

CTA Dumps

ServiceNow Certified Technical Architect (CTA)

<https://www.certleader.com/CTA-dumps.html>



NEW QUESTION 1

As an implementation progresses, which elements does a ServiceNow capability map typically indicate?
Choose 3 answers

- A. Deployed products
- B. Maturity of deployment
- C. Integration points with external systems
- D. Licensed unused products
- E. Business unit organizational structure

Answer: ABC

Explanation:

A ServiceNow capability map evolves as an implementation progresses. It typically indicates:

A: Deployed products: The map shows which ServiceNow products or modules have been deployed and are actively used within the organization.

B: Maturity of deployment: It may visually represent the maturity level of each deployed product, indicating how fully it is being utilized and integrated.

C: Integration points with external systems: The map highlights how ServiceNow integrates with other systems and applications within the organization's IT landscape.

Why not the other options?

D: Licensed unused products: While this information might be useful, it's not typically shown on a capability map, which focuses on active deployments.

E: Business unit organizational structure: This is not directly related to the ServiceNow implementation or its capabilities.

[Reference: ServiceNow implementation best practices, Capability mapping, =====]

NEW QUESTION 2

What components constitute the application layer security within ServiceNow? Choose 3 answers

- A. Multi-Factor Authentication (MFA)
- B. Platform Encryption (PE)
- C. Access Control Lists (ACLs)
- D. Full Disk Encryption (FDE)
- E. IP address access control

Answer: ACE

Explanation:

Application layer security in ServiceNow focuses on protecting data and functionality within the ServiceNow application itself. The following components contribute to this:

A: Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple forms of authentication (e.g., password, security token, biometric verification) to access the application.

C: Access Control Lists (ACLs): ACLs define which users or roles have permission to access, modify, or delete specific data and functionality within the application.

E: IP address access control: While technically a network layer control, IP address access control is often implemented and managed within the ServiceNow application. It restricts access to the instance based on IP address ranges.

Why not the other options?

B: Platform Encryption (PE): This is a broader encryption solution that protects data at rest across the platform, not specifically at the application layer.

D: Full Disk Encryption (FDE): This encrypts the entire hard drive of the server where the ServiceNow instance is hosted, providing protection at the infrastructure level, not the application layer.

[Reference: ServiceNow Security documentation, Application Security best practices, =====]

NEW QUESTION 3

What does a ServiceNow governance framework typically define? Choose 3 answers

- A. How decisions are made
- B. What decisions need to be made
- C. Who is involved in decision-making
- D. Recurring schedules for governance meetings
- E. How work gets done on the platform

Answer: ABC

NEW QUESTION 4

A system administrator, Priya, notices that certain Configuration Items (CIs) in the CMDB have not populated the required and recommended fields, impacting data integrity. Which KPI should Priya review to diagnose this issue?

- A. Compliance
- B. Correctness
- C. Completeness
- D. Relationships

Answer: C

NEW QUESTION 5

Under technical governance policies, what does environmental management in ServiceNow primarily define?

- A. Instance structure
- B. Data ownership
- C. User access policies

D. Application customization

Answer: A

Explanation:

In the context of ServiceNow technical governance, environmental management primarily focuses on defining the instance structure. This includes:
Instance Segmentation: Determining how many instances are needed (e.g., separate instances for development, test, and production) and how they relate to each other.

Instance Upgrades: Establishing policies and procedures for managing instance upgrades, including scheduling, testing, and communication.

Instance Maintenance: Defining guidelines for ongoing maintenance activities, such as patching, backups, and performance monitoring.

Why not the other options?

B: Data ownership: Data ownership is typically addressed within data governance policies, not specifically environmental management.

C: User access policies: User access policies are part of security governance and are handled through roles, permissions, and access control lists.

D: Application customization: Application customization is governed by development and configuration standards, not directly by environmental management.

[Reference: ServiceNow platform documentation, ITIL 4 framework, =====]

NEW QUESTION 6

When advising on release and instance management, what should be considered as key governance factors?

Choose 3 answers

A. Release performance and instance usage analytics

B. Operating model and development approach

C. Platform scope and deployed applications

D. Day-to-day instance performance metrics

E. Number and purpose of instance environments

Answer: BCE

NEW QUESTION 7

What are key considerations for data integrations in ServiceNow? Choose 3 answers

A. Duplicating data across all systems

B. Accessing and using only authorized data

C. Fetching only clean and accurate data

D. Maximizing data transfer volume

E. Maintaining a single source of truth

Answer: BCE

NEW QUESTION 8

What should be included in the go-live planning to handle and manage potential risks?

A. A list of key performance metrics to track the performance.

B. A back-out plan and mitigation plan for unforeseen circumstances.

C. A detailed communication plan for all stakeholders.

D. A schedule for user training and support sessions.

Answer: B

NEW QUESTION 9

Which data types are considered part of Master/Core Data in ServiceNow?

Choose 3 answers

A. Approval Policies

B. Transaction logs

C. CMDB data

D. Service model data

E. User information

Answer: ACE

Explanation:

Master/Core data in ServiceNow refers to the foundational data that is essential for the platform's operation and various applications. This includes:

A: Approval Policies: These define the rules and workflows for approvals within the platform, impacting various processes.

C: CMDB data: The Configuration Management Database (CMDB) contains critical information about IT assets, services, and their relationships.

E: User information: Data about users, their roles, and their permissions is crucial for access control and security.

Why not the other options?

B: Transaction logs: These are operational data that record system activities, not core master data.

D: Service model data: While important, service model data is typically built upon the foundation of master data like the CMDB and user information.

[Reference: ServiceNow data management best practices, =====]

NEW QUESTION 10

What are common group types used in ServiceNow for managing foundational data? Choose 3 answers

A. Assignment groups

B. Workflow groups

C. Security groups

D. Financial groups

E. Process groups

Answer: ABC

NEW QUESTION 10

What is the main focus in the Foundation stage of implementing the CSDM framework?

- A. Identifying and populating network infrastructure CIs
- B. Preparing accurate business information for reporting
- C. Setting up relationships between technology and business
- D. Working on CMDB tables associated with ITSM

Answer: C

Explanation:

The Foundation stage of the CSDM framework focuses primarily on establishing the core structure of your CMDB. This involves:

Defining the scope:Determine which services and applications will be managed within the CMDB.

Building the foundation data model:Implement the core CSDM classes and their relationships. This includes key classes like Application Service, Business Application, and Technical Service Offering.

Populating foundational data:Start populating the CMDB with basic information about your core services, applications, and the technologies that support them.

Why not the other options?

A:While network infrastructure CIs are important, they are not the primary focus in the Foundation stage. The focus is on the core service and application model.

B:Accurate business information is crucial for reporting, but the Foundation stage prioritizes establishing the structural relationships within the CMDB.

D:Working with ITSM tables is part of the broader CMDB implementation, but the Foundation stage focuses on the core CSDM classes, which extend beyond ITSM.

[Reference:ServiceNow CSDM documentation, =====]

NEW QUESTION 15

Why is IP address access control considered part of the network layer despite being implemented in the application layer?

- A. It performs data tokenization and substitution for security.
- B. It uses encryption to protect data at rest in the ServiceNow instance.
- C. It restricts access to the instance based on IP address ranges.
- D. It manages user authentication to the ServiceNow platform.

Answer: C

NEW QUESTION 18

What are the recommended error handling strategies for ServiceNow integrations? Choose 3 answers

- A. Ignore minor errors to reduce system load
- B. Establish a process to review and monitor errors
- C. Classify errors into specific categories
- D. Create email notifications for all integration errors
- E. Log all errors to a centralized location

Answer: BCE

NEW QUESTION 21

What is the primary purpose of security threat modeling?

- A. To identify potential threats and develop mitigations.
- B. To manage the encryption key management process.
- C. To backup, restore and recover critical customer data.
- D. To configure trusted IP address ranges in the system.

Answer: A

NEW QUESTION 26

In Identity Provider (IdP) initiated SSO, what is the primary protocol used for communication between the IdP and the enterprise application?

- A. JSON Web Token (JWT) authentication
- B. OAuth 2.0 authorization framework
- C. OpenID Connect (OIDC) protocol
- D. Security Assertion Markup Language (SAML)

Answer: D

NEW QUESTION 29

Starting with the Washington DC release, what will replace Database Encryption for data at rest in ServiceNow?

- A. Column Level Encryption (CLE)
- B. Cloud Encryption
- C. Full Disk Encryption (FDE)
- D. IP Address Access control (IPAC)

Answer:

B

NEW QUESTION 30

What is the primary purpose of the Test Management 2.0 application in ServiceNow?

- A. To streamline manual testing processes
- B. To generate test cases automatically
- C. To automate software testing processes
- D. To replace human testers with AI

Answer: A

NEW QUESTION 31

When should security be set up in the ServiceNow application build process?

- A. Only when issues are encountered during operations
- B. After configuring all the application workspaces
- C. After configuring all required integrations
- D. Before configuring interfaces or business logic

Answer: D

NEW QUESTION 36

What type of testing is characterized by an unplanned approach where the tester's understanding and insight are the most important factors?

- A. Usability testing
- B. Performance testing
- C. Ad hoc testing
- D. Load testing

Answer: C

NEW QUESTION 38

What type of testing requires human observation to measure how user-friendly, efficient, or convenient the software or product is for end-users?

- A. Smoke testing
- B. Usability testing
- C. Integration testing
- D. System testing

Answer: B

NEW QUESTION 41

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CTA Exam with Our Prep Materials Via below:

<https://www.certleader.com/CTA-dumps.html>