PassQueen
a.k.a dumpsqueen.com

Certified Implementation Specialist - Service Mapping

ServiceNow CIS-SM

Version Demo

Total Demo Questions: 13

Total Premium Questions: 136

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Service Mapping Overview	24
Topic 2, Discovery Fundamentals	44
Topic 3, Service Mapping Configuration	16
Topic 4, Service Mapping Patterns	39
Topic 5, Service Mapping Administration	11
Topic 6, Mix Questions	2
Total	136

QUESTION NO: 1

Which is the most common risk that can negatively impact a Service Mapping engagement?

A. The customer is not using Active Directory for credential authentication

B. The customer external firewall only communicates on outbound port 80 and 443

C. The customer security team is not made aware early enough in the engagement of the credential requirements

D. The MID Server resource requirements are beyond capacity of the customer

ANSWER: C

Explanation:

The customer security team is not made aware early enough in the engagement of the credential requirements is correct because credential planning and security approval are foundational dependencies for Service Mapping discovery. Service Mapping uses MID Servers and configured credentials to connect to infrastructure components, collect identification and relationship data, and perform the discovery activities needed to build an accurate application-service map. Security teams commonly control the approval, creation, scope, storage, and permitted use of the required service accounts and network access. If they are engaged late, the project can be delayed while access is reviewed, accounts are provisioned, least-privilege permissions are agreed, or required connectivity is authorized. This affects the engagement schedule directly and can limit the data available for mapping until the dependency is resolved. Early collaboration lets the implementation team document credential types, target technologies, required privileges, MID Server placement, and governance expectations before mapping work begins. It also supports a controlled credential-management process rather than introducing unreviewed access late in delivery. ServiceNow documents that credentials are used by discovery patterns and other processes running through a MID Server, making credential readiness central to successful Service Mapping execution. See the ServiceNow Service Mapping credentials documentation and the ServiceNow Discovery credentials documentation.

QUESTION NO: 2

Which of the following are benefits a service map can bring during an Incident resolution? (Choose three.)

A. Quickly identifies any recent incidents that occurred on components of the impacted service.

B. Narrows down possible affected components when a service is impacted.

C. Helps reduce the number of unplanned changes in a customer environment.

D. Helps pinpoint code errors after a faulty application is identified.

E. Quickly identifies any recent changes performed on components of the impacted service.

ANSWER: A B E

Explanation:

A service map provides a current, visual view of the configuration items and dependency relationships that support a business service. This context helps an incident resolver understand the service topology quickly, rather than investigating individual infrastructure or application components in isolation. “Narrows down possible affected components when a service is impacted.” is a core incident-resolution benefit because the map shows the upstream and downstream dependencies that can be contributing to the outage or degradation.

“Quickly identifies any recent changes performed on components of the impacted service.” is also valuable because change activity is important troubleshooting context. When a service begins failing after a change, seeing relevant changes associated with mapped service components helps responders prioritize their investigation and correlate the incident with potential causes.

“Quickly identifies any recent incidents that occurred on components of the impacted service.” similarly supports faster diagnosis by exposing operational history for the service’s constituent components. Related incident patterns can reveal recurring failures, affected dependencies, and areas requiring focused analysis. Service Mapping is designed to provide this

service-aware dependency context for operational processes such as incident management. See ServiceNow Service Mapping and ServiceNow Service Mapping documentation.

QUESTION NO: 3

From Pattern Designer under the CI Attributes section, next to the name field, the key displayed in this example represents?

A. Tabular variable

B. Coalesce key

C. Criterion attribute

D. Custom variable

ANSWER: B

Explanation:

Coalesce key is correct. In ServiceNow Pattern Designer, a coalesce key identifies the attribute or combination of attributes used to determine whether a discovered configuration item corresponds to an existing record in the CMDB. During pattern execution, Service Mapping uses this identifying information to match the CI that is being discovered with a previously stored CI record. If a matching CI is found, the pattern can update that record rather than creating a duplicate; if no match exists, it can create the appropriate new CI. The key shown beside a CI attribute such as *name* therefore indicates that the attribute participates in CI identification and reconciliation for the pattern's result. This is especially important for maintaining CMDB data quality, because reliable identification rules help ensure that service maps represent consistent, nonduplicated infrastructure and application records. Pattern authors should select identifying attributes that are stable and meaningful for the CI class being discovered. ServiceNow's Service Mapping documentation describes Pattern Designer as the interface for creating and modifying discovery patterns, while CMDB identification and reconciliation controls how incoming discovery data is matched to CMDB records. See ServiceNow Service Mapping documentation and ServiceNow CMDB Identification and Reconciliation documentation.

QUESTION NO: 4

Given the CMDB class structure shown below, if an implementer were to extend the Server [cmdb_ci_server] table, which one of the following best describes the fields that would be inherited by the new table?

A. All fields configured for the Server [cmdb_ci_server] table and its child classes would be inherited.

B. All fields configured for the Server [cmdb_ci_server] table and its parent and child classes would be inherited.

C. No fields would be inherited from any class.

D. All fields configured for the Server [cmdb_ci_server] table and its parent classes would be inherited.

ANSWER: D

Explanation:

All fields configured for the Server [cmdb_ci_server] table and its parent classes would be inherited. In ServiceNow, extending a table creates a child table in the inheritance hierarchy. The new child table automatically includes the columns defined directly on its immediate parent, Server [cmdb_ci_server], as well as columns inherited by Server from every ancestor higher in the hierarchy. For CMDB classes, this commonly includes attributes established on foundational CI classes, allowing the specialized class to retain standard identification, lifecycle, ownership, and other shared CI data while adding fields specific to its own purpose.

This inheritance model is central to the CMDB class structure: parent-table fields are available to records in descendant classes, while a child class can introduce additional fields without changing the parent or sibling classes. The new table therefore receives the complete field set already available on Server through its parent lineage, and an implementer can then add any fields required for the specialized server type. ServiceNow's table-extension guidance describes how a child table

inherits fields from its parent, and CMDB documentation explains that CI classes are organized as an extensible class hierarchy. See ServiceNow: Extending tables and ServiceNow: CMDB class model.

QUESTION NO: 5

Which of the following are appropriate activities before starting Service Mapping discovery for a new application service? (Choose three.)

A. Validate that a MID Server can reach the entry point and relevant targets

B. Configure credentials with access to the target technologies

C. Confirm the entry point address, port, and protocol

D. Create all expected CI relationships manually in the CMDB

E. Install an agent on every server in the service

ANSWER: A B C

Explanation:

A successful mapping activity requires the appropriate technical access and a valid starting point. The implementer should confirm that a MID Server can reach the entry point and dependent infrastructure, configure credentials that permit discovery of the relevant targets, and validate the entry-point address, port, and protocol. These preparations allow Service Mapping to identify the application and follow its dependencies.

Creating manual CI relationships or manually drawing the expected topology is not required before mapping. Service Mapping discovers and creates the application dependency context from the configured entry point. See the Service Mapping documentation and Discovery credentials documentation.

QUESTION NO: 6

Which one of the following describes how a MID Server communicates with a ServiceNow instance?

A. Initiates on HTTPS

B. Responds on HTTPS

C. Responds on HTTP

D. Initiates on HTTP

ANSWER: A

Explanation:

The correct answer is **Initiates on HTTPS**. A MID Server is installed within an organization's internal network and creates an outbound, encrypted HTTPS connection to the ServiceNow instance. This outbound design is important because it lets the MID Server access internal resources, such as servers, applications, and network devices, without requiring the ServiceNow instance to make unsolicited inbound connections through the organization's firewall.

The MID Server uses the External Communication Channel (ECC) Queue to exchange work with the instance. It polls the instance over HTTPS for commands and returns the results through that same secure communication mechanism. In practice, the instance places work in the ECC Queue, and the MID Server retrieves and processes it after initiating contact. This architecture supports Service Mapping discovery and credentialed activities inside private networks while maintaining a controlled network boundary.

ServiceNow documents that MID Servers communicate with an instance using outbound HTTPS and that the MID Server's communication is managed through the ECC Queue. See the ServiceNow MID Server documentation and the ECC Queue documentation.

QUESTION NO: 7

Which of the following conditions can prevent a MID Server from successfully discovering a UNIX or Linux target during Service Mapping? (Choose three.)

A. SSH connectivity between the MID Server and target is blocked

B. The configured SSH credential is invalid

C. The target account lacks required command or process-access permissions

D. The ServiceNow instance cannot initiate an inbound connection to the target

E. The target does not have a web browser installed

ANSWER: A B C

Explanation:

A MID Server must be able to establish the required remote connection and authenticate with an account that has sufficient permissions to collect discovery information. Discovery can fail when SSH is blocked between the MID Server and target, when the configured credential is invalid, or when the authenticated account lacks permission to execute required commands or read required process information.

The ServiceNow instance does not need direct inbound network access to the target host because the MID Server performs the target-side communication. See the UNIX credentials documentation and the MID Server documentation.

QUESTION NO: 8

Which of the following reasons would a prospect consider purchasing ServiceNow Event Management? (Choose three.)

A. Determine impacted services from a given event/alert.

B. Provide software deployment capabilities to patch problem infrastructure.

C. Automatically generate incidents for certain classes of alerts.

D. Provide state of the art monitoring capabilities across a wide array of different types of infrastructure.

E. Consolidate events from disparate monitoring tools into a consolidated central system.

ANSWER: A C E

Explanation:

ServiceNow Event Management is designed to ingest and normalize events and alerts from existing monitoring tools, correlate related signals, and present operational teams with actionable alerts in a central location. Therefore, “Consolidate events from disparate monitoring tools into a consolidated central system.

” is a core value proposition: it reduces tool silos and helps teams focus on the most meaningful operational issues.

“Determine impacted services from a given event/alert.” is also a key reason to use Event Management, particularly when it is used with CMDB service context and Service Mapping. Service-aware event correlation helps operators understand the business services and applications affected by infrastructure conditions, supporting faster prioritization and resolution.

“Automatically generate incidents for certain classes of alerts.” is correct because Event Management can use alert-management rules and workflows to create incidents for qualifying alerts. This connects operational detection to ITSM processes without requiring manual ticket creation for every actionable condition. These capabilities support a more automated, service-centric operations model. See the ServiceNow IT Operations Management overview and the ServiceNow Event Management documentation.

QUESTION NO: 9

When using a Delimited Text Parsing Strategy, what delimiter and position will parse 2014 from the string?

2014/02/07-17:49:36

A. Delimiter of space and position 1

B. Delimiter of / and position 0

C. Delimiter of / and position of 1

D. Delimiter of 2014 and position 1

ANSWER: B

Explanation:

Delimiter of / and position 0 is correct. A Delimited Text Parsing Strategy separates a returned value into ordered segments using the delimiter specified in the pattern step. Splitting `2014/02/07-17:49:36` on the forward slash creates three segments: `2014`, `02`, and `07-17:49:36`. Service Mapping identifies these resulting segments by a zero-based position, so the first segment is at position `0`. Therefore, selecting `/` as the delimiter and `0` as the position returns `2014`.

This parsing approach is useful in Service Mapping patterns when command output contains structured values but is not already exposed as a directly usable attribute. The delimiter should be the literal character that separates the required field from the following data, and the selected position should correspond to the required field's ordinal location after the split. In this case, the year occurs before the first slash, making it the first parsed token. ServiceNow pattern authoring and parsing are part of Service Mapping's pattern-based discovery capabilities; see the Service Mapping product documentation and the Pattern Designer documentation.

QUESTION NO: 10

Using Pattern Designer, when configuring the first step in an Identification Section, which one of the following is considered a good practice?

A. Create a table for the process parameters

B. Check if connectivity variables are defined

C. Use a Parse file operation to extract necessary information from a configuration file

D. Use a Match operation on the process executable or command variable

ANSWER: D

Explanation:

Use a Match operation on the process executable or command variable is the recommended practice for the first step of an Identification section. Identification establishes whether the running process or endpoint being examined is the application represented by the pattern. A Match operation provides a clear, deterministic test against process evidence already collected by Discovery, such as the executable name, executable path, or command-line arguments. This gives the pattern a reliable anchor before it performs additional commands, parsing, and classification work.

Starting with process-based matching also helps ensure that subsequent steps run only in the appropriate application context. Command-line values are particularly useful because they can identify a product instance, configuration location, port, or other distinctive runtime argument when multiple processes may have similar executable names. The identification logic should be specific enough to recognize the intended application while remaining resilient to expected variation in installation paths and runtime values. Service Mapping patterns use identification and connection logic to discover application components and their relationships; well-defined initial identification is therefore central to accurate mapping. See the ServiceNow Service Mapping patterns documentation and the Pattern Designer documentation.

QUESTION NO: 11

Reconciliation Rules for the Application [cmdb_ci_appl] table are configured exactly the same for both ServiceNow and SCCM data sources and the following priorities are configured:

ServiceNow Priority: 100

SCCM Priority: 200

Which of the following is true?

Choose 3 answers:

A. Applications discovered by Altiris can be updated by SCCM

B. Applications discovered by SCCM can be updated by Altiris

C. Applications discovered by ServiceNow can be updated by SCCM

D. Applications discovered by Altiris can create application CIs in the CMDB

E. Applications discovered by SCCM can create application CIs in the CMDB

ANSWER: B D E

Explanation:

Reconciliation controls whether a data source is allowed to create a CI and whether it can update attribute values on a CI that is already in the CMDB. For the Application class, the configured precedence gives the ServiceNow data source priority 100 and SCCM priority 200. A smaller priority number has higher precedence, so ServiceNow is the higher-priority source where the two configured sources conflict. The stated configuration does not prevent SCCM from creating Application CIs; source precedence is principally used to protect updates to values already managed by a higher-priority source, rather than to prohibit CI creation.

Applications discovered by SCCM can be updated by Altiris because Altiris is not one of the two data sources governed by the stated ServiceNow-versus-SCCM priority comparison. Likewise, applications discovered by Altiris can create application CIs in the CMDB, and applications discovered by SCCM can create application CIs in the CMDB. These outcomes reflect the distinction between CI creation and reconciliation of updates from competing configured data sources. In a production instance, ensure that identification rules produce a reliable match before applying updates, and define reconciliation rules for every source whose field-level authority must be controlled. ServiceNow describes these mechanisms in its CMDB reconciliation documentation and Identification and Reconciliation Engine documentation.

QUESTION NO: 12

Which of the following represents the skills needed that a Service Mapping administrator or implementer should have? (Choose four.)

A. Understanding of XML, Regex, Delimited text, and JSON

B. Understanding of protocols such as HTTP, TCP, SNMP, SOAP, and REST

C. Scripting capabilities with respect to Unix and Windows commands

D. Intermediate or above Windows and Unix administration skills

E. Sufficient skills to build an enterprise web site

F. Understanding of relational database theory

ANSWER: A B C D

Explanation:

Service Mapping implementation requires a blend of infrastructure, network, and data-parsing expertise because maps are built by discovering application components, identifying the connections between them, and interpreting information returned by probes and patterns. **Understanding of XML, Regex, Delimited text, and JSON** is needed to extract and normalize discovery output from varied command results, configuration files, APIs, and other structured or semi-structured sources. **Understanding of protocols such as HTTP, TCP, SNMP, SOAP, and REST** supports identifying communication paths and configuring or troubleshooting the protocols through which Service Mapping obtains information about applications and dependencies.

Scripting capabilities with respect to Unix and Windows commands are essential for creating, validating, and troubleshooting the commands that patterns execute on target hosts. Service Mapping administrators and implementers also need **Intermediate or above Windows and Unix administration skills** to understand processes, services, ports, permissions, file locations, and operating-system behavior encountered while mapping an application. These competencies allow an implementer to build reliable patterns and resolve discovery issues across the application stack. ServiceNow describes Service Mapping as a capability that discovers application services and their components and dependencies; its implementation training also identifies the technical foundation expected for this work. See ServiceNow Service Mapping Implementation training and ServiceNow Service Mapping documentation.

QUESTION NO: 13

Which one of the following is the baseline Identification Rule (CI Identifier) used to determine inserts or updates to all servers discovered by ServiceNow Discovery or Service Mapping?

A. Application Rule

B. Server Rule

C. Hardware Rule

D. Device Rule

ANSWER: B

Explanation:

Server Rule is the baseline CI Identifier rule used for server CIs created or updated through ServiceNow Discovery and Service Mapping. The Identification and Reconciliation Engine (IRE) evaluates identification rules to decide whether incoming discovery data matches an existing CMDB CI or represents a new CI that should be inserted. For server-related CI classes, the baseline Server Rule supplies the identifier criteria that let IRE consistently recognize the same physical or virtual server across repeated discovery runs and data updates.

This rule is important because Discovery and Service Mapping do not simply write directly to the CMDB without validation. They send CI data through the identification process, which applies the appropriate rule for the CI class and uses the configured identifier entries to establish a reliable match. That behavior prevents unnecessary duplicate server records while allowing attributes from a newly discovered or mapped server to update the correct existing CI. ServiceNow documents CI identification rules and their use by IRE in its CMDB identification guidance: CI identification. Additional Discovery and CMDB context is available in the ServiceNow Discovery documentation.