PassQueen
a.k.a dumpsqueen.com

Implementing Cisco Connected Physical Security 1

Cisco 648-238

Version Demo

Total Demo Questions: 18

Total Premium Questions: 184

Buy Premium PDF

https://passqueen.com

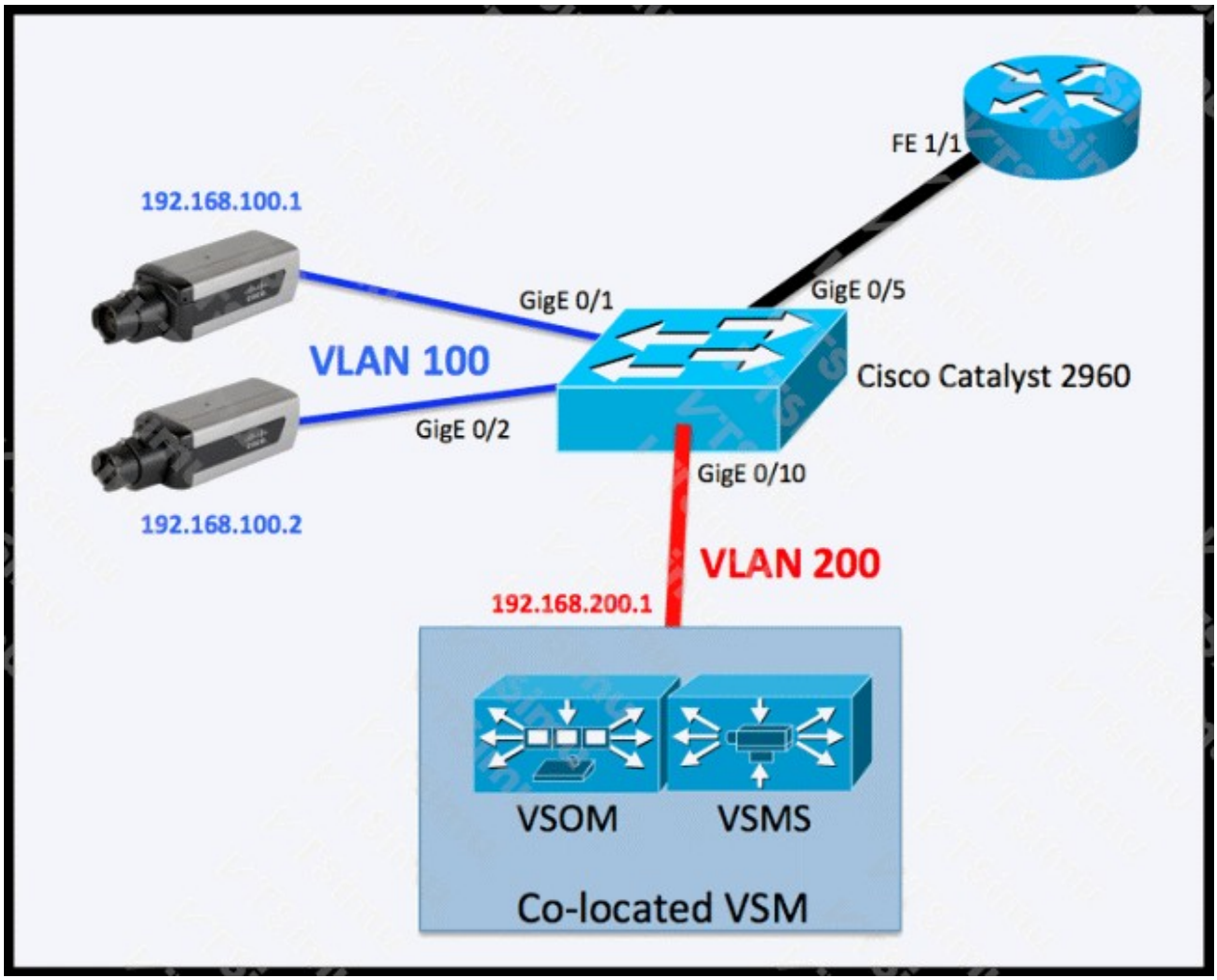
support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cisco Physical Access Control	3
Topic 2, Cisco Video Surveillance	180
Topic 3, Mix Questions	1
Total	184

QUESTION NO: 1

Refer to the exhibit.



Cameras and a Cisco VSM server are connected to a Layer 2 switch.

Which three steps will allow the Cisco VSM servers to see video traffic from the two IP cameras? (Choose three.)

A. GigE 0/10 should be configured to accept traffic from all VLANs using the #switchport mode access vlan all command.

B. GigE 0/10 should be configured to dynamic mode using the #switchport mode dynamic desirable command.

C. Implement "router-on-a-stick".

D. Implement inter-VLAN routing.

E. The link between GigE 0/5 and FE 1/1 should be configured as a trunk port.

ANSWER: C D E

Explanation:

Implementing **"router-on-a-stick"**, implementing **inter-VLAN routing**, and configuring **the link between GigE 0/5 and FE 1/1 as a trunk port** provide the required Layer 3 reachability between the VSM server and cameras located in separate VLANs. A Layer 2 switch forwards traffic only within an individual VLAN; therefore, communication between the camera VLANs and the VSM server VLAN requires a routing function. Router-on-a-stick supplies that function by using router subinterfaces, with each subinterface assigned to the applicable VLAN and acting as that VLAN's default gateway. This is an implementation of inter-VLAN routing.

The switch-to-router connection must carry traffic for all participating VLANs simultaneously. Configuring the GigE 0/5-to-FE 1/1 link as an IEEE 802.1Q trunk preserves VLAN identification across that physical connection, allowing the router's VLAN-

tagged subinterfaces to receive and route camera and VSM traffic correctly. Once this connectivity is present, the VSM server can establish the IP communication needed to receive and manage camera video streams. Cisco's inter-VLAN routing guidance describes router-on-a-stick and the trunk requirement: Cisco: Inter-VLAN Routing Configuration. Cisco's VLAN configuration documentation also explains trunk operation and VLAN tagging: Cisco IOS XE VLAN Configuration Guide.

QUESTION NO: 2

When troubleshooting camera issues, which technology allows you to find the IP address of a Cisco IP camera from the Cisco switch it is connected to?

A. DHCP

B. SNMP

C. CDP

D. medianet

ANSWER: C

Explanation:

CDP is correct because Cisco Discovery Protocol is a Cisco-proprietary Layer 2 neighbor-discovery protocol that devices use to advertise identifying information to directly connected Cisco devices. A Cisco IP camera that supports and has CDP enabled sends CDP advertisements on its switch port. The connected Cisco switch records the camera as a CDP neighbor, including useful troubleshooting details such as the platform, local interface, port ID, and one or more advertised network-layer addresses. An administrator can inspect this information from the switch with commands such as `show cdp neighbors detail`, making it possible to identify the camera's IP address even when the address is not otherwise known. This is particularly useful for confirming which physical switch interface serves a camera and correlating that endpoint with its management address during incident triage. CDP operates between directly connected neighbors, so it provides endpoint-discovery data at the access-switch edge rather than requiring a separate address-management lookup. Cisco documents the protocol's neighbor-discovery function and the information available through CDP show commands in its CDP Configuration Guide. Cisco also describes CDP support and related network integration capabilities in its IP camera deployment guidance.

QUESTION NO: 3

When the CPS-MSP-2RU-K9 server is turned on, it starts beeping and continues to do so, even if the server seems to be operational.

What is causing this issue?

A. The clock battery in the server is drained and must be replaced.

B. One of the fans in the power supply has failed.

C. The incoming power voltage into the power supply is too low or too high.

D. One of the hard disk drives has failed and must be replaced.

ANSWER: D

Explanation:

One of the hard disk drives has failed and must be replaced. The CPS-MSP-2RU-K9 can remain apparently operational after an individual disk failure because its storage is designed to use RAID redundancy. In a redundant RAID configuration, the operating system and physical-security applications can continue running while the RAID controller uses the remaining healthy disks to provide access to data. The server is nevertheless in a degraded and unprotected state: a further disk failure can cause loss of the RAID volume and interruption of recording or other security services.

The persistent audible alarm at startup is a hardware-health notification intended to bring this degraded storage condition to the administrator's attention. The appropriate response is to identify the disk reported as failed through the server's management interface or RAID-controller utility, verify the failed-drive indicator, and replace that drive with a supported replacement according to the maintenance procedure. After the replacement disk is installed, the RAID controller rebuilds the affected array; the alarm condition clears once the controller recognizes that storage redundancy has been restored. Cisco's server documentation and support resources provide hardware-maintenance and RAID-management guidance: Cisco UCS C-Series Rack Servers support and Cisco installation and configuration guides.

QUESTION NO: 4

In VSM 6.3.2, which of the following options cannot be used to create a snapshot?

A. BMP

B. TIFF

C. PNG

D. VSD

ANSWER: D

Explanation:

VSD is the correct answer. In Cisco Video Surveillance Manager 6.3.2, a snapshot is a still-image capture taken from a camera video stream and saved in one of the supported image-file formats. Snapshot creation is intended to produce a portable image that can be viewed, shared, printed, or retained as visual evidence without requiring the video-management application. VSD is not a still-image encoding or image-file format for snapshot output, so it cannot be selected as a snapshot creation format. The snapshot capability is part of the Cisco VSM client and video-viewing workflow, where users capture a single frame from live or recorded video and export it as an image. This distinction matters operationally because snapshots are evidence artifacts that must remain accessible through standard image-viewing tools and suitable for reports or incident documentation. Cisco's VSM documentation set describes client functions, video operations, and supported product behavior for the 6.3 release family. See the Cisco Video Surveillance Manager 6.3 Release Notes and Cisco's Physical Security product documentation index.

QUESTION NO: 5

Before connecting a group of IP cameras to a PoE switch, which two items should be verified? (Choose two.)

A. The total camera power requirement does not exceed the switch PoE power budget

B. Each switch port can provide the power required by the attached camera

C. Every camera is assigned to the switch native VLAN

D. The camera video codec matches the switch operating system

E. The switch management IP address is identical to the camera IP address

ANSWER: A B

Explanation:

The total camera power requirement does not exceed the switch PoE power budget and **each switch port can provide the power required by the attached camera** are correct. A switch has a finite total PoE budget that must support all powered devices connected to it. The aggregate requirement must include cameras, illuminators, heaters, PTZ functions, and other features that may increase the power drawn by an endpoint.

It is also necessary to confirm that an individual port supports the applicable PoE standard and has sufficient power available for the particular camera. A camera that requires more power than the port can supply may fail to boot, disable optional features, or repeatedly restart. Cisco provides PoE concepts and platform guidance in its Power over Ethernet overview.

QUESTION NO: 6

After initial setup, a system administrator enters the IP address of the Cisco VSM server into the URL bar of the web browser and the Cisco VSMC login page is loaded.

Which two situations is causing the issue? (Choose two.)

A. Cisco VSOM is not the selected default login view.

B. Cisco VSOM is not running on this server.

C. Cisco VSMS is being managed by a separate Cisco VSOM server.

D. Under the Operations Manager menu in Cisco VSMC, the default home page is set to Cisco VSMC instead of Cisco VSOM.

ANSWER: B C

Explanation:

Cisco VSOM is not running on this server and Cisco VSMS is being managed by a separate Cisco VSOM server are the situations that result in the Cisco Video Surveillance Manager Client (VSMC) login page appearing when the server IP address is used. VSMC provides the System Manager interface and is used to administer the Video Surveillance Manager system, including VSOM server instances. VSOM, the Operations Manager component, supplies the operational interface for monitoring and managing cameras, recordings, and related video-surveillance functions. Therefore, a server that has no locally running VSOM instance can only present its VSMC interface. Likewise, when a VSMS deployment is assigned to and managed by a VSOM instance on another server, the local server does not host the Operations Manager login interface; administration at that address remains through VSMC. The administrator should verify the VSOM service status and identify which server hosts the VSOM instance responsible for the VSMS deployment, then access that VSOM server for operations. Cisco's VSM documentation describes the distinct System Manager and Operations Manager roles and their deployment relationships. See the Cisco Video Surveillance Manager User Guide and the Cisco Video Surveillance Manager installation and configuration guides.

QUESTION NO: 7

As the system administrator, you have been asked to immediately delete cameras (and recordings) in Cisco VSM that are located at a building that was recently vacated by your company. Two days later, the night shift operator reports that although live video is unavailable, archived video from the vacated building is viewable.

What must you do to purge the video archives?

A. Wait until the retain recording timers expire, and then the archived video is purged automatically.

B. Select the camera(s) in Cisco VSOM - Cameras and choose Full Delete.

C. Move the soft-deleted cameras to a restricted location that is accessible only to system admins.

D. Blacklist the camera(s) so that they no longer show up in Cisco VSM.

ANSWER: B

Explanation:

Select the camera(s) in Cisco VSOM - Cameras and choose Full Delete. is correct because removing a camera through the normal deletion workflow can leave it soft-deleted. Soft deletion removes the camera from active operation, so live video is no longer available, but retains the associated archive data. This behavior allows an administrator to recover the camera configuration or preserve evidence when deletion was accidental or when video must remain available for operational or legal retention purposes.

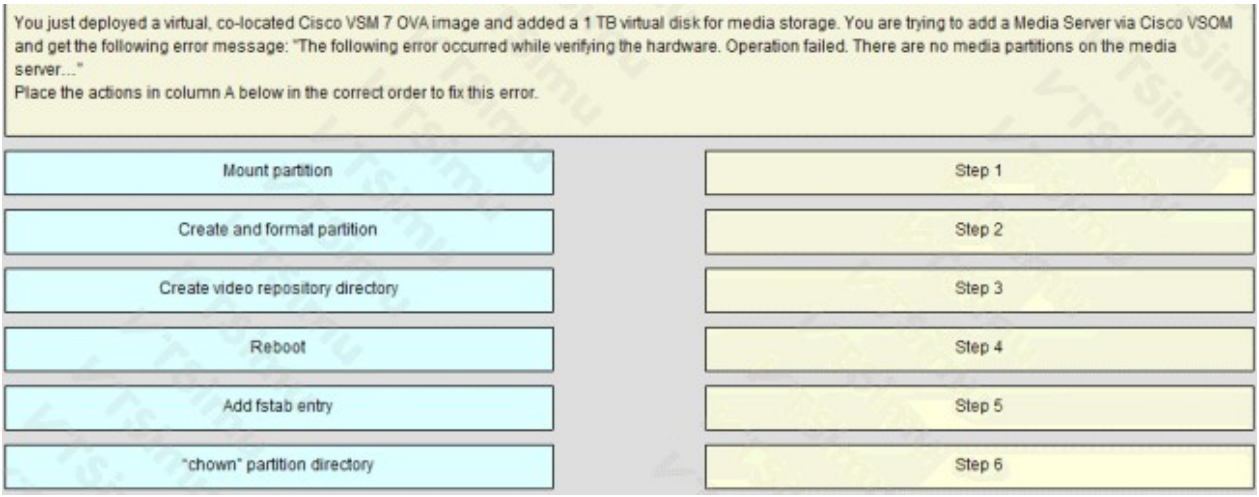
When the requirement is to remove both the camera and its retained recordings immediately, the administrator must perform a Full Delete from the Cameras area of Cisco Video Surveillance Operations Manager. Full Delete permanently removes the camera record and initiates deletion of its associated archived video, rather than waiting for the configured recording-

retention period to age the content out. This is the appropriate administrative action when the site has been vacated and the recordings must be purged instead of merely being unavailable for new live viewing.

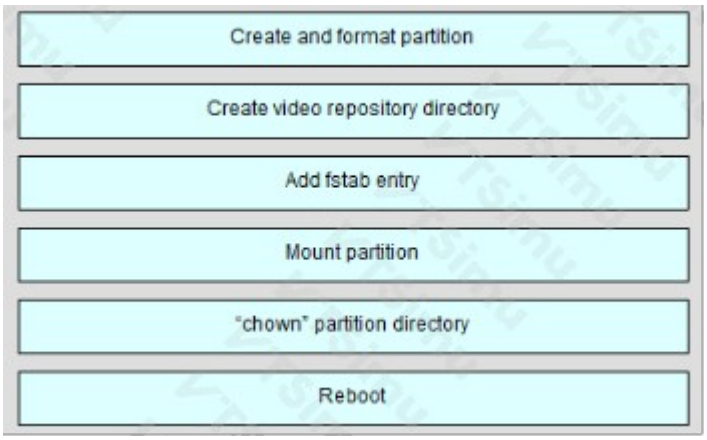
For Cisco physical-security product documentation and available VSM releases, see the Cisco Video Surveillance Manager User Guide list and the Cisco Video Surveillance Manager support page.

QUESTION NO: 8 - (DRAG DROP)

Select & Place:



ANSWER:



Create and format - Step 1, Create Video - Step 2, Add fstab - Step 3, Mount partition - Step 4, chown - Step 5, Reboot - Step 6

Explanation:

A newly attached virtual disk is not usable by Cisco Video Surveillance Manager as media storage until the operating system has a formatted filesystem, a defined mount location, and a persistent mount configuration. The correct workflow starts by creating and formatting the partition. This gives the added virtual disk a usable filesystem on which recordings and repository data can be stored.

Next, create the video repository directory. That directory is the local mount point that represents the storage location to the Media Server. Add the filesystem definition to `/etc/fstab` after the mount-point directory exists. The fstab entry makes the disk-to-directory relationship persistent, so the media partition is automatically restored after a system restart rather than disappearing from the configured repository path.

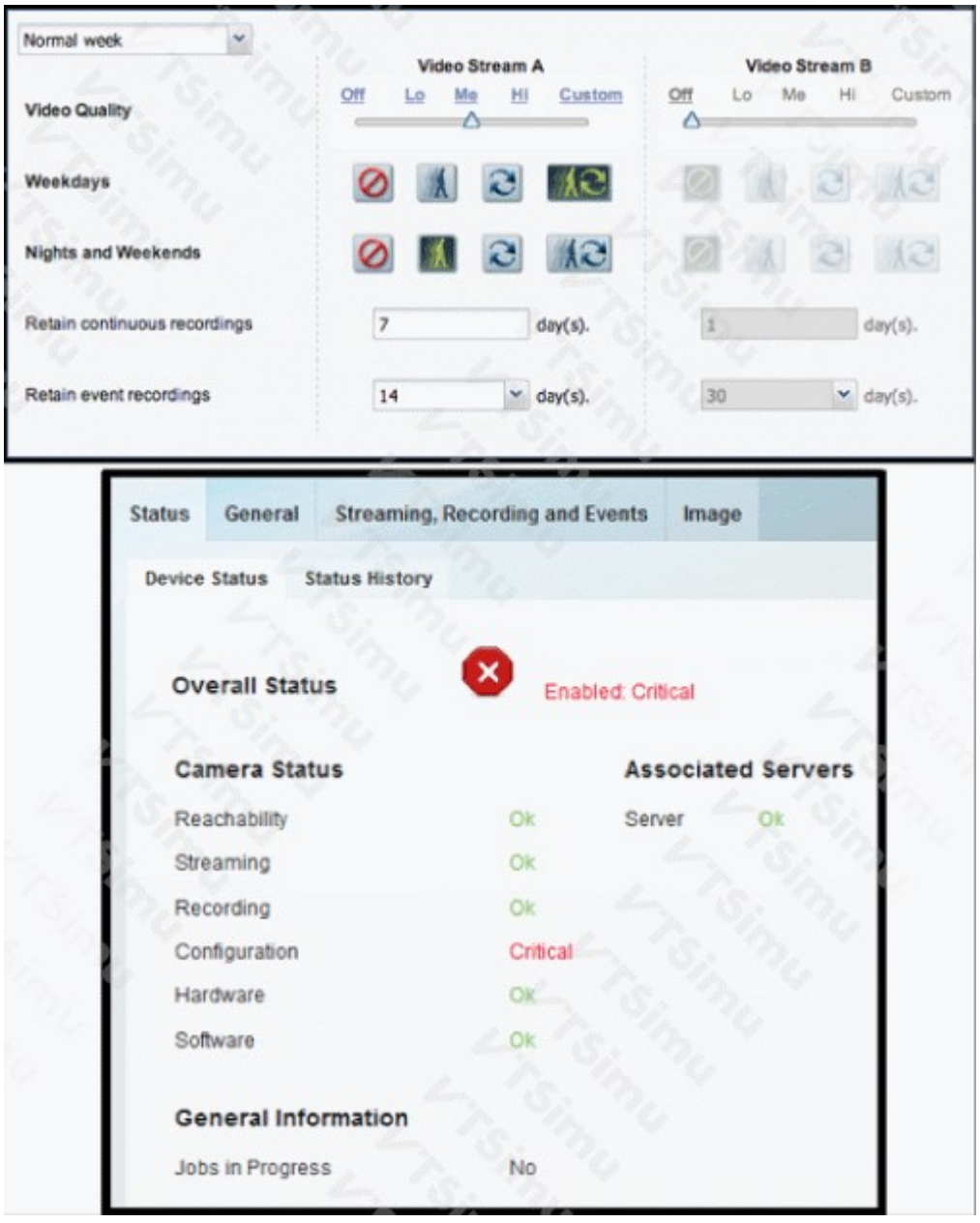
Mount the partition once the fstab entry is in place. Mounting makes the newly formatted filesystem available immediately at the repository directory, allowing the Media Server to access the actual disk space. Then apply `chown` to the partition directory so the applicable service account has the ownership required to create, manage, and write video repository data.

Proper ownership is essential because a mounted filesystem can be present and healthy while still being unusable to the application if the service lacks write access.

Finally, reboot the virtual machine. This confirms that the persistent mount definition is valid and that the partition comes back online at the expected repository path during startup. This sequence resolves the missing-media-partition condition by making the added storage both accessible now and durable across reboots. For background on persistent filesystem mounts, see the Red Hat documentation for persistent storage naming and mounts and the fstab manual page.

QUESTION NO: 9

Refer to the exhibit.



After you configure a new Cisco IP camera and save the configuration, you notice that under the Device Status tab for the same camera, Overall Status is Enabled: Critical. Despite the status, you can view the camera image and stream the video.

What is causing the Critical configuration status?

A. No motion detection window has been set.

B. The wrong template has been applied to the camera.

C. The selected resolution is unsupported.

D. There is a mismatch between the template settings and configurations on the IP camera itself.

ANSWER: A

Explanation:

No motion detection window has been set. The camera is reachable and its video stream is operating, so the Critical state does not indicate a basic network, registration, or video-transport failure. Instead, this status reflects an incomplete required camera configuration. When motion detection is enabled or expected by the camera configuration, at least one motion-detection window must be defined to identify the portion of the image in which motion events are evaluated. Without a defined window, the system can still receive and display live video, but it cannot apply the intended motion-event behavior. Cisco video-surveillance management platforms distinguish video availability from configuration health, allowing a device to continue streaming while flagging a missing required analytic or event-related setting as critical. Defining and saving an appropriate motion-detection window completes that portion of the camera setup and resolves the configuration condition. Cisco documentation for camera administration and event configuration is available in the Cisco IP Cameras documentation and the Cisco Video Surveillance Manager user-guide collection.

QUESTION NO: 10

Which two statements about wide dynamic range (WDR) cameras are true? (Choose two.)

A. WDR cameras can preserve detail in both bright and dark areas of the same scene

B. WDR is useful at entrances with a bright background

C. WDR automatically increases the camera frame rate

D. WDR eliminates the need for IR illumination at night

E. WDR requires MJPEG encoding

ANSWER: A B

Explanation:

WDR cameras can preserve detail in both bright and dark areas of the same scene and **WDR is useful at entrances with a bright background** are correct. A WDR camera is designed to handle scenes with a substantial difference between the brightest and darkest areas. Depending on the camera implementation, it may combine multiple exposures or use image processing to produce an image with usable detail across the scene.

This capability is especially valuable at entrances, loading bays, and lobby doors, where a subject inside a darker building may be framed against a bright outdoor background. WDR does not increase sensor resolution, replace infrared illumination, or determine the compression method used by the camera. See Axis guidance on wide dynamic range in network video.

QUESTION NO: 11

Which core component of the Cisco Video Surveillance solution is responsible for distribution, archiving, and storage of video feeds?

A. Cisco VSOM

B. Cisco SASD

C. Cisco VSMS

D. Cisco PSOM

ANSWER: C

Explanation:

Cisco VSMS is the correct component because the Cisco Video Surveillance Media Server is the media-handling layer of the Cisco physical-security architecture. It receives video streams from cameras and encoders, manages recording operations, and stores archived video on its associated storage resources. It also distributes live and recorded video streams to authorized client applications and viewing systems, allowing operators to access the required feeds without each client connecting directly to every camera. In this role, VSMS provides the core recording, retention, retrieval, and streaming services needed for a scalable surveillance deployment. Its storage and archive functions support the preservation of video evidence according to configured recording schedules, events, and retention requirements, while its distribution capabilities make video available for monitoring and investigation workflows. This separation of media services from higher-level operational management enables the surveillance solution to scale storage and streaming capacity independently as camera counts and client-viewing demands increase. Cisco identifies Video Surveillance Media Server as a core element for video recording and storage in its Video Surveillance Manager solution documentation. See Cisco's Video Surveillance Manager product information and the Cisco Video Surveillance Media Server documentation.

QUESTION NO: 12

When configuring the privilege level on a Cisco IP camera, which of the following is not a valid option?

A. Administrator

B. User

C. Monitor

D. Viewer

ANSWER: B

Explanation:

User is the correct selection because it is not one of the defined privilege-level names used by the Cisco IP camera user-account configuration relevant to this platform. Cisco camera administration interfaces assign permissions through named privilege levels rather than through a generic "User" level. These predefined levels control the scope of camera access, including whether an authenticated account can administer configuration, monitor camera operation, or access video as a viewer. Consequently, when the configuration requires selection of a privilege level, an account described simply as **User** does not match a valid privilege-level value and cannot be selected as such. This distinction matters operationally because privilege levels enforce role-based access to camera functions and help prevent ordinary video-access accounts from receiving administrative capabilities. Cisco's physical-security documentation and IP-camera support resources provide the applicable camera administration guidance and product documentation: Cisco IP Cameras Support and Cisco Physical Security documentation.

QUESTION NO: 13

Which four camera configurations are valid? (Choose four.)

A. CIVS-IPC-3530:1280x720 at 30 fps

B. CIVS-IPC-3530:1280x800 at 30 fps

C. CIVS-IPC-3530:1920x1080 at 5 fps

D. CIVS-IPC-6030:1280x720 at 30 fps

E. CIVS-IPC-6030:1280x800 at 30 fps

F. CIVS-IPC-6030:1920x1080 at 15 fps

ANSWER: A B D F

Explanation:

The valid configurations are **CIVS-IPC-3530:1280x720 at 30 fps**, **CIVS-IPC-3530:1280x800 at 30 fps**, **CIVS-IPC-6030:1280x720 at 30 fps**, and **CIVS-IPC-6030:1920x1080 at 15 fps**. The CIVS-IPC-3530 is a 1.3-megapixel camera whose supported full-frame-rate operating modes include both 1280-by-720 and 1280-by-800 at 30 frames per second. Its image sensor and encoding specifications do not provide a 1920-by-1080 operating mode. The CIVS-IPC-6030 is a 2-megapixel camera that supports 1280-by-720 video at 30 frames per second and its maximum 1920-by-1080 resolution at 15 frames per second. These resolution/frame-rate pairings are important because the camera's supported modes are fixed by its sensor, image-processing capability, and codec performance; a resolution alone is not sufficient to establish that a configuration is valid. Cisco's legacy product documentation and support resources for the relevant camera families are available through the Cisco Video Surveillance 3000 Series support page and the Cisco Video Surveillance 6000 Series support page.

QUESTION NO: 14

Which three server platforms for Cisco Physical Security have built-in support for redundant power supplies? (Choose three.)

A. Cisco UCS C-Series

B. Cisco UCS B-Series

C. Cisco UCS E-Series

D. Cisco UCS Express / SRE 9xx

E. Cisco CPS-MSP-2RU-K9

ANSWER: A B E

Explanation:

Cisco UCS C-Series, Cisco UCS B-Series, and Cisco CPS-MSP-2RU-K9 are the Cisco Physical Security server platforms that provide built-in redundant-power capability. UCS C-Series rack servers are designed with multiple hot-swappable power-supply units, allowing the server to continue operating if one supply or its associated power feed fails. Cisco documents the redundant power-supply architecture for C-Series platforms in its server installation and service documentation: Cisco UCS C220 Server documentation.

UCS B-Series blade servers obtain redundant power through the UCS 5108 Blade Server Chassis. The chassis uses a shared power infrastructure with multiple power supplies and redundancy modes, so a power-supply failure does not inherently remove power from installed blades. This chassis-level design is described in the Cisco UCS 5108 Blade Server Chassis documentation.

Cisco CPS-MSP-2RU-K9, the two-rack-unit Cisco Physical Security Multiservices Platform, likewise supports redundant power supplies for the higher availability expected of a physical-security server deployment. Redundant power is meaningful in this context because surveillance recording, video management, and related security services must remain available during an individual power-supply or feed failure.

QUESTION NO: 15

In the Cisco VSM 7.0.x solution, which three functions is Cisco VSOM used for? (Choose three.)

A. View live and recorded video.

B. Record video from IP cameras.

C. Upgrade the Cisco VSMS.

D. Modify the IP address of associated media servers.

E. Configure IP cameras, archives, and events.

F. Configure storage repositories for the system.

ANSWER: A D E

Explanation:

Cisco Video Surveillance Operations Manager (VSOM) is the management and operations component of the Cisco Video Surveillance Manager solution. It provides the operator-facing interface for viewing both real-time camera streams and video that has already been retained in the system. Thus, *View live and recorded video.* is a core VSOM function. VSOM is also the central configuration point for surveillance operations: administrators use it to add and configure cameras, define archives, and create event-related behavior, making *Configure IP cameras, archives, and events.* correct. In a distributed VSM deployment, VSOM maintains the association with Cisco Video Surveillance Media Servers and provides the management workflow for updating the address information of those associated servers. Therefore, *Modify the IP address of associated media servers.* is also a VSOM function. These capabilities reflect VSOM's role as the centralized management layer, while media-server processes perform the underlying video handling and recording work. Cisco's VSM documentation and product maintenance resources are available through the Cisco Video Surveillance Manager support page and the Cisco maintenance guides list.

QUESTION NO: 16

On a VSMS server, what is YaST used for?

A. To check the status of the RAID storage

B. To configure the network settings

C. To monitor the network performance

D. To troubleshoot video stream errors

ANSWER: B

Explanation:

YaST is used to configure the network settings on a VSMS server. YaST (Yet another Setup Tool) is SUSE Linux's administration framework, and its Network Settings module provides the supported interface for configuring network interfaces, IP addressing, routing, DNS, host names, and related connectivity parameters. Because a VSMS deployment depends on reliable communication among cameras, media servers, storage, client workstations, and management services, correctly defining the server's network configuration is a fundamental installation and maintenance task. Administrators can use YaST's graphical or text-based interface to apply these settings directly on the server console, which is particularly useful in appliance-style deployments where Linux configuration files are not normally edited manually. SUSE documents that network configuration can be managed through YaST and describes configuration of interfaces and network services in its system administration guide. Cisco's Physical Security documentation portal provides the product documentation context for Cisco video-surveillance platforms and their supporting server infrastructure. See the SUSE Linux Enterprise Server network configuration documentation and the Cisco Physical Security product documentation portal.

QUESTION NO: 17

A fixed-lens camera using a 3.6 mm lens is replaced with a 12 mm lens while the image sensor remains the same. What is the expected result?

A. The camera will have a wider field of view and greater image magnification

B. The camera will have a narrower field of view and greater image magnification

C. The camera will have a wider field of view and less image magnification

D. The camera resolution will increase without changing the field of view

ANSWER: B

Explanation:

The camera will have a narrower field of view and greater image magnification is correct. Increasing focal length narrows the angle of view captured by a camera. A 12 mm lens therefore captures a smaller portion of the scene than a 3.6 mm lens, while making objects within that smaller scene appear larger. This can be useful when monitoring a more distant target, such as a gate, doorway, or vehicle lane.

The tradeoff is reduced scene coverage. Lens selection must balance the distance to the target, required identification detail, sensor size, and the area that must remain visible. Axis provides an overview of lens selection and field-of-view concepts in its network video lens guide.

QUESTION NO: 18

Which three statements about the Cisco 4- and 8-channel standalone encoder are true?

A. They both support dual streaming on all ports.

B. They both support motion detection.

C. They both support simultaneous video and audio.

D. They both support H.264 compression.

ANSWER: B C D

Explanation:

The Cisco 4- and 8-channel standalone encoders both provide motion-detection capability, allowing the encoder to identify activity in configured video scenes and generate events that can be used by the video-surveillance application. Both models also support simultaneous video and audio operation, enabling analog-camera video to be encoded while associated audio is captured and carried with the surveillance stream. This is important where an operator needs both visual evidence and audio context from a monitored location.

Both encoder platforms support H.264 compression. H.264 provides efficient video compression for transmitting and storing surveillance footage while preserving video quality at practical bandwidth and storage levels. These common capabilities make either model suitable for integrating multiple analog cameras into a Cisco video-surveillance deployment, with the channel count being the principal distinction between the platforms. Cisco's product documentation for these standalone encoders identifies motion detection, audio/video functionality, and H.264 among their supported surveillance features. See the Cisco Video Surveillance encoder data sheet and the Cisco Video Surveillance support documentation.