DUMPSARENA

SOA Security Lab

SOA S90.20

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

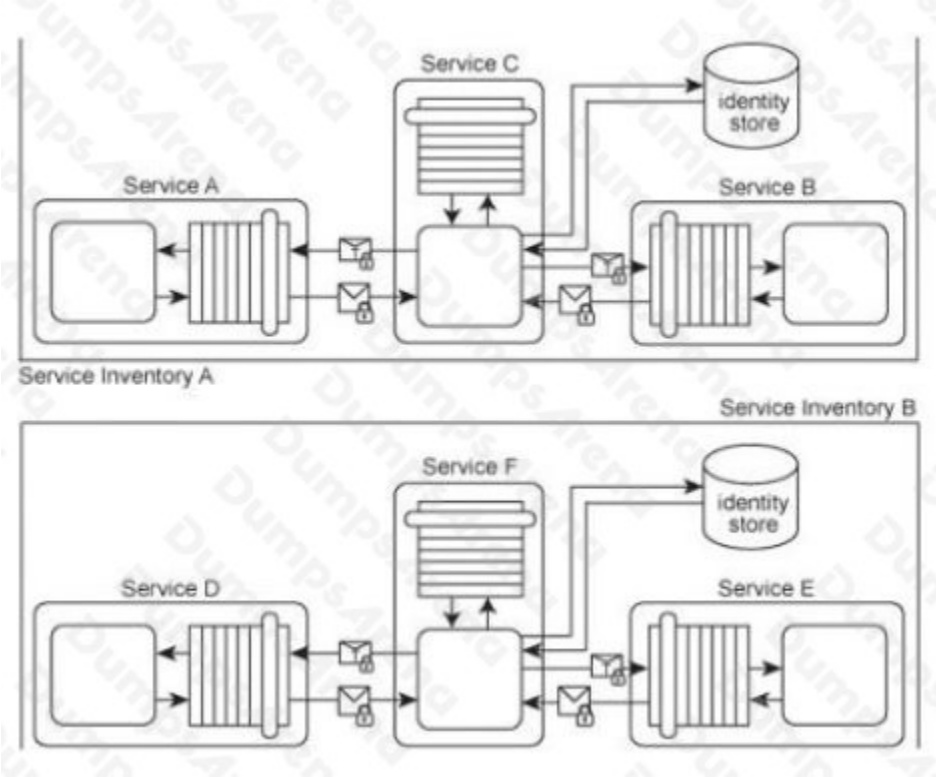
https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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?

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.

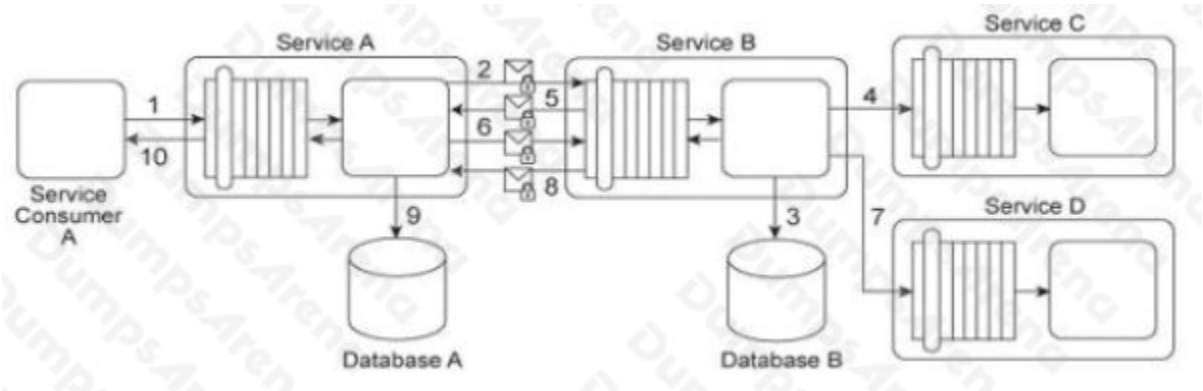
C. A trust relationship needs to be established between the two authentication brokers. This trust relationship can enable the authentication brokers to accept Kerberos tickets issued by each other.

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 NO: 2

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?

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

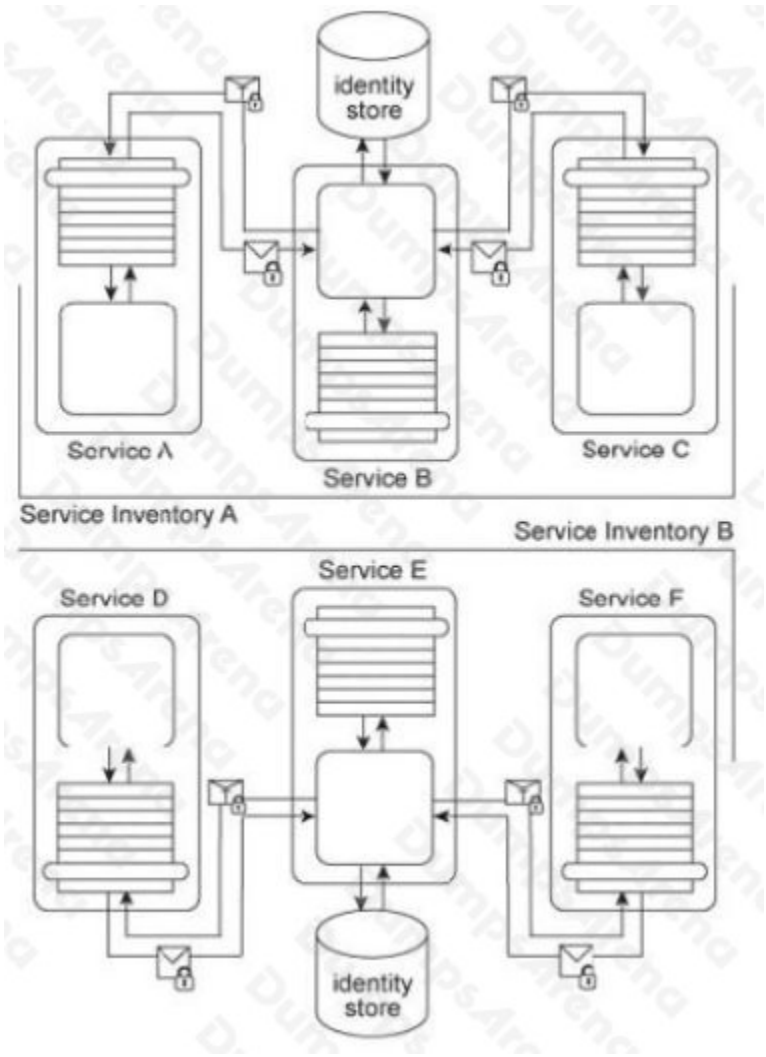
used by the subsequent services to authenticate and authorize the request message and is also carried forward as the security credential included in messages sent to Services C and D.

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 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 NO: 3

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.



To date, the two service inventories have existed independently from each other. However, a requirement has emerged that the services in Service Inventory A need to be able to use the services in Service Inventory B, and vice versa.

How can cross-service inventory message exchanges be enabled with minimal changes to the existing service inventory architectures and without introducing new security mechanisms?

A. Because SAML tokens cannot be used across multiple security domains, authentication brokers C and E need to be replaced with one single authentication broker so that one token issuer is used for all services across both of the service inventories.

B. The current security mechanism already fulfills the requirement because SAML tokens can be used across multiple security domains. The only change required is for each authentication broker to be configured so that it issues service inventory-specific assertions for SAML tokens originating from other service inventories.

C. The individual domain service inventories need to be combined into one enterprise service inventory. The Service Perimeter Guard pattern can be applied to establish a contact point for request messages originating from outside the service inventory. Within the service inventory, services no longer need to be authenticated because they are all part of the same trust boundary.

D. The Trusted Subsystem pattern is applied to encapsulate Services B and E using a central utility service that balances request and response messages exchanged between Services B and E, depending on which service inventory the messages originate from. The utility service also contains transformation logic to ensure that the SAML tokens issued by

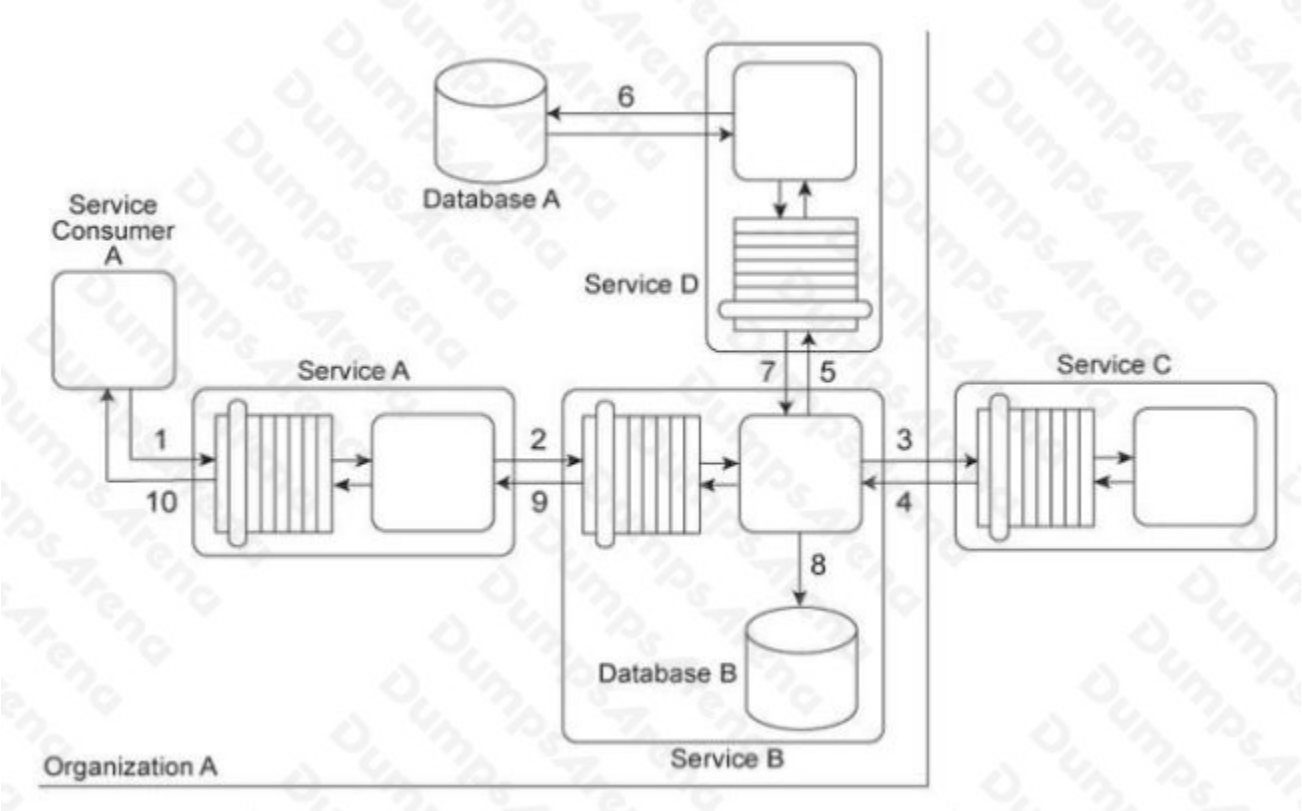
Services B and E are compatible. This guarantees that an issued SAML token can be used across Service Inventories A and B without further need for runtime conversion.

ANSWER: B

QUESTION NO: 4

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?

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 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 If a request message originates from an IP address not listed as one of the IP addresses associated with Service then the response message is rejected.

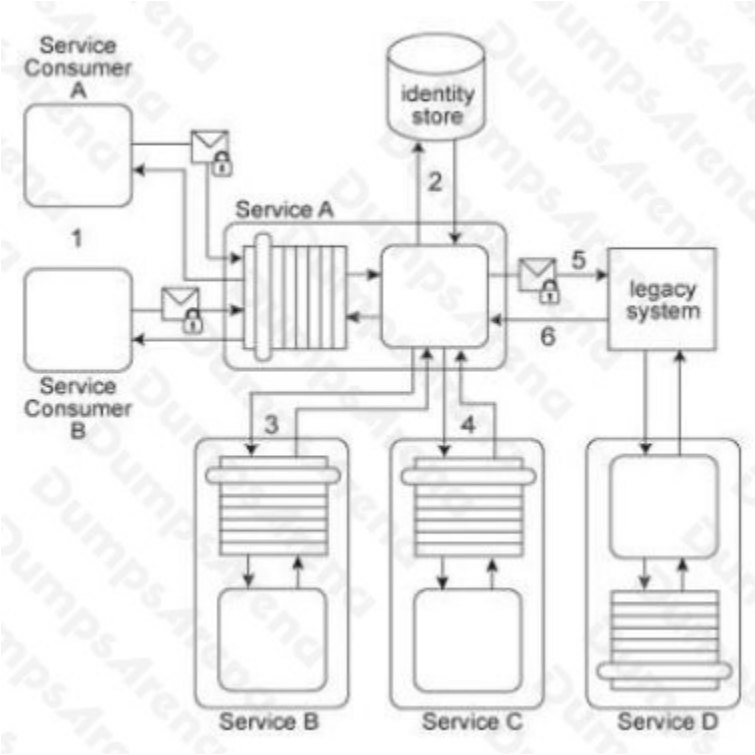
D. Apply the Direct Authentication pattern so that Service C is required to provide security credentials, such as Username tokens, with any response messages it sends to Service B. Furthermore, add logic to Service A so that it can validate security credentials passed to it via response messages from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

ANSWER: A

QUESTION NO: 5

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?

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