922-101

Communication Server 1000 Linux Platform Architecture

DEMO

QUESTION NO: 1

You have installed the Linux Base onto a Commercial Off the Shelf (COTS) server that will be configured as a Member Server. You are ready to perform the Security Configuration. All LAN connections are in place and functioning normally. After connectingthrough a browser, what is your next step to perform the Security Configuration ofthis COTS Member server?

A. Enter the IP address of the Certificate Authority in the address bar of the browser.
B. Enter the IP address of the Primary Security server in the address bar of the browser.
C. Enter the FQDN of the COTS Member server in the address bar of the browser.
D. Enter the FQDN of the Primary Security server in the address bar of the browser.

Answer: C

QUESTION NO: 2

A customer is deploying a Communication Server (CS) Rls. 6.0 system. They plan to have aDell R300 COTS configured as the Primary Security Server and a CPPM configured as a Backup Security Server. Which statements regarding the roles of the Primary and Backup Security Server are true? (Choose two.)

A. You must have a Backup Security Server for the CS 1000 network.
B. The Backup Security Server is automatically promoted to Primary Security Server.
C. The Primary Security Server cannot be demoted to a member server.
D. The Backup Security Server automatically handles authentication requests when the Primary is down.

Answer: C,D

QUESTION NO: 3

A customer is deploying a Communication Server 1000 Rls. 6.0 High Availability system andwould like to know what options for Signaling Server functionality exist. Which options can the customer deploy? (Choose two.)

A. CPPMVxWorks-based Signaling Server
B. CPPM Linux-based Signaling Server
C. COTSVxWorks-based Signaling Server
D. COTS Linux-based Signaling Server

Answer: B,D

QUESTION NO: 4

A large corporation recently deployed five Communication Server (CS) 1000 Rls. 6.0 systems to support their regional call center environment. All five systems function under thesame Unified Communications Management Security Domain. During a busy workday some UCM administrators cannot login. Which UCM feature is most likely the reason administrators cannot login to UCM?

A. The UCM network reached the maximum number of concurrent users.
B. The UCM network reached the maximum number of Virtual Terminal sessions.
C. The UCM network reached the maximum number of Secure Socket Shell (SSH) sessions.
D. The UCM network reached the maximum numbers of administrators which can simultaneouslylogin.

Answer: D

QUESTION NO: 5

You have just installed and configured a Primary Security Server with the Element Manager and Subscriber Manager Applications deployed. The Communication Server (CS) 1000E Rls. 6.0 Call Server is part of this server security domain. All connections are up andrunning. You click the new CS 1000 Rls. 6.0 system link on the Elements window, and the Web browser returns with the following message:
"Destination IP address cannot be reached."
Which situation can be the problem? (Choose two.)

A. The browser window has not been refreshed.
B. The Element Manager is unable to reach the MC32S via the ELAN.
C. The wrong Call Server IP address was entered during the application deployment.
D. The Public Key Certificates for Web SSL were not added in the Call Server.

Answer: C

QUESTION NO: 6

While visiting a site where a fully functional Communication Server (CS) 1000 Rls. 6.0 system is supporting a call center, you were instructed to visually inspect the cabling of the servers. However, upon opening the door to a server rack, you accidentally disconnected thepower from the Primary Security server and there is not a backup security server. Which scenario most likely describes the behavior of the member servers when both the Primary and Security Servers are out of service?

A. Member servers flush their trusted CA list and restrictsusers from logging in.
B. Member servers exchange backup SSL certificates in their trusted CA list.
C. Member servers assume the Alternate Certificate Authority functionality until the Primary Security Server returns to service.
D. Member servers continue to trust each other because of valid certificates in their trusted CA list.

Answer: D

QUESTION NO: 7

A customer that recently deployed a Communication Server 1000 Rls. 6.0 system with Unified Communications Management would like to take advantage of the UCM log forwardingcapability. Which statement regarding UCM Logging Services is true?

A. Only Application logs can be forwarded to aSyslog server.
B. Only OAM and Security logs can be forwarded to aSyslog server.
C. Application, OAM and Security logs can all be forwarded to aSyslog server.
D. Only Security logs can be forwarded to aSyslog server.

Answer: B

QUESTION NO: 8

A customer is installing a Communication Server (CS) 1000E Rls. 6.0 System with Unified Communications Management. The Linux base software has been installed and the CPPM Co-Resident Call Server and Signaling server has been configured as a member server within an existing CS 1000 Rls 6.0 security domain. Which statement describes the process theadministrator must use to deploy applications to the CPPM Co-Resident?

A. Log in to the UCM of the Primary Security Server and access the Base Manager to deploy.
B. Log in to the Base Manager and access local Deployment Manager to deploy.
C. Log in to the Base Manager and access central Deployment Manager to deploy.
D. Log in to the UCM of the Primary Security Server and access central Deployment Manager to deploy.

Answer: D