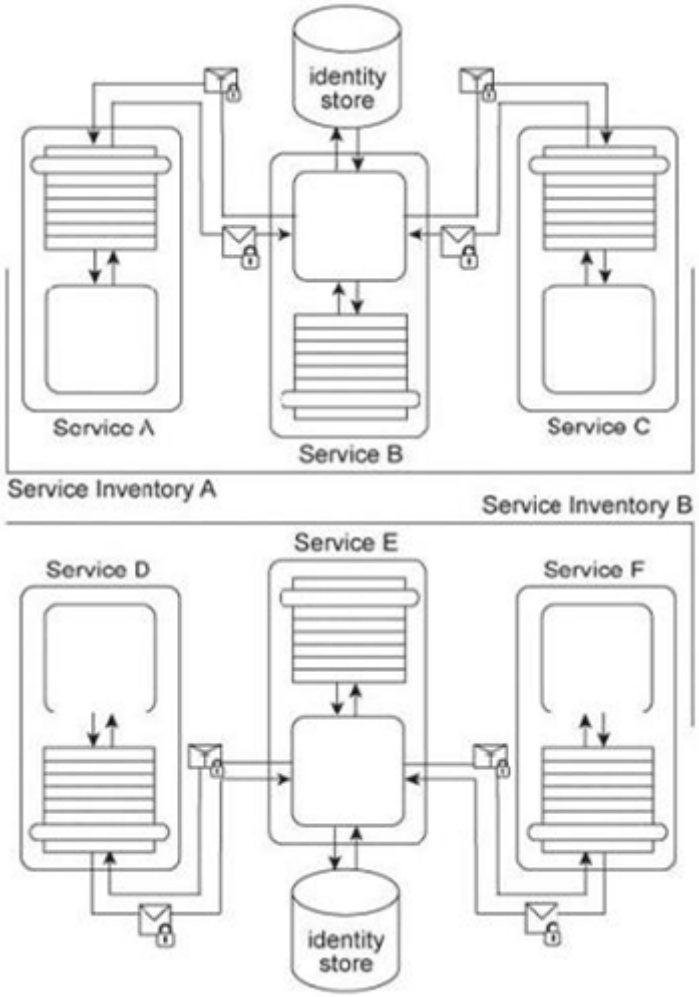
A

Question 3

Question Type: MultipleChoice

Services A, B, and C reside in Service Inventory A and Services D, E, and F reside in Service Inventory B .Service B is an authentication broker that issues WS-Trust based SAML tokens to Services A and C upon receiving security credentials from Services A and C .Service E is an authentication broker that issues WS-Trust based SAML tokens to Services D and F upon receiving security credentials from Services D and E .Service B uses the Service Inventory A identify store to validate the security credentials of Services A and C

.Service E uses the Service Inventory B identity store to validate the security credentials of Services D and F .It is decided to use Service E as the sole authentication broker for all services in Service Inventories A and B .Service B is kept as a secondary authentication broker for load balancing purposes. Specifically, it is to be used for situations where authentication requests are expected to be extra time consuming in order to limit the performance burden on Service E .Even though Service B has all the necessary functionality to fulfill this new responsibility, only Service E can issue SAML tokens to other services. How can these architectures be modified to support these new requirements?


identity store
Service A
Service B
Service C
Service Inventory A
Service Inventory B
Service D
Service E
Service F
identity store

Options:

A- When time consuming authentication requests are identified, Service E can forward them to Service B .Upon performing the authentication, Service B sends its own signed SAML token to Service E .Because Service E trusts Service B .it can use the Service B-specific SAML token to issue an official SAML token that is then sent to the original service consumer (that requested authentication) and further used by other services.

B- To provide load balancing, a service agent needs to be implemented to intercept all incoming requests to Service E .The-service agent uses a random distribution of the authentication requests between Service B and Service E .Because the request messages are distributed in a random manner, the load between the two authentication brokers is balanced.

C- Because both Service B and Service E issue SAML tokens, these tokens are interchangeable. In order for both services to-receive the same amount of authentication requests, a shared key needs to be provided to them for signing the SAML tokens. By signing the SAML tokens with the same key, the SAML tokens generated by Service B cannot be distinguished from the SAML tokens generated by Service E .

D- Because the federation requirements ask for SAML tokens generated by Service E, Service B cannot function as an-authentication broker. To address the load balancing requirement, a new utility service needs to be introduced to provide functionality that is redundant with Service E .This essentially establishes a secondary authentication broker to which Service E can defer time-consuming authentication tasks at runtime.

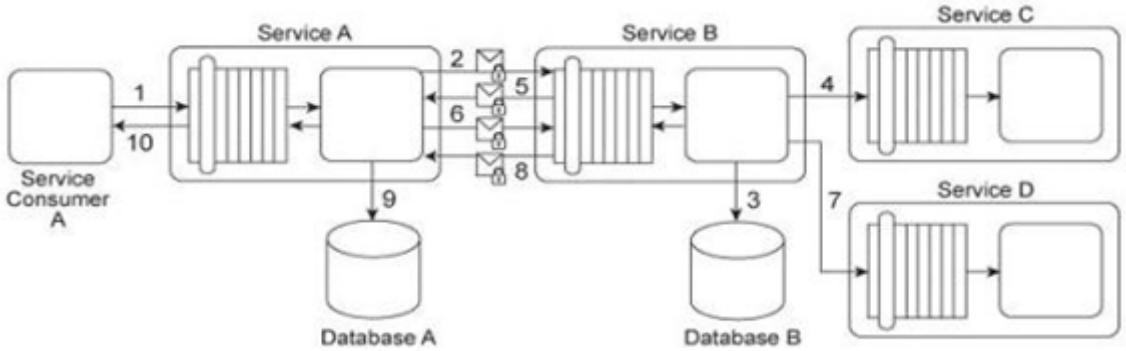
Answer:

B

Question 4

Question Type: MultipleChoice

Service Consumer A sends a request message to Service A (1), after which Service A sends a request message with security credentials to Service B (2). Service B authenticates the request and, if the authentication is successful, writes data from the request message into Database B (3). Service B then sends a request message to Service C (4), which is not required to issue a response message. Service B then sends a response message back to Service A (5). After processing Service B's response, Service A sends another request message with security credentials to Service B (6). After successfully authenticating this second request message from Service A, Service B sends a request message to Service D (7). Service D is also not required to issue a response message. Finally, Service B sends a response message to Service A (8), after which Service A records the response message contents in Database A (9) before sending its own response message to Service Consumer A (10). To use Service A, Service Consumer A is charged a per usage fee. The owner of Service Consumer A has filed a complaint with the owner of Service A, stating that the bills that have been issued are for more usage of Service A than Service Consumer A actually used. Additionally, it has been discovered that malicious intermediaries are intercepting and modifying messages being sent from Service B to Services C and D .Because Services C and D do not issue response messages, the resulting errors and problems were not reported back to Service B .Which of the following statements describes a solution that correctly addresses these problems?



Options:

A- The Data Confidentiality and Data Origin Authentication patterns need to be applied in order to establish message-layer-confidentiality and integrity for messages sent to Services C and D .The Direct Authentication pattern can be applied to require that service consumer be authenticated in order to use Service A .

B- Messages sent to Services C and D must be protected using transport-layer encryption in order to ensure data confidentiality. Service consumers of Service A must be authenticated using X.509 certificates because they can be reused for several request messages.

C- Apply the Service Perimeter Guard and the Message Screening patterns together to establish a perimeter service between Service Consumer A and Service A .The perimeter service screens and authenticates incoming request messages from Service Consumer A .After successful authentication, the perimeter service generates a signed SAML assertion that is used by the subsequent services to authenticate and authorize the request message and is also carried forward as the security credential included in messages sent to Services C and D .

D- Apply the Brokered Authentication to establish an authentication broker between Service Consumer A and Service A that can carry out the Kerberos authentication protocol. Before invoking Service A, Service Consumer A must request a ticket granting ticket and then it must request service granting tickets to all services in the service composition, including Services C and D .Messages sent by Service B to Services C and D must further be encrypted with the public key of Service Consumer A .

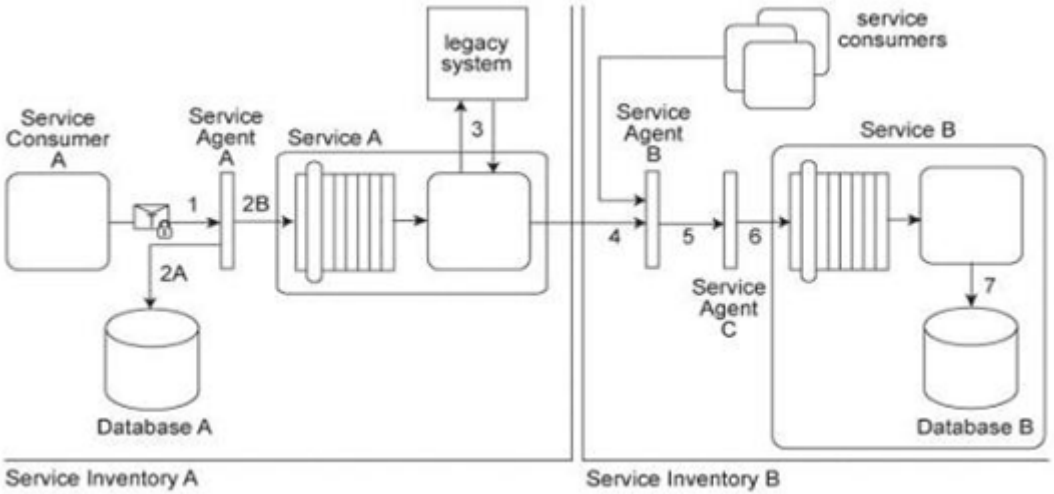
Answer:

A

Question 5

Question Type: MultipleChoice

Service Consumer A sends a request message with an authentication token to Service A, but before the message reaches Service A, it is intercepted by Service Agent A (1). Service Agent A validates the security credentials and also validates whether the message is compliant with Security Policy A .If either validation fails, Service Agent A rejects the request message and writes an error log to Database A (2A). If both validations succeed, the request message is sent to Service A (2B). Service A retrieves additional data from a legacy system (3) and then submits a request message to Service B Before arriving at Service B, the request message is intercepted by Service Agent B (4) which validates its compliance with Security Policy SIB then Service Agent C (5) which validates its compliance with Security Policy B .If either of these validations fails, an error message is sent back to Service A .that then forwards it to Service Agent A so that it the error can be logged in Database A (2A). If both validations succeed, the request message is sent to Service B (6). Service B subsequently stores the data from the message in Database B (7). Service A and Service Agent A reside in Service Inventory A .Service B and Service Agents B and C reside in Service Inventory B .Security Policy SIB is used by all services that reside in Service Inventory B .Service B can also be invoked by other service from within Service Inventory B .Request messages sent by these service consumers must also be compliant with Security Policies SIB and B .New services are being planned for Service Inventory A .To accommodate service inventory-wide security requirements, a new security policy (Security Policy SIA) has been created. Compliance to Security Policy SIA will be required by all services within Service Inventory A .Some parts of Security Policy A and Security Policy SIB are redundant with Security Policy SIA .How can the Policy Centralization pattern be correctly applied to Service Inventory A without changing the message exchange requirements of the service composition?



Options:

A- The parts of Security Policy A and Security Policy SIB that are redundant with Security Policy SIA are removed so that there is no overlap among these three security policies. A new service agent is introduced into Service Inventory A to validate compliance to the new Security Policy SIA prior to messages being validated by Service Agent A .Another new service agent is introduced into Service Inventory B to validate compliance to the new Security Policy SIA prior to messages being validated by Service Agents B and C .

B- The parts of Security Policy A that are redundant with Security Policy SIA are removed so that there is no overlap between these two security policies. A new service agent is introduced into Service Inventory A to validate compliance to the new Security Policy SIA prior to messages being validated by Service Agent A .

C- The parts of Security Policy A and Security Policy SIB that are redundant with Security Policy SIA are removed so that there is no overlap among these three security policies. Service Agent A is updated so that it can validate messages for compliance with both Security Policy A and Security Policy SIA .Service Agent B is updated so that it can validate messages for compliance with both Security

Policy SIA and Security Policy SIB .Service Agent C remains unchanged.

D- Due to the amount of overlap among Security Policy A, Security Policy SIA, and Security Policy SIB, the Policy Centralization pattern cannot be correctly applied without changing the message exchange requirements of the service composition.

Answer:

B

Question 6

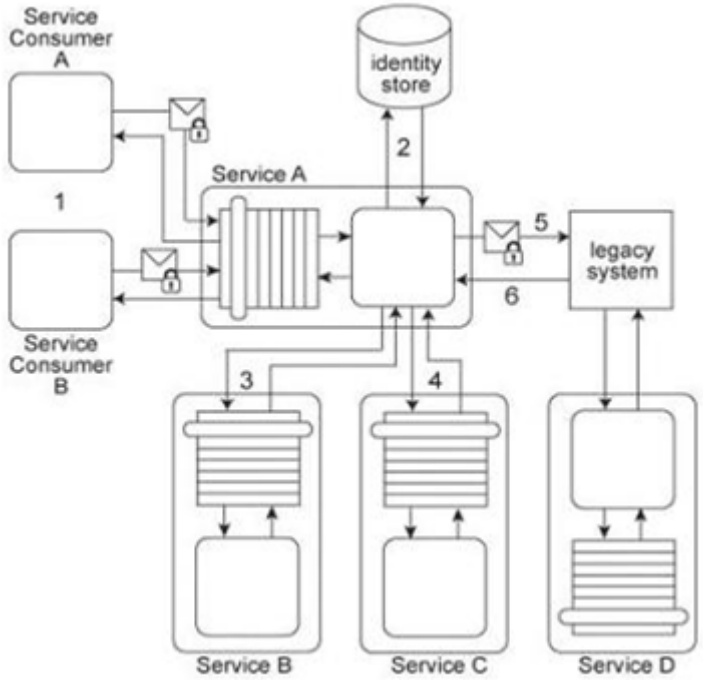
Question Type: **MultipleChoice**

Service A has two specific service consumers, Service Consumer A and Service Consumer B (1). Both service consumers are required to provide security credentials in order for Service A to perform authentication using an identity store (2). If a service consumer's request message is successfully authenticated, Service A processes the request by exchanging messages with Service B (3) and then Service C (4). With each of these message exchanges, Service A collects data necessary to perform a query against historical data stored in a proprietary legacy system. Service A's request to the legacy system must be authenticated (5). The legacy system only provides access control using a single account. If the request from Service A is permitted, it will be able to access all of the data stored in the legacy system. If the request is not permitted, none of the data stored in the legacy system can be accessed. Upon successfully retrieving the requested data (6), Service A generates a response message that is sent back to either Service Consumer A or B .The legacy system is also used independently by Service D without requiring any authentication. Furthermore, the legacy system has no auditing feature and therefore cannot record when data access from Service A or Service D occurs. If the legacy system encounters an error when processing a request, it generates descriptive error codes. This service composition architecture needs to be upgraded in order to fulfill

the following new security requirements:

1. Service Consumers A and B have different access permissions and therefore, data received from the legacy system must be filtered prior to issuing a response message to one of these two service consumers.

2. Service Consumer A's request messages must be digitally signed, whereas request messages from Service Consumer B do not need to be digitally signed. Which of the following statements describes a solution that fulfills these requirements?



Options:

A- The Trusted Subsystem pattern is applied by introducing a utility service that encapsulates the legacy system. To support-access by service consumers issuing request messages with and without digital signatures, policy alternatives are added to Service A's service contract. Service A authenticates the service consumer's request against the identity store and verifies compliance to the policy. Service A then creates a signed SAML assertion containing an authentication statement and the authorization decision. The utility service inspects the signed SAML assertions to authenticate the service consumer and then access the legacy system using a single account. The data returned by the legacy system is filtered by the utility service, according to the information in the SAML assertions.

B- The Trusted Subsystem pattern is applied by introducing a utility service that encapsulates the legacy system. Two different policies are created for Service A's service contract, only one requiring a digitally signed request message. The utility service accesses the legacy system using the single account. Service A authenticates the service consumer using the identity store and, if successfully authenticated, Service A send a message containing the service consumer's credentials to the utility service. The identity store is also used by the utility service to authenticate request messages received from Service A .The utility service evaluates the level of authorization of the original service consumer and filters data received from the legacy system accordingly.

C- The Trusted Subsystem pattern is applied by introducing a utility service that encapsulates the legacy system. After successful authentication, Service A creates a signed SAML assertion stating what access level the service consumer has. The utility service inspects the signed SAML assertion in order to authenticate Service A .The utility service accesses the legacy system using the account information originally provided by Service Consumer A or B .The utility service evaluates the level of authorization of the original service consumer and filters data received from the legacy system accordingly.

D- The Trusted Subsystem pattern is applied together with the Message Screening pattern by introducing a utility service that-encapsulated the legacy system and contains message screening logic. First, the utility service evaluates the incoming request messages to ensure that it is digitally signed, when necessary. After successful verification the request message is authenticated, and Service A performs the necessary processing. The data returned from the legacy system is filtered by the utility service's message screening logic in order to ensure that only authorized data is returned to Service Consumers A and B .

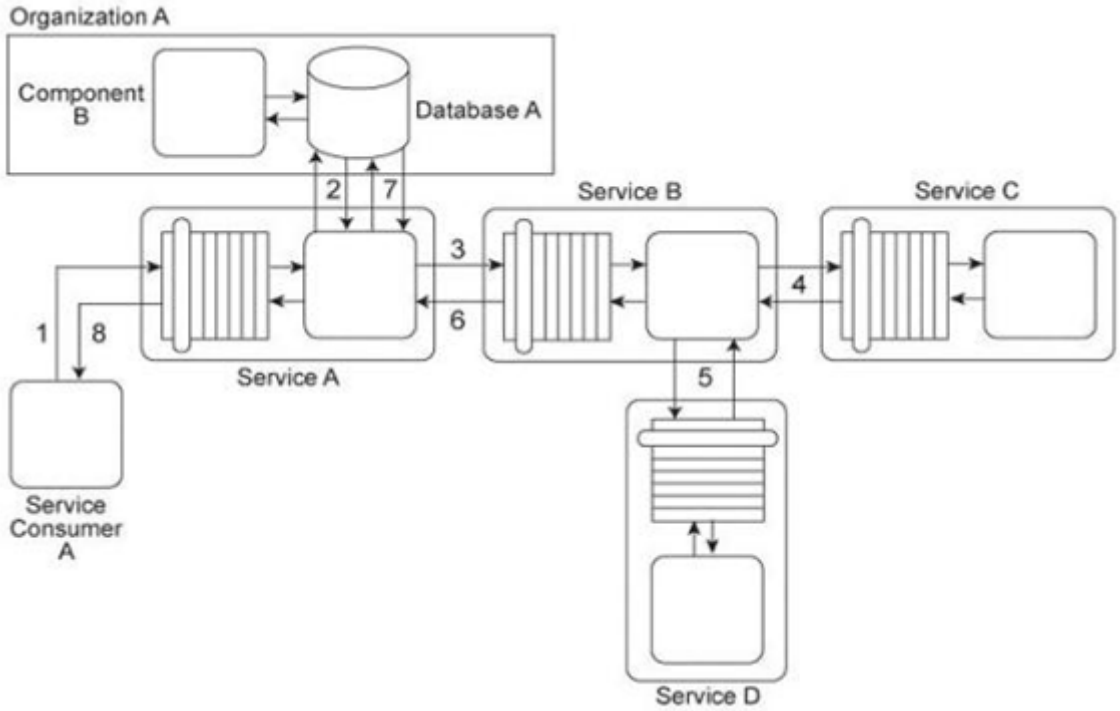
Answer:

A

Question 7

Question Type: MultipleChoice

Service Consumer A sends a request message to Service A (1) after which Service A retrieves financial data from Database A (2). Service A then sends a request message with the retrieved data to Service B (3). Service B exchanges messages with Service C (4) and Service D (5), which perform a series of calculations on the data and return the results to Service A .Service A uses these results to update Database A (7) and finally sends a response message to Service Consumer A (8). Component B has direct, independent access to Database A and is fully trusted by Database A .Both Component B and Database A reside within Organization A .Service Consumer A and Services A, B, C, and D are external to the organizational boundary of Organization A .Service A has recently experienced an increase in the number of requests from Service Consumer A .However, the owner of Service Consumer A has denied that Service Consumer A actually sent these requests. Upon further investigation it was determined that several of these disclaimed requests resulted in a strange behavior in Database A, including the retrieval of confidential data. The database product used for Database A has no feature that enables authentication of consumers. Furthermore, the external service composition (Services A, B, C, D) must continue to operate at a high level of runtime performance. How can this architecture be improved to avoid unauthenticated access to Database A while minimizing the performance impact on the external service composition?



Options:

A- Service Consumer A generates a pair of private/public keys (Public Key E and Private KeyD) and sends the public key to-Service A .Service A can use this key to send confidential messages to Service Consumer A because messages encrypted by the public key of Service Consumer A-can only be decrypted by Service A The Data Origin Authentication pattern can be further applied so that Service A can authenticate Service Consumer A by verifying the digital signature on request messages. The Message Screening pattern is applied to a utility service that encapsulates Database A in order to prevent harmful input.

B- The Brokered Authentication pattern is applied so that each service consumer generates a pair of private/public keys and sends the public key to Service A .When any service in the external service composition (Services A, B, C, and D) sends a request message to another service, the request message is signed with the private key of the requesting service (the service acting as the service consumer). The service then authenticates the request using the already established public key of the service consumer. If authentication is successful, the service generates a symmetric session key and uses the public key of the service consumer to securely send the session key back to the service consumer. All further communication is protected by symmetric key encryption. Because all service consumers are authenticated, all external access to Database A is secured.

C- A utility service is established to encapsulate Database A and to carry out the authentication of all access to the database by Service A and any other service consumers. To further support this functionality within the utility service, an identity store is introduced. This identity store is also used by Service A which is upgraded with its own authentication logic to avoid access by malicious service consumers pretending to be legitimate service consumers. In order to avoid redundant authentication by services within the external service composition, Service A creates a signed SAML assertion that contains the service consumer's authentication and authorization information.

D- Implement a firewall between Service Consumer A and Service A .All access to Service A is then controlled by the firewall rules. The firewall contains embedded logic that authenticates request messages and then forwards permitted messages to Service A .Moreover, the firewall can implement the Message Screening pattern so that each incoming message is screened for malicious content. This solution minimizes the security processing performed by Service A in order to maintain the performance requirements of the external service composition.

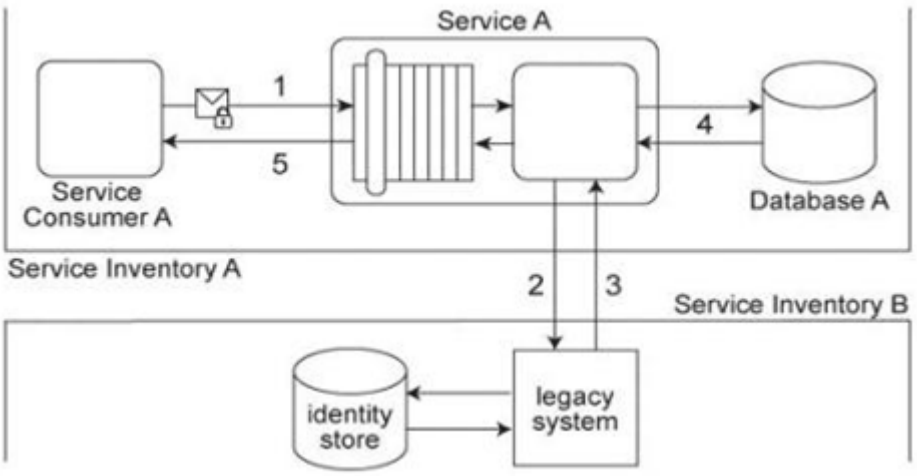
Answer:

C

Question 8

Question Type: MultipleChoice

Service Consumer A submits a request message with security credentials to Service A (1). The identity store that Service A needs to use in order to authenticate the security credentials can only be accessed via a legacy system that resides in a different service inventory. Therefore, to authenticate Service Consumer A, Service A must first forward the security credentials to the legacy system (2). The legacy system then returns the requested identity to Service A (3). Service A authenticates Service Consumer A against the identity received from the legacy system. If the authentication is successful, Service A retrieves the requested data from Database A (4), and returns the data in a response message sent back to Service Consumer A (5). Service A belongs to Service Inventory A which further belongs to Security Domain A and the legacy system belongs to Service Inventory B which further belongs to Security Domain B .(The legacy system is encapsulated by other services within Service Inventory B, which are not shown in the diagram.) These two security domains trust each other. Communication between Service A and the legacy system is kept confidential using transport-layer security. No intermediary service agents currently exist between the two service inventories. However, it has been announced that due to the introduction of new systems, some intermediary service agents may be implemented in the near future. Additionally, the legacy system has been scheduled for retirement and will be replaced by a new identity management system that will provide a new identity store. Because the new identity store will need to serve many different systems, there are concerns that it could become a performance bottleneck. As a result, services (including Service A and other services in Security Domains A and B) will not be allowed to directly access the new identity store. Which of the following statements describes a solution that can accommodate the requirements of the new identity store, the authentication requirements of Service A, and can further ensure that message exchanges between Security Domains A and B remain confidential after intermediary service agents are introduced?



Options:

A- Apply the Trusted Subsystem pattern to implement a utility service abstracting the new identity management system. Service A forwards Service Consumer As credentials to the utility service to verify Service Consumer As identity. The utility service authenticates the request originating from Service A .After successful authentication, the utility service uses its own credentials to retrieve the requested identity, and then send the identity to Service A, Therefore, effectively reducing the processing need of the identity management system. The current transport-layer security can still be used, in order to secure the communication between Service A and the new utility service, as it more efficient than the message-layer security.

B- Apply the Trusted Subsystem pattern by abstracting away the new identity management system using a utility service that authenticates the request from Service A and then uses its own credentials to retrieve the requested identity from the new identity management system. For the utility service to authenticate Service As request, it needs to be provisioned with a new identity database that contains identities for all authorized service consumers of the new utility service. In order to secure the communication between Service A and the new utility service, use message-layer security as it provides security over multiple hops considering the need to

secure the message in case an intermediary is introduced in future.

C- Replicate the identity database used by the new identity management system. Because the Security Domains A and B trust each other, protection of the identity store is guaranteed. Use Service Agents to monitor changes to the identity database used by the new identity management system and to update the replica. This would satisfy the security needs of Service A, would eliminate the need to request services from Service Inventory B, and ensure that current identity information is available for Service A .Because Service A would not need to access services across different trust domains, the current transport-layer security is sufficient.

D- Apply the Brokered Authentication pattern to establish an authentication broker. Instead of Service A directly authenticating-Service Consumer A, Service Consumer A submits a request message with security credentials to the authentication broker, which authenticates Service Consumer A against the new identity store and then issues a SAML token to Service Consumer A that it can use for message exchanges with other services, if necessary. In order to secure cross-service inventory message exchanges, the Data Confidentiality pattern is applied to establish message-layer security.

Answer:

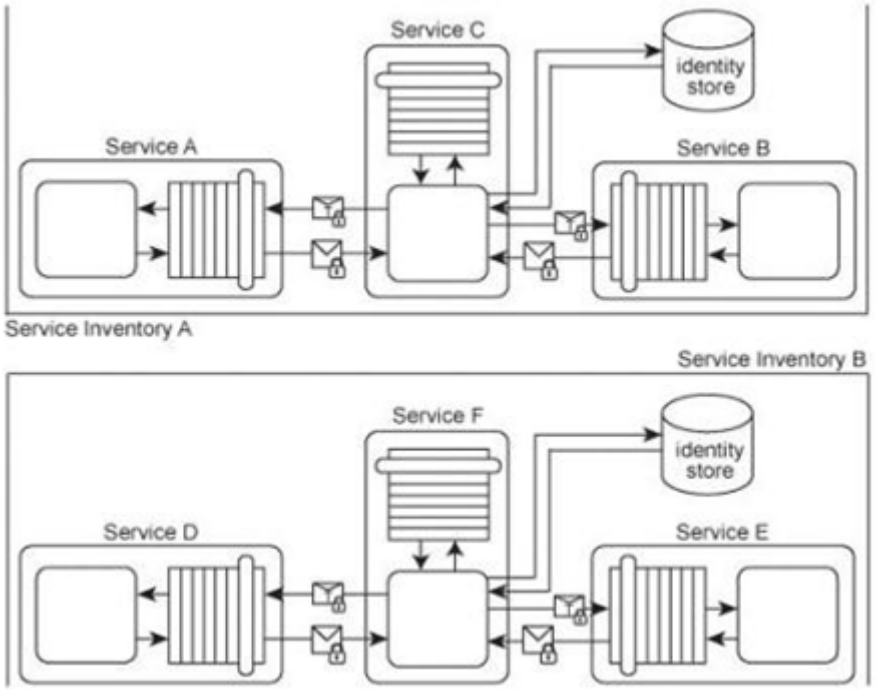
D

Question 9

Question Type: MultipleChoice

Services A, B and C belong to Service Inventory A .Services D, E and F belong to Service Inventory B .Service C acts as an authentication broker for Service Inventory A .Service F acts as an authentication broker for Service Inventory B .Both of the authentication brokers use Kerberos-based authentication technologies. Upon receiving a request message from a service consumer,

Services C and F authenticate the request using a local identity store and then use a separate Ticket Granting Service (not shown) to issue the Kerberos ticket to the service consumer. Currently, tickets issued in one service inventory are not valid in the other. For example, if Service A wants to communicate with Services D or E, it must request a ticket from the Service Inventory B authentication broker (Service F). Because Service Inventory A and B trust each other, the current cross-inventory authentication is considered unnecessarily redundant. How can these service inventory architectures be improved to avoid redundant authentication?



Options:

A- Create a single, enterprise-wide service inventory by merging Service Inventories A and B .Instead of the current Kerberos-based brokered authentication, the merged service inventory can use X.509 digital certificates to remove the burden from the local authentication brokers. Designate either Service C or Service F as the central authentication service with the responsibility to validate service consumer X.509 digital certificates. After successful validation, the authentication service can issue a signed SAML token to be used within the entire service inventory.

B- The same Kerberos tickets can be used across both service inventories by updating the security policies of the services that require Kerberos tickets. Because each authentication broker issues Kerberos tickets, the only difference between these tickets is the identity of the issuer. For-example, because services in Service Inventory A already accept Kerberos tickets issued by Service C, Service F just needs to be included in the security policies of these services. Similarly, services in Service Inventory B that accept Kerberos tickets issued by Service F need to include the acceptance of Kerberos tickets issued by Service C in their security policies.

C- A trust relationship needs to be established between the two authentication brokers. This trust relationship can enable the authentication brokers to accept Kerberos tickets issued by each other.

D- Replace Services C and F with a single authentication broker so that one single token can be used with services across both service inventories. This can be achieved by merging the content of the two identity stores.

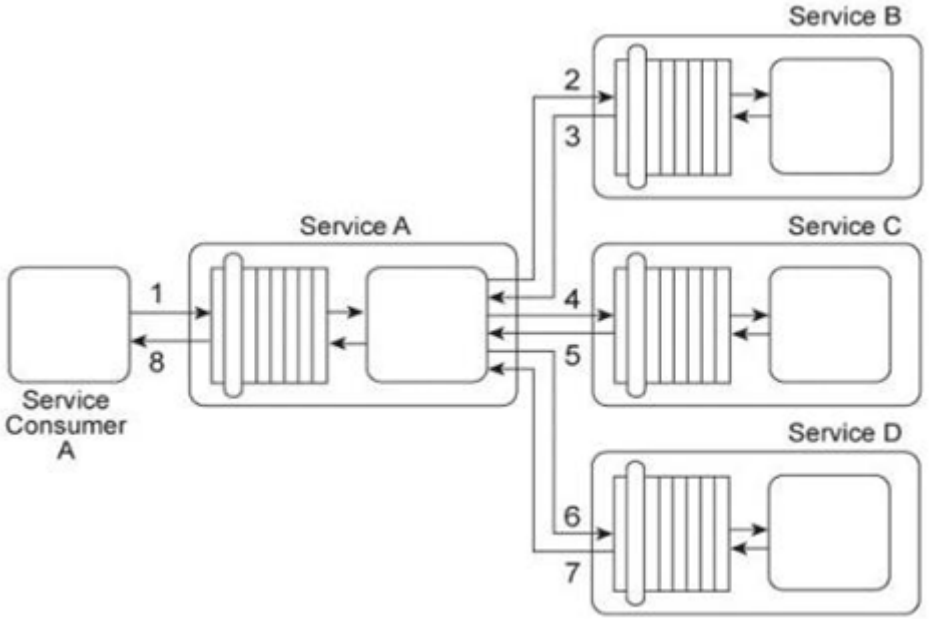
Answer:

C

Question 10

Question Type: MultipleChoice

Service A provides a data retrieval capability that can be used by a range of service consumers, including Service Consumer A, In order to retrieve the necessary data. Service Consumer A first sends a request message to Service A (1). Service A then exchanges request and response messages with Service B (2, 3). Service C (4, 5), and Service D (6. 7). After receiving all three response messages from Services B .C .and D, Service A assembles the collected data into a response message that it returns to Service Consumer A (8). The Service A data retrieval capability has been suffering from poor performance, which has reduced its usefulness to Service Consumer A .Upon studying the service composition architecture, it is determined that the performance problem can be partially attributed to redundant validation by service contracts for compliance to security policies. Services B and C have service contracts that contain the same two security policies. And, Service D has a service contract that contains a security policy that is also part of Service A's service contract. What changes can be made to the service contracts in order to improve the performance of the service composition while preserving the security policy compliance requirements?



Options:

A- Apply the Policy Centralization pattern in order to establish a single security policy for the entire service composition. The-redundant policies residing in the service contracts of Services A .B, C and D need to be removed and grouped together into one master policy definition enforced by Service A .This way, redundant policy validation is eliminated, thereby improving runtime performance.

B- Apply the Policy Centralization pattern in order to establish two centralized policy definitions and ensure that policy enforcement logic is correspondingly centralized. The first policy definition includes the redundant security policies from Services A and D and the second policy definition contains the redundant security policies from Services B and C .

C- All policies are analyzed for similarities, which are then extracted and, by applying the Policy Centralization pattern, combined into a single policy definition. This 'meta-policy' is then positioned to perform validation of the response message generated by Service A, prior to receipt by Service Consumer A .If validation fails, an alternative error message is sent to Service Consumer A instead.

D- Apply the Standardized Service Contract principle in order to remove redundancy within service contracts by ensuring that all four service contracts comply with the same policy standards. This further requires the application of the Service Abstraction principle to guarantee that policy definitions are sufficiently streamlined for performance reasons.

Answer:

B