DUMPSBOSS.

Mist AIAssociate (JNCIA-MistAI)

Juniper JN0-253

Version Demo

Total Demo Questions: 12

Total Premium Questions: 120

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Mist AI Fundamentals	52
Topic 2, Wireless Assurance	30
Topic 3, Wired Assurance	11
Topic 4, WAN Assurance	9
Topic 5, Marvis Virtual Network Assistant	18
Total	120

QUESTION NO: 1

Which statement is correct about the relationship between Juniper Mist organizations and sites?

A. A Juniper Mist superuser login grants access to all organizations.

B. One Juniper Mist organization can contain multiple sites.

C. You must have one Juniper Mist superuser login for each site.

D. One Juniper Mist site can contain multiple organizations.

ANSWER: B

Explanation:

One Juniper Mist organization can contain multiple sites. Mist uses a hierarchical configuration model in which an organization is the top-level administrative container and sites are created beneath it. An organization commonly represents a customer, company, or other administrative domain, while a site represents a physical location—such as an office, branch, campus, or warehouse—or a logical subdivision of that environment. This structure lets administrators centrally manage organization-level resources and settings while applying configurations, assigning devices, and viewing operational information in the appropriate site context. Consequently, a single organization can be used to manage a distributed enterprise with many locations, each represented by its own site. Devices are then associated with the relevant site within that organization. This organization-to-site relationship is fundamental to navigating and administering the Mist portal, including tasks such as configuring WLANs, assigning access points, and monitoring user and network experience for individual locations. Juniper's documentation describes organizations as containing sites and identifies the site as the level at which devices are organized. See the Juniper Mist configuration hierarchy documentation and the Juniper Mist sites documentation.

QUESTION NO: 2

What are two important components monitored under WAN Edge Health SLEs? (Choose two.)

A. CPU utilization

B. memory utilization

C. application response times

D. ISP reachability

ANSWER: A B

Explanation:

WAN Edge Health SLEs include device-resource classifiers that identify conditions likely to affect the stability and forwarding capacity of an SD-WAN edge. **CPU utilization** is monitored because excessive control-plane or data-plane CPU consumption can prevent the WAN edge from processing routing, tunnel, security, and packet-forwarding tasks efficiently. A sustained high-CPU condition is therefore a meaningful indicator of degraded edge health and contributes to the SLE assessment.

memory utilization is also monitored because a WAN edge operating with high memory consumption may be unable to maintain normal software processes, routing information, sessions, and operational services reliably. Mist identifies high memory use as a WAN Edge Health classifier, enabling administrators to correlate an impaired SLE score with a resource condition on the appliance. Together, CPU and memory metrics give operations teams direct visibility into whether a device itself, rather than an external path, is limiting WAN service quality. Juniper describes Mist AI-driven operations and service-level monitoring at Juniper Mist AIOps and provides WAN documentation through the Juniper Documentation portal.

QUESTION NO: 3

Which two features are part of Juniper Mist Wired Assurance? (Choose two.)

A. template-based configuration for switches

B. template-based configuration for routers

C. WxLAN policies

D. port profiles

ANSWER: A D

Explanation:

Juniper Mist Wired Assurance includes **template-based configuration for switches** and **port profiles**. Wired Assurance centrally manages supported Juniper EX and QFX switches from the Mist cloud, using configuration templates to provide consistent, repeatable deployment at the organization, site, or switch level. Templates simplify operational administration by defining common switch settings, such as VLANs, network configuration, services, and device-specific variables, without requiring administrators to build each switch configuration independently.

Port profiles are also a Wired Assurance capability. A port profile defines the intended behavior and configuration of one or more switch ports, including settings such as access or trunk mode, VLAN membership, PoE behavior, and security-related port controls. Administrators can apply port profiles to standardize edge-port configurations across a wired environment. This supports faster provisioning and helps maintain consistent policy implementation as endpoint requirements change. Together, centralized templates and reusable port profiles are foundational Wired Assurance features for automating switch configuration and wired-access operations through the Mist dashboard.

Juniper documents these wired-switch configuration capabilities in the Mist Wired Assurance documentation and its switch configuration documentation.

QUESTION NO: 4

Which two subscriptions are required to use Marvis Minis? (Choose two.)

A. WiFi Management and Assurance

B. Marvis for Wireless

C. vBLE Engagement

D. Premium Analytics

ANSWER: A B

Explanation:

Marvis Minis requires an active wireless-assurance entitlement together with the Marvis service entitlement for wireless. **WiFi Management and Assurance** provides the Mist cloud wireless-management and assurance foundation: it licenses the APs and supplies the telemetry, service-level experience data, and operational context that Minis uses when it runs synthetic client tests. **Marvis for Wireless** enables the Marvis capabilities that include Marvis Minis for the wireless environment. Minis is therefore not purchased as an independent add-on; it is available to organizations entitled to Marvis for Wireless, while the underlying wireless infrastructure must also be covered by the applicable WiFi Management and Assurance subscription. This pairing allows the digital-twin clients to validate the actual Wi-Fi service path proactively and present results through Marvis. Juniper's Marvis Minis documentation states that Minis support is automatically included for an organization with an active Marvis for Wireless subscription, and Juniper's subscription documentation describes Marvis subscriptions as additional to the relevant base Assurance subscription. See Juniper Marvis Minis documentation and Juniper subscription overview.

QUESTION NO: 5

You are standardizing a group of remote EX Series switches. Every switch must receive common VLAN and DNS settings, while user-facing interfaces must consistently receive the same access VLAN and PoE behavior.

Which two Mist Wired Assurance configuration methods should you use? (Choose two.)

A. A switch template for the common VLAN and DNS settings

B. A port profile for the user-facing interface settings

C. A WLAN template for the common VLAN and DNS settings

D. An organization label for the user-facing interface settings

ANSWER: A B

Explanation:

A switch template is used to define reusable common switch settings, including elements such as VLANs and DNS configuration. **A port profile** is used to standardize the intended configuration of switch interfaces, including access or trunk behavior, VLAN assignment, and PoE settings. Device roles help apply configurations at scale, but they do not replace the template and port-profile objects that define these settings.

QUESTION NO: 6

Which two statements describe port profiles? (Choose two.)

A. They can be assigned to multiple ports.

B. They include a set of interface configurations.

C. They must be assigned to only one port.

D. They include a set of routing configurations.

ANSWER: A

Explanation:

They can be assigned to multiple ports. This describes the essential purpose of a port profile in Juniper Mist Wired Assurance: it is a reusable template for switch-port policy and configuration. Rather than configuring each physical port independently, an administrator defines the desired port behavior once in a profile and associates that profile with applicable ports. This supports consistent deployment of common endpoint connectivity policies, such as those needed for user-device, voice, IoT, or uplink-facing ports, while reducing repetitive configuration work and the risk of configuration drift. A single profile can therefore be used repeatedly where the same port behavior is required, including across relevant ports on managed switches in the organization. Reusability also makes operational changes more efficient: updating the intended port policy in the profile provides a centrally managed way to maintain consistent configuration for its assigned ports. This profile-based operational model is part of Mist's cloud-managed wired-assurance approach to simplifying switch administration. For Juniper's overview of Mist's AI-native wired operations, see Juniper Mist AI. Additional Mist documentation resources are available at Mist Documentation.

QUESTION NO: 7

You are asked to display your network devices using the Juniper Mist GUI as a single solution. Your network is made up of a wireless infrastructure of only Juniper APs, and the wired infrastructure has a mix of Juniper and non-Juniper switches. Your solution must ensure that all devices are displayed in the Juniper Mist GUI.

Given this scenario, how would you accomplish this task?

A. Use Wired Assurance with the Monitoring option.

B. Use Juniper Mist Marvis Actions.

C. Use Juniper Mist Asset Visibility.

D. Use Wi-Fi Management and Assurance with LLDP enabled on all switches.

ANSWER: A

Explanation:

Use Wired Assurance with the Monitoring option. Wired Assurance provides a common Juniper Mist cloud interface for wired infrastructure and can monitor supported third-party switches in addition to Juniper switches. This is important in a mixed-switch environment because the monitoring workflow allows non-Juniper devices to be added to the organization for visibility rather than requiring every switch to be Juniper-managed. The switches are typically integrated through supported telemetry mechanisms such as SNMP, enabling their inventory and operational status to be represented in the Mist interface.

The Juniper access points are already native Mist-managed devices and are displayed through the wireless portion of the platform. Combining that native wireless visibility with Wired Assurance's managed and monitoring capabilities gives the administrator one GUI in which to view the Juniper APs, Juniper switches, and supported non-Juniper switches. This matches the requirement for a single operational view while retaining the appropriate level of management or monitoring for each wired-device type. Juniper describes Wired Assurance as a cloud service for wired-network operations and visibility; see Juniper Wired Assurance and the Mist Wired Assurance documentation.

QUESTION NO: 8

An organization is developing an operations portal. The portal must update client markers on a floor-plan map as new location information becomes available and must also create an external incident whenever a Mist alarm occurs.

Which two integration methods should be used? (Choose two.)

A. WebSocket

B. REST API polling

C. E-mail notification

D. Webhook

ANSWER: A D

Explanation:

WebSocket is appropriate for the real-time client-location requirement because it maintains an open connection through which the portal can receive continuously updated information. **Webhooks** are appropriate for the alarm requirement because Mist can push matching event payloads to a customer-controlled HTTPS endpoint when an event occurs.

The REST API is suited to on-demand configuration and historical-statistics queries, but it is not the primary event-push mechanism. E-mail notifications do not provide a structured integration interface for automatically creating incidents.

QUESTION NO: 9

A hospital wants to reduce the time spent locating mobile medical equipment and also provide visitors with indoor directions to departments and patient services.

Which two Juniper Mist Location Services capabilities address these requirements? (Choose two.)

A. Asset Visibility

B. Wireless Assurance

C. Wayfinding

D. Dynamic Packet Capture

ANSWER: A C

Explanation:

Asset Visibility supports locating tagged equipment and other important objects within a building. **Wayfinding** provides indoor navigation experiences that can direct visitors to destinations using maps and location-aware applications.

Wireless Assurance focuses on network service experience, and Dynamic Packet Capture is a troubleshooting function. Neither provides the required asset-tracking or navigation capability.

QUESTION NO: 10

Under which category would you identify bad cables using Marvis Actions?

A. Connectivity

B. security

C. Layer 1

D. Clients

ANSWER: C

Explanation:

Layer 1 is the correct category for identifying bad cables in Marvis Actions. A cable is part of the physical network infrastructure, which corresponds to Layer 1 of the network model. In the Mist portal, the Marvis Actions dashboard groups detected issues into categories so administrators can quickly focus on the relevant domain. Selecting the Layer 1 category exposes physical-layer actions, including the bad-cable action.

Marvis identifies a bad-cable condition by analyzing telemetry and error patterns associated with wired links. This can include indicators such as excessive packet or frame errors, link instability, and related switch-port behavior. Presenting this finding as an actionable Layer 1 issue helps operations teams isolate a likely physical cabling fault and investigate or replace the affected cable efficiently. Juniper's Marvis Actions documentation describes Layer 1 as the location for resolving physical-layer issues and identifies bad cable as an action in that category. See the Juniper Marvis Actions documentation and the Juniper bad-cable action documentation for details.

QUESTION NO: 11

Your organization currently uses Access Assurance for 802.1X authentication of wireless users using user certificates. All users are currently placed in the same VLAN after authentication.

There are multiple VLANs at your sites.

In this scenario, how would you configure Access Assurance to make the network more secure?

A. Configure MAC Authentication Bypass (MAB) and assign WxLAN roles based on groups of MAC addresses.

B. Configure user authentication using EAP-TTLS and assign WxLAN roles based on AD user group.

C. Configure host (machine) authentication using EAP-TLS and assign WxLAN roles based on AD user group.

D. Configure user authentication using EAP-TLS and assign WxLAN roles based on AD user group.

ANSWER: D

Explanation:

Configure user authentication using EAP-TLS and assign WxLAN roles based on AD user group. EAP-TLS is the appropriate choice because the organization already uses user certificates for 802.1X authentication. This method provides

strong certificate-based user authentication and lets Access Assurance make an authorization decision using the authenticated user identity.

Access Assurance can use identity information and group membership to apply authorization policies. Mapping Active Directory user groups to WxLAN roles enables role-based segmentation: users in different groups can receive different roles after successful authentication, and each role can carry the intended network access policy, including the appropriate VLAN assignment. Instead of placing every successfully authenticated user into one shared VLAN, this creates separate access domains for groups such as employees, contractors, and other organizational roles. That segmentation supports least-privilege access by limiting a user to the network segment and resources appropriate for that user's established identity and group membership.

This approach retains the strong user-certificate authentication already deployed while adding policy-driven, dynamic authorization at connection time. For Juniper's Access Assurance documentation and related configuration guidance, see Juniper Mist Access Assurance documentation and Juniper Technical Documentation.

QUESTION NO: 12

Several users intermittently fail 802.1X authentication on one WLAN. The issue is difficult to reproduce, and the administrator needs packet-level evidence associated with affected clients.

Which Juniper Mist capability should be used?

A. Dynamic packet capture

B. Asset Visibility

C. Audit Logs

D. WAN Edge Insights

ANSWER: A

Explanation:

Dynamic packet capture is correct because it provides contextual packet data for troubleshooting wireless client problems, including intermittent connection and authentication failures. The captured traffic can help an administrator examine the relevant exchange without first placing a separate packet sniffer at the site. SLEs identify experience degradation, but they do not provide the packet-level evidence required for this investigation.