500-444 Q&As

Cisco Contact Center Enterprise Implementation and Troubleshooting

Pass Cisco 500-444 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/500-444.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which mode can be used to display data flow in the Script?

A. Edit Mode

B. Monitor Mode

C. Quick Edit Mode

D. Browse Mode

Correct Answer: B

Monitor Mode is a feature of the Packaged CCE Script Editor that allows you to view the flow of data through the script. This can be used to troubleshoot any issues with the script and ensure that it is functioning properly. Edit Mode is used to edit the Script, Quick Edit Mode is used to quickly edit basic script elements, and Browse Mode is used to view the data elements available in the Script.

QUESTION 2

Which two claim rules will be added to specify the claims sent from ADFS to Cisco Identity Service as part of a successful SAML assertion in PCCE? (Choose two.)

A. sAMAccountName -Logon names maintained for backward compatibility

B. user_principal -For Identifying the authentication realm of the user in the assertion sent to Cisco Identity Service.

C. E-Mail Address -For the Outgoing claim type

D. Unspecified -For the Incoming name ID format

E. uid -For Identifying the authenticated user in the claim sent to the applications

Correct Answer: AE

When configuring SAML authentication for PCCE (Cisco Packaged Contact Center Enterprise) with ADFS (Active Directory Federation Services), you will need to specify certain claim rules that determine which attributes of the user\\'s AD

account will be sent in the SAML assertion to Cisco Identity Service. sAMAccountName is a common attribute that contains the logon name for the user, used for backwards compatibility with older systems that may not support newer

authentication methods.

uid is an attribute that can be used to uniquely identify the user in the claims sent to the applications. This attribute is used in Cisco Identity Service to match the user to their corresponding PCCE account.

QUESTION 3

Which three statements describe fails in the high availability of Cisco Unified Intelligent Contact Management central

controller? (Choose three.)

A. If ICM Logger side A fails, router side B cannot send historical info to ICM Logger side A and is limited to ICM Logger side B.

B. If the private LAN fails, the Peripheral Gateways are used to help determine the active call router side of the duplex pair.

C. If ICM Logger side A fails, the impact of call processing is limited to ICM call router side

D. If one ICM call router of a duplex pair of Cisco Unified ICM call routers fails, the surviving ICM call router recognizes the failure when it receives no response to heartbeats over the private LAN.

E. There is no impact on call processing during a Cisco Unified ICM Logger failure.

F. During Cisco Unified ICM call router failover processing, calls in progress in Cisco Unified Customer Voice Portal are disconnected, but all new calls are processed successfully.

Correct Answer: ADF

A: When ICM Logger side A fails, ICM call router side B can\\'t send historical information to ICM Logger side A and is limited to ICM Logger side B. This is because ICM loggers act as a buffer between ICM call routers and the historical data

store, and if one side fails, the other side can\\'t send historical data to it.

(Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_10_5/installation/guide/icm_install/icm_high.html)

D: If one ICM call router of a duplex pair of Cisco Unified ICM call routers fails, the surviving ICM call router recognizes the failure when it receives no response to heartbeats over the private LAN. This is because ICM call routers

communicate with each other over a private LAN using heartbeats. If one ICM call router stops sending heartbeats, the other ICM call router knows that it has failed and takes over the processing of calls.

(Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_10_5/installation/guide/icm_install/icm_high.html)

F: During Cisco Unified ICM call router failover processing, calls in progress in Cisco Unified Customer Voice Portal are disconnected, but all new calls are processed successfully. This is because when a Cisco Unified ICM call router fails,

the surviving ICM call router takes over the processing of calls. This can cause calls in progress in Cisco Unified CVP to be disconnected, but new calls will be processed successfully.

(Reference:https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_10_5/installation/guide/icm_install/icm_high.html)

References:

[1] https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/crs/express_8_5/design/guide/icm85des/icm85des_chap_01.html

[2] https://www.cisco.com/c/ en/us/support/docs/unified-communications/unified-contact-center-enterprise

QUESTION 4

Where can the readiness for the CCE deployment be verified?

A. CCE Web Admin -inventory

B. CCE Web Admin -> Machines -inventory

C. CCE Web Admin -> Deployment Settings -Inventory

D. CCE Web Admin -> Infrastructure -Inventory

Correct Answer: C

The readiness for the CCE deployment can be verified by navigating to the CCE Web Admin -> Deployment Settings -Inventory page. This page contains information on the infrastructure that is required for the CCE deployment, including the number of servers, the region, and the type of deployment.

QUESTION 5

Which service is used to provide authorization between the Identity Provider (IdP) and application?

A. SAML

B. OAuthv2

C. Active Directory Federation Services (ADFS)

D. Identity Service (IdS)

Correct Answer: B

The service used to provide authorization between the Identity Provider (IdP) and application is OAuthv2. OAuthv2 is an open standard for authorization that enables applications to securely access resources from an IdP without having to manage the user credentials. OAuthv2 provides the IdP with the ability to grant limited access to its resources without having to share the user\\'s credentials. Active Directory Federation Services (ADFS) and SAML are also commonly used for authorization, but OAuthv2 is the most widely used protocol for providing authorization between an IdP and an application.