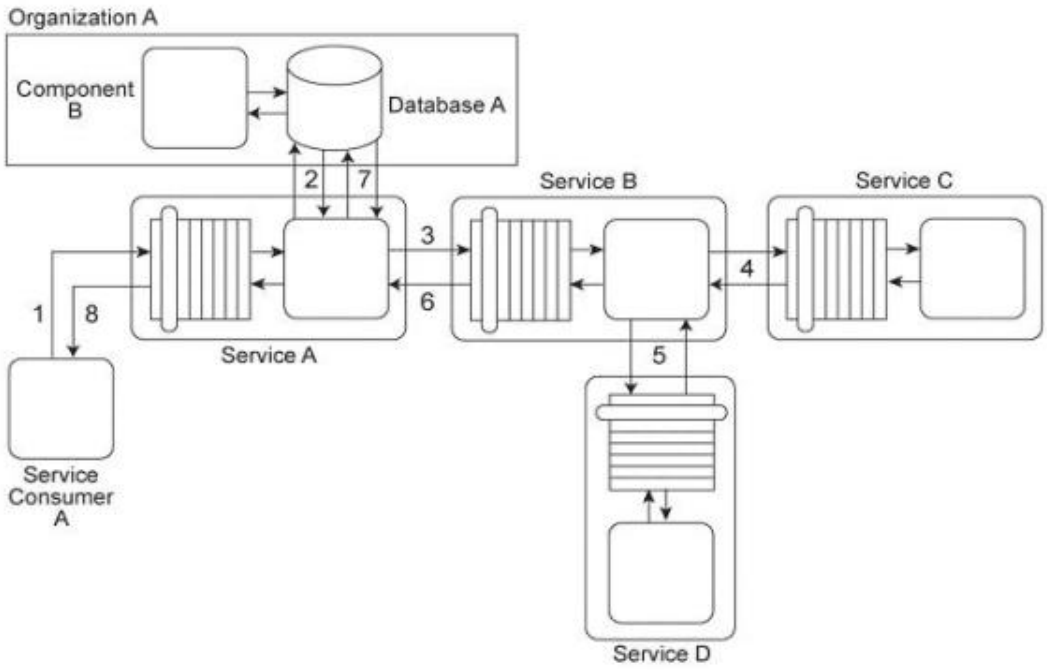
SOA S90-20A

SOA Security Lab

Version: 4.0

QUESTION NO: 1

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.



Component B is considered a mission critical program that requires guaranteed access to and fast response from Database A. Service A was recently the victim of a denial of service attack, which resulted in Database A becoming unavailable for extended periods of time (which further compromised Component B). Additionally, Services B, C, and D have repeatedly been victims of malicious intermediary attacks, which have further destabilized the performance of Service A.

How can this architecture be improved to prevent these attacks?

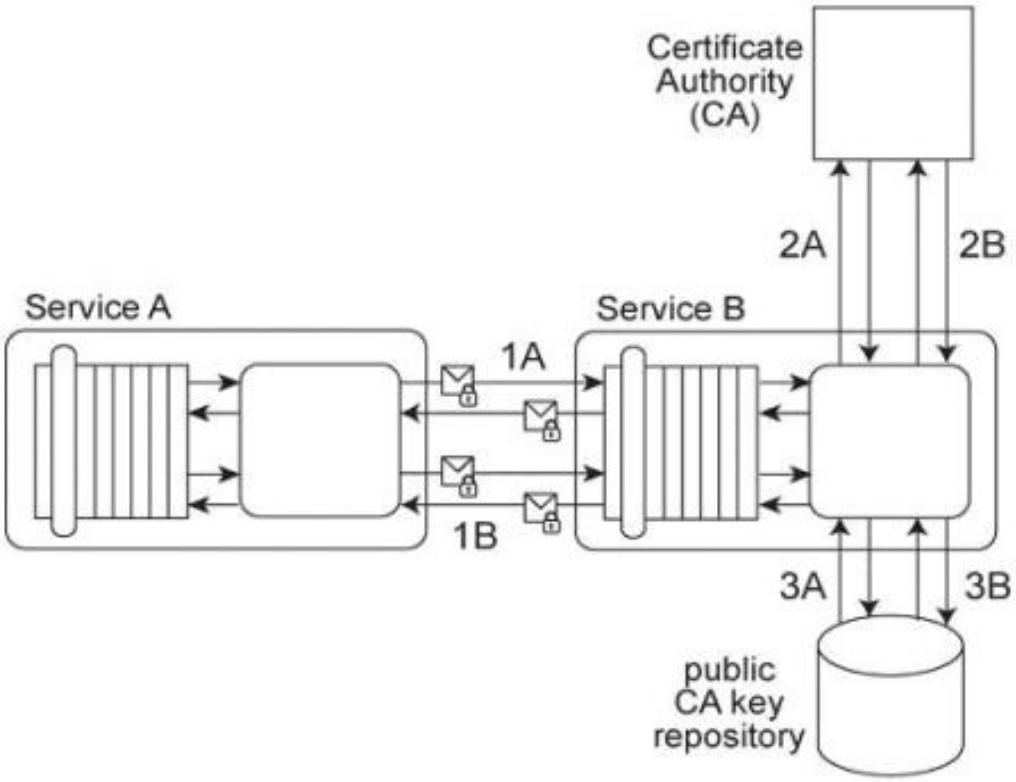
A. A utility service is created to encapsulate Database A and to assume responsibility for authenticating all access to the database by Service A and any other service consumers. Due to the mission critical requirements of Component B, the utility service further contains logic that strictly limits the amount of concurrent requests made to Database A from outside the organizational boundary. The Data Confidentiality and Data Origin Authentication patterns are applied to all message exchanged within the external service composition in order to establish message-layer security.

B. Service Consumer A generates a private/public key pair and sends this public key and identity information to Service A. Service A generates its own private/public key pair and sends it back to Service Consumer A. Service Consumer A uses the public key of Service A to encrypt a randomly generated session key and then sign the encrypted session key with the private key. The encrypted, signed session key is sent to Service A. Now, this session key can be used for secure message-layer communication between Service Consumer A and Service A. The Service Perimeter Guard pattern is applied to establish a perimeter service that encapsulates Database A in order to authenticate all external access requests.
C. Services B, C, and D randomly generate Session Key K, and use this key to encrypt request and response messages with symmetric encryption. Session Key K is further encrypted itself asymmetrically. When each service acts as a service consumer by invoking another service, it decrypts the encrypted Session Key K and the invoked service uses the key to decrypt the encrypted response. Database A is replicated so that only the replicated version of the database can be accessed by Service A and other external service consumers.
D. The Direct Authentication pattern is applied so that when Service Consumer A submits security credentials, Service A will be able to evaluate the credentials in order to authenticate the request message. If the request message is permitted, Service A invokes the other services and accesses Database A. Database A is replicated so that only the replicated version of the database can be accessed by Service A and other external service consumers.

Answer: A
Explanation:

QUESTION NO: 2

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.



To fulfill a new security requirement, Service A needs to be able to verify that the response message sent by Service B has not been modified during transit. Secondly, the runtime performance between Services A and B has been unacceptably poor and therefore must be improved without losing the ability to verify Service A's security credentials. It has been determined that the latency is being caused by redundant security processing carried out by Service B.

Which of the following statements describes a solution that fulfills these requirements?

A. Apply the Trusted Subsystem pattern to introduce a utility service that performs the security processing instead of Service B. The utility service can verify the security credentials of request messages from Service A and digitally sign messages sent to Service A to enable verification of message integrity. Furthermore, the utility service can perform the verification of security credentials submitted by Service A only once per runtime service activity. After the first messageexchange, it can issue a SAML token to Service A that gets stored within the current session. Service A can then use this session-based token with subsequent message exchange. Because SAML tokens have a very small validity period (in contrast to X.509 certificates), there is no need to perform a revocation check with every message exchange.
B. Service B needs to be redesigned so that it performs the verification of request messages from Service A only for the first message exchange during the runtime service activity. Thereafter, it can issue a SAML token to Service A that gets stored within the current session. Service A then uses this session-based token with subsequent message exchanges. Because SAML tokens have a very small validity period (in contrast to X.509 certificates), there is no need to perform a revocation check with every message exchange.
C. WS-SecurityPolicy transport binding assertions can be used to improve performance via

transport-layer security The use of symmetric keys can keep the encryption and decryption overhead to a minimum, which will further reduce the latency between Service A and Service B. By encrypting the messages, attackers cannot modify message contents, so no additional actions for integrity verification are needed.

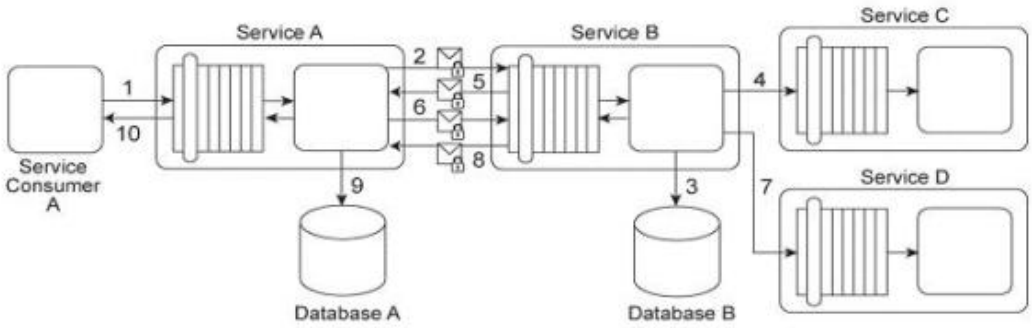
D. The Data Origin Authentication pattern can be applied together with the Service Perimeter Guard pattern to establish a perimeter service that can verify incoming request messages sent to Service B and to filter response messages sent to Service A. The repository containing the verification information about the Certificate Authorities can be replicated in the trust domain of the perimeter service. When access is requested by Service A, the perimeter service evaluates submitted security credentials by checking them against the locally replicated repository. Furthermore, it can encrypt messages sent to Service A by Service B. and attach a signed hash value.

Answer: A

Explanation:

QUESTION NO: 3

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).



Services A and B use digital certificates to support message integrity and authentication. With every message exchange between the two services (2, 5, 6, 8), the digital certificates are used. It has been determined that both Databases A and B are vulnerable to malicious attackers that may

try to directly access sensitive data records. Furthermore, performance logs have revealed that the current exchange of digital certificates between Services A and B is unacceptably slow.

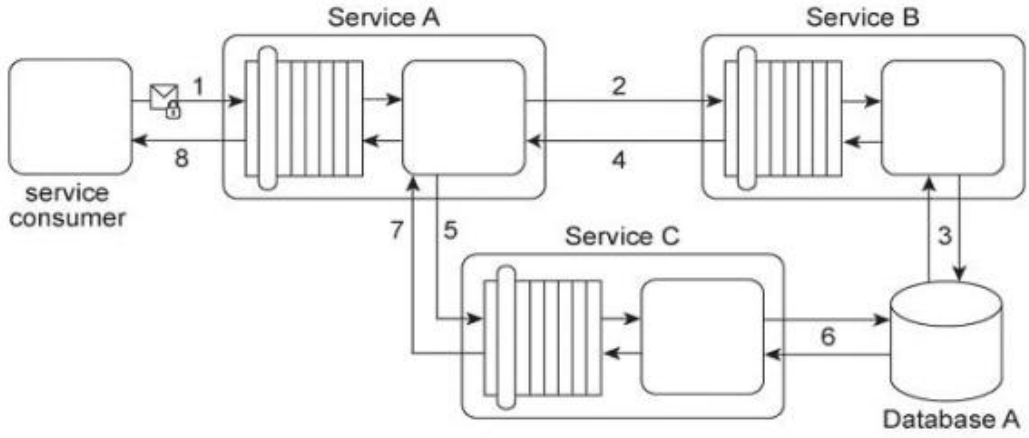
How can the integrity and authenticity of messages exchanged between Services A and B be maintained, but with improved runtime performance - and - how can Databases A and B be protected with minimal additional impact on performance?

A. Apply the Brokered Authentication pattern to establish an authentication broker that uses WS-Trust based SAML tokens for message exchanges between Services A and B. This eliminates the need for Service A to be repeatedly authenticated by Service B. Use the public key of Service A to encrypt Database A and use the public key of Service B to encrypt Database B.
B. Apply the Brokered Authentication pattern to establish an authentication broker that uses WS-SecureConversation securitycontext tokens (SCTs) to generate and transmit a symmetric session key. The session key is used to encrypt and digitally sign messages exchanged between Services A and B. For each database the Trusted Subsystem pattern is applied to require authenticated access to the database and to prevent attackers from accessing the database directly
C. Apply the Direct Authentication pattern to establish mutual authentication between Services A and B using a shared identity store. Service A attaches a Username token to the first request message sent to Service B and Service B authenticates the request message using the shared identity store. Similarly, when Service B submits a response message to Service A. it attaches its own Username token that Service A then authenticates by also using the same shared identitystore. Database A is encrypted using the Service A password as a secret encryption key and Database B is encrypted using the Service B password as a secret encryption key.
D. Apply the Brokered Authentication pattern to establish an authentication broker that uses WS-Trust based SAML tokens for message exchanges between Services A and B. This eliminates the need for Service A to be repeatedly authenticated by Service B. Database A is encrypted using the Service A password as a secret encryption key and Database B is encrypted using the Service B password as a secret encryption key.

Answer: B
Explanation:

QUESTION NO: 4

Service A provides a customized report generating capability. Due to infrastructure limitations, the number of service consumers permitted to access Service A concurrently is strictly controlled. Service A validates request messages based on the supplied credentials (1). If the authentication of the request message is successful, Service A sends a message to Service B (2) to retrieve the required data from Database A (3). Service A stores the response from Service B (4) in memory and then issues a request message to Service C (5). Service C retrieves a different set of data from Database A (6) and sends the result back to Service A (7). Service A consolidates the data received from Services B and C and sends the generated report in the response message to its service consumer (8).



This service composition was recently shut down after it was discovered that Database A had been successfully attacked twice in a row. The first type of attack consisted of a series of coordinated request messages sent by the same malicious service consumer, with the intention of triggering a range of exception conditions within the database in order to generate various error messages. The second type of attack consisted of a service consumer sending request messages with malicious input with the intention of gaining control over the database server. This attack resulted in the deletion of database records and tables. An investigation revealed that both attacks were carried out by malicious service consumers that were authorized.

How can the service composition security architecture be improved to prevent these types of attacks?

A. Apply the Data Confidentiality pattern together with the Data Origin Authentication pattern. This establishes message-levelsecurity so that all messages are encrypted and digitally signed. Secondly, the Service A logic must be enhanced so that it can keep track of the trustworthiness of its service consumers If a request message originated from a trustworthy service consumer, then the request message is processed as normal. If the request message originates from a non-trustworthy service consumer, then the request message is rejected and an error message is returned to the service consumer.
B. Apply the Service Perimeter Guard pattern together with the Trusted Subsystem pattern. This establishes a perimeter service between Database A and any service that requires access to it (including Services B and C). The perimeter service evaluates incoming data requests and filters out those that can introduce a security risk. Only request messages issued by authorized services and service consumers are forwarded to Database A. Responses originating from Database A are further evaluated by the trusted subsystem to remove any unauthorized data. The two patterns together ensure that only authorized data is returned to the service consumer and that no request messages present a security threat to Database A.
C. Apply the Exception Shielding pattern together with the Message Screening pattern. This establishes new logic within Service A that screens incoming request messages for data-driven attacks (such as SQL injection and XPath injection attacks), and also evaluates whether exception details returned by Database A contains potentially confidential or unsafe information. Any inappropriate exception information is replaced with sanitized content.
D. Apply the Trusted Subsystem pattern to protect Database A from data-driven attacks and to

evaluate whether databaseresponses contain inappropriate data. The trusted subsystem maintains a snapshot of Database A and executes the original service consumer's request message against the snapshot. The processing logic that accesses the snapshot has limited privileges in order to prevent malicious attacks from overtaking the database. If no security violation is detected during the processing of the snapshot, then the original service consumer's request is forwarded to Database A. If an error message is generated during the processing of the snapshot, then it is returned to the original service consumer and the request is not forwarded to Database A.Because the error message was generated on the snapshot, it cannot contain unsafe information about Database A.

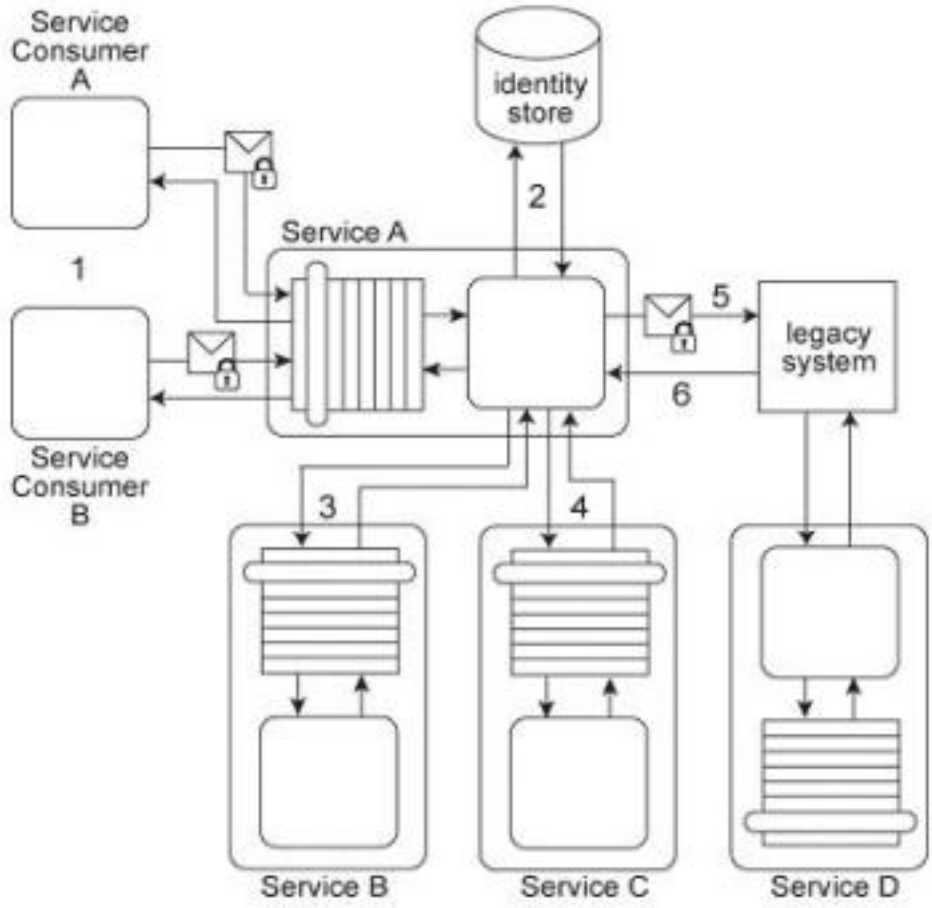
Answer: C

Explanation:

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 permission levels, and therefore, response messages sent to a service consumer must only contain data for which the service consumer is authorized. 2. All data access requests made to the legacy system must be logged. 3. Services B and C must be provided with the identity of Service A's service consumer in order to provide Service A with the requested data. 4. Response messages generated by Service A cannot contain confidential error information about the legacy system.

Which of the following statements provides solutions that satisfy these requirements?

A. To correctly enforce access privileges, Services B and C must share the identity store with Service A and directly authenticate Service Consumer A or B. Furthermore, Services B and C must each maintain two policies: one for Service Consumer A and one for Service Consumer B. After receiving a request message from a Service A. Services B and C must evaluate the validity of the request by using the identity store and the appropriate policy. Service Consumers A and B are required to submit the necessary security credentials to the legacy system as part of the request message sent to Service A. After verifying the credentials, the legacy systemeitherperforms the necessary processing orsends the response to Service A or denies access and sends an error message directly to Service Consumer A or B. The Message Screening pattern is applied to Service A so that it can perform message screening logic in order to filter out unauthorized data coming from the legacy system.
B. Apply the Trusted Subsystem pattern by introducing a new utility service that encapsulates data

access to the legacy system. After Service A authenticates a service consumer it creates a signed SAML assertion containing authentication and authorization information. The SAML assertions are used by Service A to convey the identity information of Service Consumer A or B to Services B and C. The utility service filters response messages to the service consumer based on the information in the SAML assertions. The utility service keeps a log of the all data access requests made to the legacy system. The Exception Shielding pattern is further applied to the utility service in order to prevent the leakage of confidential error information.

C. Apply the Service Perimeter Guard pattern to provide selective access privileges to Service Consumers A and B. The resulting perimeter service shares the identity store with Service A, which it uses to authenticate each request message. If authentication is successful, the request message is forwarded to Service A. Service A then also authenticates the service consumer and retrieves the service consumer's security profile from the identity store upon successful authentication. Each service consumer's security profile includes its authorized level of access. Service consumer authentication is subsequently performed using digital certificates. The Exception Shielding pattern is further applied to the perimeter service in order to prevent the leakage of confidential error information.

D. Apply the Trusted Subsystem pattern by introducing a new utility service that encapsulates data access to the legacy system. The utility service evaluates request messages by authenticating the service consumer against the identity store and also verifying the digital signature of each request. If the request is permitted, Service A forwards the service consumer's credentials to Services B and C, and to the legacy system. The response messages from Services B and C are returned to Service A, while responses from the legacy system are processed by the utility service. Logic is added to the utility service so that it can log access requests made to the legacy system.

Answer: B

Explanation:

QUESTION NO: 6

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.