2024 Best 500-444 Exam Preparation Material with New Dumps Questions [Q17-Q34

2024 Best 500-444 Exam Preparation Material with New Dumps Questions Free 500-444 Exam Files Verified & Correct Answers Downloaded Instantly

Cisco 500-444 certification exam is a highly specialized exam that focuses on the implementation and troubleshooting of Cisco's Contact Center Enterprise solution. Cisco Contact Center Enterprise Implementation and Troubleshooting certification is designed for IT professionals who specialize in contact center technologies and are looking to enhance their skills and knowledge in this area.

The Cisco 500-444 exam is intended for network engineers, administrators, and support staff who want to enhance their technical skills and knowledge of Cisco Contact Center Enterprise. The Cisco 500-444 exam is a challenging one and requires rigorous preparation to pass. Candidates must demonstrate their ability to configure and troubleshoot the system's routing protocols, media servers, and advanced scripting.

QUESTION 17

Where can the SAML Certificate Expiry details be checked in PCCE Web Administration Manager (S.RO.G)?
* Features -> Context Service
* Infrastructure Settings -> License Management
* Features -> Single Sign-On
* Infrastructure Settings -> Device Configurations -> Identity Services

The SAML Certificate Expiry details can be checked in the PCCE Web Administration Manager (S.RO.G) under the Features -> Single Sign-On menu. This menu can be used to view the certificate details, such as the issuer, validity period, and expiry date. This can be useful for ensuring that the certificate does not expire before its intended use. Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/pccx/pccx_11_0_1/pccx_b_pccx-web-admin-manager-guide-110/pccx_b_pccx-web-admin-manager-guide_chapter_011.html

QUESTION 18

Which service must be restarted after modifying the Java Keystore on the CVP servers?
* Cisco CVP Call server
* Cisco CVP VXML server
* Client license service
* Cisco CVP WebServicesManager

QUESTION 19

What is important to remember about VMs when deploying Direct Attached Storage (DAS) only systems?
* Failure of a physical server brings down only specific VMs allocated to that specific storage and installed on that VMware vSphere Host.
* Failure of a physical server doesn’t bring down all the VMs that are installed on that VMware vSphere Host.
* Failure of a VM brings down all the components that are installed on the VM.
* Failure of a VM doesn’t bring down all the components that are installed on the VM.

QUESTION 20

What are the Active and Configured agent counts for the 2K deployment model?
* 2K/4K
* 2K / 8K
* 2K/10K
* 2K/12K

Explanation

The 2K deployment model for Cisco Contact Center Enterprise (CCE) is a prepackaged solution that offers a simplified and scalable architecture for medium-sized contact centers. The 2K deployment model supports up to 2,000 active agents and up to 8,000 configured agents. An active agent is an agent who is logged in and ready to take calls. A configured agent is an agent who has a profile in the system, regardless of their login status. The 2K deployment model also supports up to 4,000 IVR ports, up to 120,000 BHCA, and up to 12,000 concurrent calls1.

References:

1: Cisco Packaged Contact Center Enterprise Solution Reference Network Design (SRND), page 2-3

QUESTION 21

Which three modes can implement single sign-on in PCCE? (Choose three.)
* Non-SSO
* SSO
* ldS
* ldP
* SAML
* Hybrid

Explanation

* SSO – Enable all agents and supervisors in the deployment for SSO.

* Hybrid – Enable agents and supervisors selectively in the deployment for SSO. …

* Non-SSO – Continue to use existing Active Directory-based and local authentication, without SSO.

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/pcce/pcce_12_6_1/maintena

QUESTION 22

Which sync is triggered when an administrator performs any create, update, or delete operation on a specific configuration item?
* Automated differential
* Push
* Manual differential
* OnDemand

QUESTION 23

What are two specifications for UC on UCS Tested Reference Configuration (TRC)? (Choose two.)
* defined as Configuration Based
* VMware vSphere is optional
* VMware vCenter is required
* defined as Rule Based
* VMware vSphere is required

The UCS Tested Reference Configuration (TRC) is a validated server configuration for running Unified Computing System (UCS) in a data center environment. It is defined as either Configuration Based or Rule Based, depending on the specific use case. Configuration Based defines the server configuration based on specific performance characteristics, while Rule Based defines the server configuration based on specific usage. VMware vCenter is required for either Configuration Based or Rule Based, while VMware vSphere is optional.

QUESTION 24

Where should a trust relationship be established by downloading and exchanging a metadata file when configuring the Cisco IdS using PCCE Web Administration Manager (S.P.O.G)?
* IdS to IdP
* IdS to IdP and IdP to IdS
* IdP to IdS
* IdS to IdP and IdP to Active Directory (AD)

QUESTION 25

What are two considerations for PCCE 2K installation? (Choose two.)
* add Router Logger after installing software
* add PGs via PG setup after installing the software
* run Domain Manager tool, add root, facility, and instance
* run Websetup after installing the software
* needs ICM/CCE software installed on all ICM/CCE servers

Explanation

According to the Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide, Release 12.0 (1), there are two considerations for PCCE 2K installation:

You need to add PGs via PG setup after installing the software. This is because the PG setup tool allows you to configure the PGs for different types of peripherals, such as CUCM, CVP, and Finesse. You can also configure the network interface cards, the PG redundancy, and the PG security settings using the PG setup tool1.

You need to run Websetup after installing the software. This is because the Websetup tool allows you to configure the PCCE components, such as the Router, Logger, AW-HDS-DDS, and CVP. You can also configure the call routing scripts, the dialed number plan, the agent teams, and the skill groups using the Websetup tool2.

You do not need to add Router Logger after installing the software, because the Router Logger is automatically installed and configured during the PCCE installation process3. You do not need to run Domain Manager tool, add root, facility, and instance, because the Domain Manager tool is only used for UCCE installations, not PCCE installations4. You do not need to install ICM/CCE software on all ICM/CCE servers, because the PCCE installation process automatically installs the ICM/CCE software on the required servers3.

References :=

Some possible references are:

1: Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide, Release 12.0 (1), Chapter:

Create Virtual Machines for Components, Section: Create VM for Unified CCE PG, 4 2: Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide, Release 12.0 (1), Chapter: Configure PCCE Components, Section: Run Websetup, 1 3: Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide, Release 12.0 (1), Chapter: Install PCCE Software, Section: Install PCCE Software on Unified CCE Rogger, 3 4: Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, Release 12.0 (1), Chapter: Install Unified CCE Software, Section: Run Domain Manager, 5

5:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterpri

QUESTION 26

What are two ways to deploy security certificates in CCE? (Choose two.)
* Certificate Authority (CA)
* 3rd party signed
* Security Authority (SA)
* Digitally signed
* Self-signed

Explanation

Security certificates are used to ensure that browser communication is secure by authenticating clients and servers on the web. There are two ways to deploy security certificates in CCE: Certificate Authority (CA) signed certificates and self-signed certificates1.

CA signed certificates are certificates that are issued by a trusted third-party entity, such as VeriSign or Thawte, that validates the identity of the certificate owner. CA signed certificates are more secure and reliable than self-signed certificates, but they also require more time and money to obtain and maintain2.

Self-signed certificates are certificates that are generated and signed by the certificate owner, without involving any third-party entity. Self-signed certificates are easier and cheaper to create and deploy, but they are less secure and trustworthy than CA signed certificates, as they can be easily forged or tampered with2.

CCE supports both CA signed certificates and self-signed certificates for securing the communication between different components, such as AW, CVP, Finesse, ECE, etc. However, some components may require additional steps or configurations to use CA signed certificates, such as importing the CA certificate into the AW machines, changing the Java truststore password, or binding the CA signed certificate in the Diagnostic Portico123.

The other options are not valid ways to deploy security certificates in CCE:

Security Authority (SA) is not a term related to security certificates, but rather a role that is assigned to a user or a group in CCE to grant them access to certain security features, such as encryption, auditing, or IPsec1.

3rd party signed certificates are not a distinct category of security certificates, but rather a synonym for CA signed certificates, as they both involve a third-party entity that signs the certificates2.

Digitally signed certificates are not a specific type of security certificates, but rather a general characteristic of all security certificates, as they all use digital signatures to verify the authenticity and integrity of the certificate data2.

References:

1: Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1) – Certificate Management for Secured Connections 2: Packaged CCE Migration Guide, Release 12.0 – Manage Security Certificates 4:

Computer forensics certifications – Infosec Resources 3: Implement CA Signed Certificates in a CCE Solution

– Cisco

QUESTION 27

Which two validations will be completed for the PCCE production deployment model on an ESXi server?

(Choose two.)
* Linux verification for containers.
* The hypervisor provides enough power.
* The lab is deployed properly.
* Ensure that the correct servers are on the correct sides.
* Correct RAM and CPU are being deployed.

QUESTION 28

Which two certificates do the Cisco Finesse primary and secondary servers accept when HTTPS protocol is used to access the administration console or agent desktop in Cisco Finesse? (Choose two.)
* Domain validation certificate
* Digital certificate
* Self-signed certificate
* Certificate authority certificate
* Root certificate

Explanation

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/finesse/finesse_1151/Admin Cisco Finesse primary and secondary servers accept both self-signed certificates and certificate authority certificates when HTTPS protocol is used to access the administration console or agent desktop in Cisco Finesse. A self-signed certificate is a certificate that is generated by the server itself and is not verified by a trusted third-party. A certificate authority certificate is a certificate that is issued by a trusted third-party vendor and is used to establish a secure connection between the server and the client. Cisco Finesse supports both types of certificates for HTTPS connections, but recommends using certificate authority certificates for better security and compatibility. Domain validation certificates, digital certificates, and root certificates are not valid options for this question. A domain validation certificate is a type of certificate authority certificate that only verifies the ownership of the domain name, but not the identity of the organization. A digital certificate is a general term that refers to any certificate that uses public key cryptography to authenticate the identity of the sender and the integrity of the data. A root certificate is a certificate that is used to validate other certificates in a chain of trust, but it is not directly used for HTTPS connections. References: Cisco Finesse Administration Guide, Release 12.6 (2) – Getting Started [Cisco Finesse] – Cisco1, Solved: Finesse Certificate Issue – Cisco Community2, Cisco Finesse Administration Guide Release 11.6(1)3, Cisco Finesse Administration Guide, Release 12.0 (1)4, Cisco Finesse Administration Guide, Release 12.6 (1)5

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/finesse/finesse_1151/Admin

QUESTION 29

What is needed to execute a particular script that is configured using script explore for a specific time?
* Dialed Number mapped to a CallType and in turn mapped to a scheduled script
* Dialed Number mapped to a CallType
* Dialed Number with scheduled script
* Agent mapped to Dialed Number and Dialed Number in turn mapped with scheduled script

Explanation

To execute a particular script that is configured using script explorer for a specific time, you need to have a dialed number mapped to a call type and in turn mapped to a scheduled script. This is because the dialed number identifies the call and associates it with a call type, which determines the routing script to be executed.

The routing script can be scheduled for different versions or times using the script explorer tool. The script explorer allows you to view, modify, and schedule scripts for different call types and dialed numbers12. References: Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.5 (1) and 12.5 (2)1, Cisco Packaged Contact Center Enterprise Features Guide, Release

12.0 (1)2.

QUESTION 30

Which powerful tool supports Element Grouping, Time of Day routing, and Call Admission Control?

* VGW
* CUSP
* CUBE
* CUCM

Explanation

CUBE is a Cisco IOS software feature that provides voice and video connectivity from IP phones to the PSTN or other IP networks. CUBE supports several advanced call control and mobility services, such as:

Element Grouping: This feature allows you to group multiple CUBE elements into a single logical entity and apply common configuration and dial plan across them. This simplifies the management and scalability of CUBE deployments.

Time of Day Routing: This feature allows you to route calls based on the time of day, day of week, or date. You can define time periods and time schedules and associate them with dial peers or voice translation rules. This enables you to implement different call routing policies for different time slots, such as business hours, after hours, holidays, etc.

Call Admission Control: This feature allows you to limit the number of concurrent calls on a CUBE element or a CUBE group based on the available bandwidth or the configured maximum number of calls. This prevents oversubscription of network resources and ensures the quality of service for voice and video calls.

References:

CUBE Configuration Guide

CUBE Element Grouping Configuration Guide

Time of Day Routing Configuration Guide

Call Admission Control Configuration Guide

QUESTION 31

What is needed to execute a particular script that is configured using script explore for a specific time?

* Dialed Number mapped to a CallType and in turn mapped to a scheduled script
* Dialed Number mapped to a CallType
* Dialed Number with scheduled script
* Agent mapped to Dialed Number and Dialed Number in turn mapped with scheduled script

In order to execute a particular script that is configured using script explorer for a specific time, it is necessary to map the dialed number to a call type, and in turn, map the call type to a scheduled script.

The dialed number is the number that a customer dials to reach the contact center. When the call is received, the call type is determined based on the dialed number. The call type is a category that describes the type of call, such as sales, support, or billing.

Once the call type is determined, the appropriate script can be executed. Script explorer allows you to configure different scripts for different call types and schedule them to be executed at specific times.

To ensure the correct script is executed at the right time, the dialed number must be mapped to the appropriate call type, and the call type must be mapped to the scheduled script.

Cisco ICM Script Explorer

(https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-command-reference-guides-list.html) Cisco ICM Call Type
(https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_10_5_1/configuration/guide/ICM_BK_I3C936F3_00_configuration-guide-10-5-1/ICM_BK_I3C936F3_00_configuration-guide-10-5-1_chapter_01.html)

QUESTION 32

How are microapps defined and configured using PCCE Web Administration Manager (S.P.O.G)?
* Call Settings-> IVR Settings->Network VRU Scripts
* Route Settings -> Media Routing Domain
* Route Settings -> Sip Server Groups
* Desktop Settings -> Resources -> Call Variables Layout

QUESTION 33

What are two upgrades for Common Ground? (Choose two.)
* updates IP address as appropriate
* in-place upgrades exist on VMs
* updates Hostname as appropriate
* includes migration of windows registry
* includes database migration

Explanation

Two upgrades for Common Ground are includes migration of windows registry and includes database migration. Common Ground is a type of upgrade that allows you to upgrade your Cisco Unified Contact Center Enterprise (CCE) components from one release to another without changing the hardware or operating system1. Common Ground upgrade is supported for virtualized deployments on VMware ESXi hosts1. Common Ground upgrade involves the following steps1:

Back up the existing configuration and data using the Disaster Recovery System (DRS).

Run the User Migration Tool to export the user accounts from the source domain to a file.

Run the Enhanced Database Migration Tool (EDMT) to migrate the Historical Data Server (HDS), Logger, and Business Analytics (BA) databases from the source servers to the destination servers.

Run the Regutil Tool to export the Cisco Systems, Inc. registry from the source servers to a file.

Run the Unified CCE Installer on the destination servers to install the new release of Unified CCE software.

Import the user accounts from the file using the User Migration Tool.

Import the Cisco Systems, Inc. registry from the file using the Regutil Tool.

Restore the configuration and data from the DRS backup.

The Common Ground upgrade includes migration of windows registry because the Regutil Tool is used to export and import the Cisco Systems, Inc. registry from the source servers to the destination servers. The registry contains important information about the Unified CCE configuration, such as the instance name, the peripheral ID, the system ID, and the license key2. The registry migration ensures that the destination servers have the same settings as the source servers after the upgrade2.

The Common Ground upgrade includes database migration because the EDMT is used to migrate the HDS, Logger, and BA databases from the source servers to the destination servers. The databases contain historical and real-time data about the Unified CCE system, such as the call records, the agent statistics, the skill group statistics, and the reporting data3. The database migration ensures that the destination servers have the same data as the source servers after the upgrade3.

The Common Ground upgrade does not update IP address as appropriate because the IP addresses of the source and destination servers are not changed during the upgrade. The IP addresses are configured during the initial installation of the Unified CCE software and are not modified by the upgrade process1.

The Common Ground upgrade does not update Hostname as appropriate because the hostnames of the source and destination servers are not changed during the upgrade. The hostnames are configured during the initial installation of the Unified CCE software and are not modified by the upgrade process

QUESTION 34

Which two certificates need to be uploaded to VOS servers for CA Signed certificate management? (Choose two.)
* CA Certificate:tomcat
* CA Signed Certificate from CSR Request:tomcat
* 3rd party signed Certificate
* CA Certificate:tomcat-trust
* CA Signed Certificate from CSR Request:tomcat-trust