[Q40-Q58 Try JN0-252 Free Now! Real Exam Question Answers Updated [Sep 21, 2024

Try JN0-252 Free Now! Real Exam Question Answers Updated [Sep 21, 2024 Get Ready to Pass the JN0-252 exam with Juniper Latest Practice Exam Q40. ..scheduled downtime lo push the latest firmware to all the APs you deployed at the site. You verified that all of the APs are working fine. When you go back to work, you notice no complaints from the users. When you check AP page, you notice that several APs have not rolled out with the latest firmware.

his scenario, how does Marvis categorize this Issue in the Marvis Action dashboard?
* The non-compliant Marvis Action is displayed.
* The high CPU Marvis Action is displayed.
* The missing VLAN Marvis Action is displayed.
* The port flap Marvis Action is displayed.
* When several APs fail to update to the latest firmware during a scheduled downtime, Marvis categorizes this issue as a “non-compliant” action.

* This categorization indicates that some APs are not adhering to the intended firmware version policy, which could potentially affect network performance or security.

* The non-compliant Marvis Action provides administrators with the necessary information to identify and rectify the issue,

ensuring all APs are updated as required.

* Reference: Juniper Networks documentation on Marvis Actions and firmware compliance.

Q41. According to Juniper Networks, what are two best practices for AP placement (excluding AP12) for optimal accuracy and stability of location-based services? (Choose two.)
* Mount the AP above the ceiling, the LED orientation does not matter.
* Enable a wireless mesh.
* Each AP should have an unobstructed line of sight to at least two other APs.
* Mount the AP on the ceiling with the LED facing the floor.

Line of Sight: For optimal accuracy and stability of location-based services, each access point (AP) should have an unobstructed line of sight to at least two other APs. This ensures robust triangulation and accurate location tracking.

Ceiling Mounting: Mounting APs on the ceiling with the LED facing the floor is recommended. This position provides the best coverage and performance for both Wi-Fi and BLE signals, essential for reliable location services.

Reference:

Juniper Mist Deployment Guide

Best Practices for AP Placement

Top of Form

Bottom of Form

Q42. You want to review client information about a specific AP.

In this scenario, where in the UI would you look?
* Access Points
* AP Insights
* Client Insights
* SLEs

Q43. You have five clients on the network and 20 minutes of statistics tot each client. In this scenario, how many user minutes does this equal?
* 100
* 20
* 80
* 120

Identify the Scenario: Five clients on the network and 20 minutes of statistics for each client.

Calculation:

User Minutes = Number of Clients Duration of Statistics.

User Minutes = 5 clients 20 minutes per client.

User Minutes = 100.

Conclusion:

The total user minutes in this scenario is 100.

Reference:

Mist Documentation on User Minutes: Mist Documentation

Q44. What Is the maximum number of Mist Edge devices supported for high availability?
* A maximum of two Mist Edge devices ate supported.
* A maximum of 16 Mist Edge devices ate supported.
* An unlimited number of Mist Edge devices are supported.
* A maximum of three Mist Edge devices are supported.

The maximum number of Mist Edge devices supported for high availability is two. This ensures that there is a backup device in place to take over in case the primary device fails, providing redundancy and maintaining network stability.

Reference:

Mist Edge Configuration Guide

Juniper Networks Mist Edge FAQs

Q45. Which Marvis Action category will detect a bad cable based on information and behavior of a single AP?
* AP
* Connectivity
* Layer 1
* Switch

Q46. Which step must you take when configuring rogue AP detection?
* Enable rogue AP detection.
* Set the proximity zones.
* Disable honeypot detection.
* Set the Radio Resource Management (RRM) interval.

Rogue AP Detection:

Rogue AP detection is crucial for maintaining network security by identifying unauthorized access points.

Configuration Step:

Enable Rogue AP Detection:

The first and necessary step in configuring rogue AP detection is enabling the feature in the Mist system.

Other Steps:

Setting proximity zones, disabling honeypot detection, and setting the RRM interval are additional configurations but not the initial or mandatory step.

Conclusion:

The correct answer is A.

Reference:

Mist Documentation on Rogue AP Detection: Mist Documentation

Q47. You are asked to configure Mist lo send e-mail alerts lo your organization administrators, who all have mailboxes that reside on the same e-mail server. Alerts are being generated and are visible in the Mist GUI. but only some administrators are receiving the alert emails.

What Is the problem in this scenario?
* The affected administrators have not enabled e-mail notifications in their Mist My Account settings.
* The user e-mail addresses are not correctly formatted.
* The organization does not have sufficient alert subscriptions.
* Your e-mail server is blocking e-mail from Mist.

Identify the Problem: Alerts are being generated and visible in the Mist GUI, but only some administrators receive the alert emails.

Possible Issues:

User email addresses not correctly formatted.

Email server blocking Mist emails.

Insufficient alert subscriptions.

Administrators not enabling email notifications.

Root Cause:

Since some administrators receive the alerts, email formatting and server blocking issues can be ruled out.

If alert subscriptions were insufficient, no administrators would receive the alerts.

The most likely cause is that the affected administrators have not enabled email notifications in their Mist My Account settings.

Resolution:

Ensure that all administrators have enabled email notifications in their Mist My Account settings.

Reference:

Mist Documentation on Notifications: Mist Documentation

Q48. ..has reported a network outage. After locating the user, you find that the switch interface facing the user Is down but there Is no alert in the Mist Ul. You want to ensure that in the future, you receive an alert when a switch *face is down. You have already verified that the Critical Switch Port Down alarm is configured and enabled on the Alerts Configuration page.

his scenario, which action in the Mist Ul will satisfy the requirement?
* Disable the Critical Switch Pott Down alarm on the Alerts Configuration page.
* Navigate to the switch in the Mist Ul and modify the Port Configuration to enable the Up/Down Port Alerts setting for the

interface.
* Navigate to the switch in the Mist Ul and modify the Port Profile configuration to enable Persistent (Sticky) MAC Learning for the Port Profile.
* Enable the Critical Switch Port Up alarm on the Alerts Configuration page.
* To ensure that you receive alerts when a switch interface goes down, you need to enable the Up/Down Port Alerts setting for the specific interface.

* This setting can be configured by navigating to the switch within the Mist UI and modifying the port configuration. Enabling this setting ensures that any changes in the port status, such as going down, will trigger an alert.

* This is critical for proactive network monitoring and to promptly address any connectivity issues.

* Reference: Juniper Networks documentation on configuring port alerts within the Mist UI.

Q49. How does Mist determine the location of clients in an Indoor setting?
* triangulation
* GPS
* probability surface
* trilateration
* Understanding Location Determination in Mist:

Mist uses advanced methods to determine the location of clients in an indoor setting.

* Possible Methods:

Triangulation: Uses angles to determine position, but not typically used by Mist.

GPS: Not feasible indoors due to signal limitations.

Probability Surface: Involves calculating the probability of a client’s location, but not the primary method used.

Trilateration: Uses the distance from multiple known points to determine the exact location.

* Mist’s Method:

Mist primarily uses trilateration to determine the location of clients by measuring the distance from at least three access points.

Q50. Which two SLEs report DHCP problems? (Choose two.)
* Successful Connects
* Time to Connect
* Capacity
* Throughput

Q51. Which two statements correctly describe the provisioning of greenfield and brownfield switches using the Mist Ul? (Choose two.)
* Greenfield switches are provisioned using the Adopt Switches button.
* Brownfield switches are provisioned using the Adopt Switches button.
* Greenfield switches are provisioned using the Claim Switches button.
* Brownfield switches are provisioned using the Claim Switches button.
* Both greenfield (new, unconfigured) and brownfield (pre-existing, configured) switches can be adopted into the Mist management

framework using the “Adopt Switches” button within the Mist UI.

* This process involves bringing the switches under Mist management by applying the necessary configurations and policies from the Mist cloud.

* The adoption process ensures that all switches, regardless of their initial state, are integrated and managed consistently within the Mist ecosystem.

* Reference: Juniper Networks documentation on switch adoption and provisioning using the Mist UI.

Q52. You just received the newest Mist AP and want to enable a feature that is only available at this time on Release Candidate 1.

In this scenario, using the Mist GUI, where would you determine which version of Release Candidate 1 is available for your AP?
* Support Tickets and Documentation -> Feature Updates
* Support Tickets and Documentation -> Ports & Endpoints
* Support Tickets and Documentation -> Mist Edge Updates
* Support Tickets and Documentation -> Firmware Updates

Reference: https://www.juniper.net/documentation/us/en/software/nce/nce-214-midsize-branch-mist-pwp/topics/topic-map/nce-214-midsize-branch-mist-example_part2.html

Q53. default, how long does an Installer role have access to a site tor Initial configuration before expiration?
* 7 days
* 24 hours
* unlimited
* 48 hours

Installer Role in Mist:

The Installer role is designed for initial site setup and configuration.

Access Duration:

By default, the Installer role has temporary access for a specific duration to ensure security and control.

Default Access Duration:

7 days: Installers typically have access to a site for 7 days, enough time to complete initial setup and configuration before access expiration.

Conclusion:

The correct answer is A.

Reference:

Mist Documentation on Role-Based Access: Mist Documentation

Q54. Under Man/Is Actions, what is required for Marvis to provide a visualization of low coverage and low-capacity issues within the network?
* a WAN edge device
* a cloud-ready switch

* a floor plan
* a Premium Analytics subscription

For Marvis, Mist AI’s virtual network assistant, to provide a visualization of low coverage and low-capacity issues within the network, a floor plan is required. This enables Marvis to map the coverage and capacity data to specific locations within the physical space, allowing for precise identification and troubleshooting of network issues.

Reference:

Juniper Mist AI Documentation

Marvis Actions

Q55. A customer wants to physically wire their interior automated sliding doors to Mist APs to directly control location access to certain office areas.

In this scenario, which Mist AP capability allows them to accomplish this task?
* header pins
* optical sensor
* audio sensor
* IoT interface

Q56. Which location mode is required to track BLE badges?
* wayfinding
* BLE asset visibility
* Wi-Fi location
* vBLE Engagement

Reference: https://www.juniper.net/us/en/products/cloud-services/asset-visibility.html

Q57. …are asked to enable Mist management at an existing site with previously configured EX3400 brownfield switches, and to add a new greenfield switch, which statement is correct in this scenario?
* You can mix brownfield switches and greenfield switches as long as they are running a Mist-supported version of Junos.
* You cannot mix greenfield and brownfield switches at the same site.
* Brownfield switches can be adopted but not managed.
* You can mix brownfield switches and greenfield switches at the same site, but only if they are running the same version of Junos.

* In the context of Mist management, “brownfield” switches refer to those that are already configured and deployed in a network, while “greenfield” switches are new and have no pre-existing configuration.

* Mist supports the integration and management of both brownfield and greenfield switches within the same site. The crucial requirement is that all switches, regardless of their initial state, must be running a version of Junos that is supported by Mist.

* This compatibility ensures that Mist can apply policies, configurations, and monitoring uniformly across all devices, facilitating a seamless management experience.

* Reference: Juniper Networks documentation on Mist AI and Junos compatibility requirements.

Q58. ..are troubleshooting a wireless authentication problem.

Which two Mist features would help you in this scenario? (Choose two.)
* audit logs
* packer capture

* client events
* access point events

Packet Capture: This feature allows for detailed inspection of traffic at the packet level. Capturing packets can help identify issues with authentication protocols, such as misconfigured settings or failures in the authentication exchange process.

Client Events: Monitoring client events provides insights into the client’s authentication attempts, including successes and failures. This data helps in pinpointing where in the process the failure occurs, whether at the client, access point, or authentication server.

Reference:

Juniper Networks Documentation