

Nokia.NRN-522.v2026-08-03.q56

Exam Code:	NRN-522
Exam Name:	Nokia 5G RAN Network Operations Expert
Certification Provider:	Nokia
Free Question Number:	56
Version:	v2026-08-03
# of views:	138
# of Questions views:	560
https://www.freepdfdumps.com/Nokia.NRN-522.v2026-08-03.q56.html	

NEW QUESTION: 1

Which AirScale management tool allows an engineer to connect directly to a single base station for local-level configuration viewing and diagnostics, as opposed to network-wide centralized management?

- A. NetAct CM Editor
- B. BTS Site Manager (local Element Manager)
- C. NetAct PM Reports
- D. SON Network Optimizer

Answer: B (LEAVE A REPLY)

The BTS Site Manager, also referred to as the local Element Manager, is the tool used to connect directly to an individual AirScale base station to view its local configuration, hardware inventory, logs, and run element-level diagnostics. It is typically used when an engineer needs granular, site-specific information that may not be fully visible through the centralized system, or when NetAct connectivity to the site is impaired. NetAct CM Editor is used for network-wide configuration management of many sites from the central OSS, NetAct PM Reports aggregates performance counters across the network, and the SON Network Optimizer automates parameter tuning across multiple cells. Because the question specifically asks about direct, single-element access for local diagnostics rather than network-wide operations, the BTS Site Manager is the correct answer, complementing NetAct in a complete remote operations toolkit.

NEW QUESTION: 2

What is the key distinction between a full site backup and a partial (configuration-only) backup in the context of base station lifecycle management?

- A. A full backup includes both the software load and the complete configuration data, while a partial backup typically captures only configuration data without the software image

- B.** A full backup only captures alarm history, while a partial backup captures performance counters
- C.** A partial backup can only be performed by a field engineer physically present at the site
- D.** There is no practical difference; both terms refer to identical backup content

Answer: [\(SHOW ANSWER\)](#)

A full site backup typically captures both the currently running software load (or a reference to it) and the complete configuration data for the network element, providing the most comprehensive restore point - useful before major changes such as software upgrades or significant hardware-related maintenance. A partial, or configuration-only, backup captures just the configuration data - the set of parameters defining how the element is provisioned - without necessarily including the software image itself. Configuration-only backups are commonly used before smaller-scope parameter changes, where the software load itself is not expected to change, since they are typically faster to perform and require less storage. Choosing the appropriate backup type depends on the scope of the planned change: a software upgrade warrants a full backup, while a routine parameter adjustment may only require a configuration backup. Neither backup type is restricted to alarm history or performance counters, and both can typically be performed remotely without requiring a field engineer to be present.

NEW QUESTION: 3

NetAct reports the transport link to a remote 5G site as 'up', but the NOC engineer still cannot establish an OandM session to the AirScale BTS. What is the MOST appropriate next troubleshooting step?

- A.** Immediately dispatch a technician to replace the RF module
- B.** Verify authentication credentials/certificates and the OandM IP/VLAN configuration on the base station
- C.** Increase the cell's reference signal transmit power
- D.** Restart the entire NetAct server

Answer: **B** [\(LEAVE A REPLY\)](#)

When basic transport/IP connectivity to a site is confirmed as up but an O and M management session still cannot be established, the issue is likely at a higher layer than physical or network-layer reachability.

Common causes include expired or mismatched security certificates, incorrect login credentials, or a misconfigured O and M IP address or management VLAN on the base station itself. A layered troubleshooting approach moves from transport, to network, to application/management-layer checks once lower layers are confirmed functional.

Replacing the RF module addresses a hardware radio issue, not an O and M session /authentication problem, and would be premature without further evidence. Adjusting reference signal power is unrelated to management connectivity. Restarting the entire NetAct server is a drastic action affecting the whole managed network and is never an appropriate first response to a single-site connectivity issue.

NEW QUESTION: 4

Which statement correctly describes how OandM (management) traffic and user-plane traffic (e.g., NG-U/N3) are typically handled on the transport network connecting an AirScale BTS?

- A.** They must always use exactly the same VLAN and IP address
- B.** They are typically separated using different VLANs and/or IP addressing for security, isolation, and traffic management purposes
- C.** OandM traffic cannot be carried over IP and requires a dedicated leased line
- D.** User-plane traffic configuration has no relationship to transport configuration at all

Answer: ([SHOW ANSWER](#))

For security, isolation, and quality-of-service reasons, AirScale base stations typically separate Operations and Maintenance (O and M) traffic from user-plane traffic (such as NG-U/N3 in 5G or S1-U in 4G) using distinct VLANs and/or IP addressing on the transport network. This separation ensures that configuration commands, alarm reporting, and software transfers travel on a logically isolated path from subscriber data, reducing the risk that issues or attacks affecting the user-plane path could impact management connectivity, and allowing each traffic type to be independently prioritized and monitored. It is incorrect that they must share identical addressing, that O and M cannot use IP (modern AirScale O and M is IP-based and typically carried over the same physical transport with logical separation), or that user-plane traffic configuration is unrelated to transport - transport interface parameters configured via NetAct CM directly determine how user-plane traffic is carried.

NEW QUESTION: 5

What is the primary purpose of the secure IPsec VPN tunnel established between a centralized Operations Center and a remote 5G site's transport network?

- A.** To boost the radio transmit power of the cell
- B.** To encrypt and authenticate OandM traffic exchanged between NetAct/NOC and the base station
- C.** To replace the need for alarm monitoring
- D.** To compress software packages before download

Answer: ([SHOW ANSWER](#))

Centralized Operations Centers connect to many geographically distributed 5G sites over shared transport infrastructure that may include third-party or public network segments. A secure tunnel, typically using IPsec, is established between the Operations Center's management domain and the site's security gateway to encrypt and authenticate all Operations, Administration, and Maintenance (O and M) traffic - including configuration commands, alarm and performance data, and software transfers - protecting it from interception, tampering, or unauthorized access. This secure channel has no effect on RF transmit power, which is governed by separate cell configuration parameters, and it does

not perform software compression, which is a function of the software packaging process itself. It also does not replace alarm monitoring, which is handled by NetAct's Fault Management module; rather, the VPN ensures that alarm data itself reaches the Operations Center securely.

NEW QUESTION: 6

What is the key difference between a graceful restart and an immediate (forced) restart of a base station unit during maintenance activities?

- A.** A graceful restart attempts to allow active sessions to complete or be handed over before the restart proceeds, reducing dropped connections, while an immediate restart proceeds without waiting, causing any active sessions to be dropped
- B.** A graceful restart permanently disables the unit, while an immediate restart only temporarily disables it
- C.** A graceful restart can only be performed by physically power-cycling the equipment on site
- D.** There is no functional difference between the two; both terms describe identical behavior

Answer: A (LEAVE A REPLY)

A graceful restart is designed to minimize the impact on active subscribers by allowing the system, where possible, to complete in-progress procedures or facilitate handovers of active sessions to neighboring cells before the restart actually takes effect, reducing the number of abruptly dropped connections. An immediate, or forced, restart proceeds without this consideration, restarting the unit right away regardless of any active sessions, which will be dropped as a result. NOC engineers may choose between these options depending on the urgency of the situation: a graceful restart is generally preferred for planned maintenance activities to minimize subscriber impact, while an immediate restart might be necessary in scenarios where a unit is unresponsive or where the urgency of resolving a critical fault outweighs the brief additional impact of dropped sessions. Neither option permanently disables the unit, and graceful restarts can be initiated remotely - they do not require physical power-cycling on site.

NEW QUESTION: 7

What best describes the role of 'remote piloting' as performed by a NOC engineer supporting a field engineer during an on-site hardware replacement?

- A.** The NOC engineer travels to the site to physically perform the hardware replacement alongside the field engineer
- B.** The NOC engineer uses centralized OandM tools to guide the field engineer through the procedure step- by-step, performing remote configuration, verification, and diagnostic actions while the field engineer carries out the physical tasks on site
- C.** The NOC engineer has no active role and simply waits for the field engineer to report task completion

D. The NOC engineer remotely controls the field engineer's vehicle to ensure timely arrival at the site

Answer: B (LEAVE A REPLY)

Remote piloting describes a collaborative working model in which a NOC engineer, using centralized O and M tools such as NetAct and element managers, actively supports a field engineer performing physical work at a site. The NOC engineer's responsibilities typically include preparing the network element for the activity (such as locking affected cells), providing real-time guidance based on system status and diagnostic data, performing remote verification steps (such as confirming a replaced module is detected and operating correctly), and executing any remote configuration steps the new hardware requires. This combination of remote expertise and on-site physical capability allows complex maintenance to be carried out efficiently without requiring every engineer involved to have both deep RAN engineering and bring physically present. It is an active, collaborative role - not a passive one - and it relates only to the technical task at hand, not to logistics such as travel arrangements.

NEW QUESTION: 8

A NOC engineer wants to confirm that a newly installed AirScale BTS has completed commissioning and is ready to carry live traffic. Which indicator provides this confirmation?

A. The site appears correctly on a public mapping application

B. The relevant cells show an unlocked/enabled administrative state and an operational 'in service' status in NetAct, with no blocking alarms

C. The transport provider confirms that fiber has been physically installed at the site

D. The power equipment vendor confirms their installation is complete

Answer: B (LEAVE A REPLY)

Commissioning brings a newly installed AirScale BTS under NetAct management, loads the correct software and configuration, and activates its cells. The definitive operational confirmation that commissioning is complete and the site is ready for live service is that the relevant cells show an unlocked (administratively enabled) state combined with an operational 'in service'/available status in NetAct, and there are no outstanding blocking faults or critical alarms preventing service. This combination of administrative and operational state, together with a clean alarm list, is what NOC engineers check before confirming a site is live. Appearing on a mapping tool, having fiber physically installed by the transport provider, or having power equipment installed are all useful prerequisite facts about the site's physical readiness, but none of them confirm that the RAN equipment itself has successfully completed commissioning and is carrying traffic.

NEW QUESTION: 9

Which KPI category includes the RRC Connection Setup Success Rate, which reflects a UE's ability to successfully gain initial access to the network?

A. Retainability

- B. Accessibility
- C. Mobility
- D. Integrity

Answer: (SHOW ANSWER)

Accessibility KPIs measure a UE's ability to successfully access network services when requested. RRC (Radio Resource Control) Connection Setup Success Rate is a foundational accessibility metric in 4G/5G, representing the percentage of RRC connection setup attempts - the first step a UE takes to establish a radio connection with the gNB - that complete successfully. A high accessibility value indicates subscribers can reliably initiate sessions when they attempt to. This differs from Retainability, which measures whether already-established connections remain stable until normally released; Mobility, which assesses handover performance as UEs move between cells; and Integrity, which assesses the quality and throughput of an established connection. Because RRC setup is the entry point to accessing the network, its success rate falls within Accessibility, a category NOC engineers monitor closely to detect access-related problems caused by congestion, misconfiguration, or hardware faults preventing initial connections.

NEW QUESTION: 10

Before activating a newly downloaded software package on a base station, why is it important to verify software compatibility with the unit's current hardware and configuration?

- A. Because activating an incompatible software package can result in activation failure, degraded functionality, or the unit failing to return to normal operation, even if the automatic fallback eventually recovers it
- B. Because software compatibility checks are only relevant for 2G equipment and do not apply to 5G base stations
- C. Because compatibility checks automatically update the site's physical inventory records
- D. Because compatibility verification eliminates the need for any post-activation monitoring

Answer: A (LEAVE A REPLY)

Verifying that a software package is compatible with a base station's specific hardware variants, installed modules, and current configuration before activation helps avoid activation failures or operational issues that can arise when a software load does not properly support the hardware it is being applied to, or when configuration elements are incompatible with structural changes introduced in the new software. While an automatic fallback mechanism may eventually recover the unit to its previous working state if activation fails, relying on fallback as the primary safeguard introduces avoidable service disruption and consumes a maintenance window without achieving the intended upgrade. Compatibility considerations are relevant across all supported technologies within Nokia's Single RAN portfolio, not just legacy systems, and compatibility checks are a software lifecycle planning activity - they do not update physical inventory records or remove the

need for post-activation health monitoring, which remains essential regardless of how thorough the pre-activation checks were.

NEW QUESTION: 11

A NOC engineer increases the configuredMaxTxPower parameter for a 5G cell as part of a coverage improvement initiative. What is the most likely operational consequence of this change?

- A.** The cell's coverage area may expand, but interference toward neighboring cells operating on the same or adjacent frequencies may also increase
- B.** The change has no impact on coverage or interference, only on the cell's software version
- C.** The cell will automatically reduce its bandwidth to compensate for the power increase
- D.** The change will immediately disable all neighbor relations associated with the cell

Answer: ([SHOW ANSWER](#))

The configuredMaxTxPower parameter sets the maximum transmit power level the cell is permitted to use for its downlink transmissions, including reference signals and traffic channels. Increasing this value generally allows the cell's signal to reach further and penetrate obstacles more effectively, potentially expanding the effective coverage area and improving signal quality for UEs at the cell edge. However, because radio signals do not respect cell boundaries, a higher transmit power also means the cell's signal will be stronger when received by UEs and sensors in neighboring cell areas, which can increase co-channel or adjacent-channel interference - particularly relevant in dense deployments where cells are closely spaced. This trade-off means power changes should be planned carefully and their impact monitored through KPIs such as SINR and throughput in both the target cell and its neighbors. The parameter has no direct effect on software version, bandwidth configuration, or neighbor relation status, which are governed independently.

NEW QUESTION: 12

A site reports a 'Rectifier Fault' or 'DC Power Fault' alarm together with multiple equipment alarms across different cabinets. What does the rectifier/DC power fault alarm relate to?

- A.** A software licensing issue on the base station
- B.** The site's AC-to-DC power supply system feeding the equipment
- C.** The configuration of neighboring cells
- D.** NetAct user account permissions

Answer: **B** ([LEAVE A REPLY](#))

A 'Rectifier Fault' or 'DC Power Fault' alarm relates to the site's power infrastructure - specifically the rectifier units that convert incoming AC mains power into the DC voltage used by BTS equipment, often backed by a battery system to ride through short outages. When this alarm appears alongside multiple equipment alarms across different cabinets or modules at the same site, it strongly suggests a shared power supply problem affecting all equipment dependent on that source, rather than independent hardware faults occurring

coincidentally across multiple unrelated components. This is unrelated to software licensing, neighbor cell configuration, or NetAct user permissions. Recognizing this pattern helps the NOC engineer correctly identify a power infrastructure issue as the likely root cause, prompting checks on AC mains status, battery backup health, or coordination with site facilities/power maintenance teams, rather than independently chasing each equipment alarm as a separate RAN hardware fault.

NEW QUESTION: 13

Which of the following best describes 'fault isolation' as performed by NOC technical support before deciding whether to dispatch a field engineer?

- A.** Replacing hardware components at random until the alarm clears
- B.** Using available remote diagnostics - alarms, correlation, PM data, interface status, and logs - to determine whether the fault likely lies in the baseband, RF, transport, or external/environmental domain
- C.** Assuming every fault automatically requires a full site rebuild
- D.** Disregarding any alarm correlation information available

Answer: B ([LEAVE A REPLY](#))

Fault isolation is the systematic process by which NOC technical support narrows down the likely location and cause of a fault using all available remote diagnostic information, before deciding whether a remote fix is possible or a field dispatch is required. This includes reviewing active alarms and their correlation (distinguishing root-cause from symptom alarms), examining relevant performance management data for anomalies, checking the status of interfaces between functional domains such as baseband-to-RF links or transport interfaces, and reviewing element logs where available. The goal is to determine whether the fault most likely resides in the baseband processing unit, an RF module, the transport network, or an external /environmental factor such as power or cooling, so that any field dispatch is properly scoped with the correct parts, tools, and instructions. Randomly replacing components, assuming a full rebuild is always needed, or ignoring correlation data are inefficient approaches that proper fault isolation is designed to avoid.

NEW QUESTION: 14

How do NetAct and the AirScale BTS local Element Manager (Site Manager) typically relate to each other in day-to-day remote operations?

- A.** NetAct eliminates any need for local element-level management tools
- B.** NetAct provides centralized, network-wide OAM, while the Element Manager provides detailed, element-specific local access for in-depth diagnostics
- C.** The Element Manager centrally manages multiple base station sites across the network
- D.** NetAct manages only 2G/3G technologies, while the Element Manager manages only 5G

Answer: ([SHOW ANSWER](#))

NetAct provides a consolidated, network-wide view of alarms, performance, configuration, and software status for all managed base stations, enabling efficient centralized operations at scale - this is the day-to-day tool for NOC monitoring and bulk provisioning. The BTS Site Manager (Element Manager) complements NetAct by providing detailed, element-specific access for situations requiring deep local diagnostics, such as reviewing local hardware status, logs, or actions not yet reflected centrally, or when central connectivity to a site is degraded. These two tools work together rather than as substitutes for one another. NetAct supports Nokia's Single RAN concept across 2G, 3G, 4G, and 5G technologies on shared hardware, so describing it as 2G/3G-only is incorrect, and the Element Manager is scoped to a single element rather than managing multiple sites network-wide, which is NetAct's role.

NEW QUESTION: 15

For security segmentation, NOC personnel typically do not connect directly from their workstations to production AirScale base stations. Instead, they first authenticate to an intermediate, hardened host. What is this intermediate host commonly called?

- A.** DNS server
- B.** Jump server / bastion host
- C.** Load balancer
- D.** Edge router

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 16

An operator is considering reducing the PM Result Output Period (ROP) for a set of cells from 15 minutes to

1 minute to enable near real-time troubleshooting. What is the most significant operational trade-off of this change?

- A.** Shorter ROPs make KPI formulas invalid and unusable
- B.** Shorter ROPs significantly increase the volume of measurement data generated and the load on collection and storage systems
- C.** Shorter ROPs automatically disable all alarm notifications for the affected cells
- D.** Shorter ROPs prevent NetAct from displaying any historical performance trends

Answer: ([SHOW ANSWER](#)**)**

Reducing the Result Output Period increases the frequency at which performance counters are collected, processed, and stored, which proportionally increases the volume of measurement data generated by each network element. Moving from a 15-minute to a 1-minute ROP, for example, would generate roughly fifteen times more data points over the same time period. This places significantly higher demand on the file transfer, processing, and storage capacity of NetAct and any downstream analytics systems, and can also increase signaling and processing load on the base stations themselves. While finer granularity can be valuable for short-term, targeted troubleshooting of a specific cell

during an active investigation, it is not typically sustainable as a network-wide, long-term configuration. KPI formulas remain valid regardless of ROP, alarm notifications are a separate mechanism unaffected by PM ROP settings, and historical trending remains possible - it simply involves more granular data points.

Valid NRN-522 Dumps shared by Actual4test.com for Helping Passing NRN-522 Exam! Actual4test.com now offer the **newest NRN-522 exam dumps**, the Actual4test.com NRN-522 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NRN-522 dumps with Test Engine here: https://www.actual4test.com/NRN-522_examcollection.html (122 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 17

A transport alarm 'Ethernet link down' is raised on the BTS-side interface toward the aggregation router. What is an appropriate FIRST remote action for the NOC engineer?

- A.** Replace the RF module at the site
- B.** Check the physical/data-link layer status and interface configuration of that port, and coordinate with the transport provider if needed before considering on-site dispatch
- C.** Modify the cell's neighbor relation list
- D.** Increase the configured cell bandwidth

Answer: (SHOW ANSWER)

When a transport-side alarm such as 'Ethernet link down' is raised on the BTS-facing interface toward the aggregation router, the appropriate first remote action is to investigate the physical and data-link layer status of that interface - checking link/port status, interface configuration such as speed and duplex settings and VLAN membership, and any visible cable/connector status indicators through management tools. If the issue appears to originate on the transport provider's side of the connection (such as a leased line or microwave link fault), coordinating with that provider is the next step. Only if remote checks cannot resolve the issue, or clearly indicate a physical hardware or cabling fault at the site, would on-site dispatch be considered.

Replacing the RF module addresses radio hardware, not a transport link fault, and modifying neighbor relations or cell bandwidth are RAN configuration changes that would not resolve a physical link failure.

NEW QUESTION: 18

A field team is planning a site visit to investigate a persistent coverage issue and requests information from the NOC to help prepare. What information can the NOC engineer most usefully provide to support this site survey?

- A.** The current cell configuration, recent alarm history, and relevant performance data (such as RSRP /SINR distributions and throughput trends) for the affected cell and its neighbors
- B.** The personal contact details of subscribers who have filed complaints about the area
- C.** The original purchase invoice for the site's equipment
- D.** A list of unrelated sites located in a different region of the country

Answer: (SHOW ANSWER)

When a field team is preparing to investigate a persistent coverage issue, remotely available operational data can significantly improve the efficiency and focus of their site visit. The NOC engineer can provide the current configuration of the affected cell (including parameters such as transmit power, tilt settings, and azimuth where available), a review of recent alarm history to identify any recurring or unresolved fault indications, and relevant performance data such as RSRP/SINR distributions and throughput trends, which can help characterize the nature of the coverage issue (for example, distinguishing a coverage gap from an interference problem) before the field team arrives. This context allows the field team to prioritize their investigation - for example, focusing on antenna alignment if tilt/azimuth data looks unusual, or focusing on potential external interference sources if SINR is poor despite adequate RSRP. Subscriber personal information, equipment purchase records, and data about unrelated sites would not provide relevant technical context for this investigation.

NEW QUESTION: 19

In NetAct's role-based access control model, which role would typically be assigned to a NOC engineer who needs to perform routine cell parameter and neighbor relation changes, but should NOT be able to modify user accounts or system-wide security settings?

- A.** System Administrator
- B.** Operator with Configuration Management (CM) provisioning privileges
- C.** Guest / read-only user
- D.** Database Administrator

Answer: B (LEAVE A REPLY)

NetAct's role-based access control allows different roles to be granted permission sets aligned with job responsibilities. An 'Operator' role with CM provisioning privileges is scoped to perform day-to-day configuration tasks - such as modifying cell parameters, neighbor relations, or power settings - without holding the broader privileges of a System Administrator, who manages user accounts, security policy, and overall NetAct system configuration. A Guest or read-only user can view alarms, performance reports, and configuration data but cannot make changes, so this role would prevent the engineer from performing the required provisioning tasks at all. A Database Administrator role focuses on the underlying database infrastructure supporting NetAct rather than RAN configuration provisioning. Assigning an Operator role with CM privileges follows the least-privilege

principle: the engineer receives exactly the access required to perform routine provisioning, and nothing more.

NEW QUESTION: 20

When planning a maintenance window for a software activation affecting multiple cells at a site, which factor is most important for the NOC team to consider in order to minimize subscriber impact?

- A.** The current software version number, since higher version numbers always indicate lower traffic
- B.** Historical traffic patterns for the site, choosing a time period when traffic is at its lowest to minimize the number of active sessions affected by the restart
- C.** The PLMN ID of the site, since different PLMN IDs require different maintenance windows
- D.** The number of active alarms at the site, since more alarms always mean lower traffic

Answer: B (LEAVE A REPLY)

Because software activation typically requires affected cells to restart, briefly interrupting service for any actively connected UEs, the most important factor in selecting a maintenance window is identifying a time period when traffic at the site is at its lowest, based on historical traffic pattern analysis. Sites can have different busy-hour profiles depending on their location and the population they serve - for example, a site near a business district may have low traffic late at night, while a site in a residential entertainment area might have different patterns - so generic assumptions about 'off-peak' hours should ideally be validated against actual historical data for that specific site. Software version numbers, PLMN IDs, and current alarm counts have no inherent relationship to traffic levels and should not be used as proxies for determining the best maintenance window; traffic pattern data is the relevant and reliable input for this planning decision.

NEW QUESTION: 21

A 'Loss of Synchronization Reference' alarm appears on a 5G cell. Which input to the BTS is this alarm most directly associated with?

- A.** The GNSS/timing reference (e.g., GPS) or other synchronization source feeding the base station
- B.** The cell's neighbor relation list
- C.** The handover success rate KPI
- D.** The NetAct user account password

Answer: A (LEAVE A REPLY)

5G base stations require accurate frequency, and for many configurations (especially TDD operation and features like carrier aggregation) phase/time synchronization, typically derived from a GNSS receiver such as GPS or from a network-distributed timing source such as Synchronous Ethernet or PTP/IEEE 1588 over the transport network. A 'Loss of

Synchronization Reference' alarm indicates the BTS has lost access to its timing source. This can lead to degraded performance and, in TDD deployments, can cause uplink/downlink timing misalignment between neighboring cells (interference), and may force the cell out of service if synchronization cannot be maintained. The correct troubleshooting focus is therefore the GNSS antenna /receiver, related cabling, satellite visibility/obstructions, or the alternative network-based synchronization path - not neighbor relation configuration, handover KPIs, or NetAct account credentials, none of which relate to the BTS's timing reference source.

NEW QUESTION: 22

Cell Availability KPI is typically calculated based on which factor?

- A.** The percentage of time during a measurement period that a cell is in service, not blocked by faults or administrative locks
- B.** The number of active NetAct user sessions at a given moment
- C.** The total number of software upgrades performed on the cell
- D.** The signal strength reported by a single UE in the cell

Answer: A (LEAVE A REPLY)

Cell Availability is a KPI that reflects the proportion of time during a measurement period that a cell is actually capable of carrying traffic - that is, it is not blocked by an active fault condition or an administrative lock (an intentional disable for maintenance). It is typically expressed as a percentage of total elapsed time, with downtime due to either faults or planned outages subtracted from the period considered. This KPI provides a high-level view of how reliably a cell has been able to serve subscribers over time, and sustained low availability for a particular cell would prompt investigation into recurring faults or excessive planned outages. It is unrelated to the number of active NetAct user sessions, the count of software upgrades performed (although upgrades may contribute to planned downtime), or signal strength reported by an individual UE, which is a radio measurement rather than a network-wide availability statistic.

NEW QUESTION: 23

Which NetAct functional area provides tools that allow an operator to apply the same parameter change consistently to multiple AirScale base stations or cells in a single operation?

- A.** Fault Management
- B.** Performance Management
- C.** Configuration Management (Bulk/Mass Update)
- D.** Software Management only

Answer: C (LEAVE A REPLY)

NetAct's Configuration Management (CM) area provides bulk/mass update capabilities that let an operator define a parameter change once - such as updating a neighbor relation, adjusting a power parameter, or enabling a feature - and apply it consistently across many

base stations or cells in a single, auditable operation. This is fundamental to standard provisioning tasks covered in remote operations, allowing large-scale configuration rollouts without logging into each element individually, while maintaining consistency and an audit trail of who changed what and when. Fault Management focuses on collecting, displaying, and correlating alarms rather than making configuration changes. Performance Management focuses on collecting and reporting KPI/counter data. Software Management can distribute and activate software packages across multiple base stations, but it does not handle parameter and configuration provisioning, which is the specific domain of Configuration Management's bulk operations tools.

NEW QUESTION: 24

A NOC engineer observes that a 5G cell's average downlink user throughput has dropped significantly, but the cell's PRB utilization remains low and no transport alarms are active. Which root cause is most consistent with these observations?

- A.** The cell is severely congested due to a sudden increase in connected users
- B.** Degraded radio link quality is causing a shift toward lower-order modulation and coding schemes
- C.** The backhaul link to the cell site has failed completely
- D.** The cell has been administratively locked by an operator

Answer: B (LEAVE A REPLY)

When PRB utilization is low, the cell is not resource-constrained, which rules out congestion as the cause of reduced throughput. A complete transport failure or an administrative lock would prevent the cell from carrying any traffic at all, which contradicts the scenario where the cell is still active and reporting measurements. The most consistent explanation is degraded radio conditions - for example, increased interference, reduced signal-to-noise ratio (SINR), or coverage issues - which force the scheduler to select lower-order Modulation and Coding Scheme (MCS) values for connected users. Lower MCS values mean each allocated resource block carries fewer bits, directly reducing achievable throughput even though plenty of PRB capacity remains available. Investigating MCS distribution counters and SINR-related measurements alongside checking for nearby interference sources or antenna/feeder issues would be the appropriate next troubleshooting step.

NEW QUESTION: 25

When a software package is transferred to a base station via SFTP as part of a remote software delivery, what is the purpose of performing a checksum verification on the downloaded file before activation?

- A.** To confirm that the downloaded file has not been corrupted or altered during transfer, ensuring that activation proceeds using a complete and intact software image
- B.** To automatically translate the software package into a different programming language
- C.** To determine the geographic location of the base station

D. To calculate the cell's current handover success rate

Answer: ([SHOW ANSWER](#))

A checksum (or hash value) verification compares a calculated value derived from the downloaded software file against an expected reference value provided by the software source. If the values match, this confirms that the file was transferred completely and without corruption or unauthorized modification during the transfer process - which is particularly important for large software images transferred over networks where transient errors, interruptions, or transmission issues can occasionally cause partial or corrupted downloads.

Activating a software package from a corrupted or incomplete file could lead to activation failures, unpredictable behavior, or a unit that fails to return to normal operation - even before any compatibility or configuration considerations come into play. Checksum verification is a foundational integrity check performed as part of the software delivery process and has no relationship to programming language translation, geographic location determination, or performance KPI calculations, which are entirely unrelated functions.

NEW QUESTION: 26

A NOC engineer observes an 'alarm storm' - dozens of alarms appearing within seconds across multiple cells served by the same site. What is the MOST likely explanation?

- A.** Each cell independently and coincidentally developed an unrelated hardware fault at exactly the same moment
- B.** A shared resource serving all those cells - such as the transport link, power supply, System Module, or synchronization source - has failed
- C.** NetAct has a software defect that always duplicates alarms across cells
- D.** These alarms are unrelated to the site and can be safely ignored

Answer: ([SHOW ANSWER](#))

An 'alarm storm' - many alarms appearing across multiple cells at a single site within a short window - is a classic indicator that a shared resource serving all of those cells has failed. Multiple cells at a site commonly depend on the same System Module (baseband), the same transport connection back to the aggregation/core network, the same power supply, or the same synchronization source; a failure in any one of these shared elements can simultaneously impact every dependent cell, producing a burst of correlated alarms. Recognizing this pattern allows the NOC engineer to search for a single common-cause fault - for example, a transport outage or System Module failure - rather than treating each cell's alarms as independent issues requiring separate investigation. It is extremely unlikely that multiple independent hardware faults occur simultaneously by coincidence, and such patterns should never be dismissed as a routine NetAct bug or simply ignored.

NEW QUESTION: 27

What is a 'threshold crossing alert' (TCA), and how does it differ from a standard equipment fault alarm?

- A.** It is functionally identical to an equipment fault alarm in every respect
- B.** It is generated when a monitored performance counter or KPI (e.g., PRB utilization) crosses a configured threshold, indicating a performance condition rather than necessarily a hardware failure
- C.** It applies only to software license expiry alarms
- D.** It is a fixed system value that operators cannot configure

Answer: B (LEAVE A REPLY)

A threshold crossing alert (TCA) is generated when a monitored performance counter or KPI - such as PRB utilization, processor load, or a quality metric - crosses an operator-configured threshold value, providing visibility into a performance-related condition that may or may not correspond to an actual hardware fault.

For example, sustained high PRB utilization on a cell might trigger a TCA flagging a capacity concern, prompting capacity planning or optimization actions, even though no equipment has failed. This differs fundamentally from a standard equipment fault alarm, which is raised in direct response to a detected hardware or communication failure condition. TCAs are configurable by the operator, allowing thresholds to be tuned to the network's specific performance targets and capacity planning needs, and they are not limited to software license conditions, nor are they fixed, unconfigurable values.

NEW QUESTION: 28

A NOC team is investigating a degradation in E-RAB / QoS flow setup success rate for a specific gNB.

Which approach is MOST effective for identifying the root cause?

- A.** Reviewing only high-level marketing performance summaries
- B.** Correlating the KPI degradation with active alarms, recent configuration changes, and relevant counters (e.g., resource congestion, transport, signaling) for that gNB during the affected period
- C.** Restarting NetAct entirely without further analysis
- D.** Assuming the cause is always the subscribers' devices without checking network-side data

Answer: B (LEAVE A REPLY)

Investigating a degradation in E-RAB or 5G QoS flow setup success rate for a specific gNB is most effectively approached by correlating multiple data sources covering the affected time period: checking active alarms on that gNB (hardware, transport, or signaling faults), reviewing the configuration management audit trail for any recent parameter change that coincided with the degradation, and examining relevant performance counters such as resource availability/congestion indicators, transport interface statistics, and signaling success/failure counts. This multi-source correlation identifies whether the degradation stems from a hardware fault, a configuration error, a capacity constraint, or a transport issue, enabling targeted remediation. Reviewing only high-level summary reports lacks the technical granularity required. Restarting NetAct is a drastic, unfocused action unrelated to

a single gNB's issue and risks disrupting network-wide monitoring. Assuming the cause is always subscriber devices, without first checking network-side data, skips the most relevant and controllable areas of investigation.

NEW QUESTION: 29

A NOC engineer is trying to isolate whether a fault originates in the baseband processing unit or in an RF module of an AirScale BTS. What is a useful FIRST diagnostic step?

- A.** Immediately replace the antenna
- B.** Check the status and alarm details of the interface (such as CPRI/eCPRI links) between the System Module and the RF unit
- C.** Restart the entire NetAct management server
- D.** Increase transmit power to see if the fault changes

Answer: B (LEAVE A REPLY)

When isolating a fault between baseband processing units and RF modules, checking the status and alarm details of the interconnecting interface - typically a CPRI or eCPRI link in AirScale architectures - between the System Module and the Radio unit is a logical first step. Alarms or abnormal status on this link can quickly reveal whether the problem lies in the connection itself (such as a fiber/cable fault or configuration mismatch) or within one of the connected components. This follows the principle of checking interfaces and boundaries before assuming a specific component has failed, avoiding unnecessary or premature hardware replacement. Replacing the antenna skips this diagnostic step entirely and risks an unwarranted field action.

Restarting NetAct is a network-wide action inappropriate for a single-site fault. Increasing transmit power to

'test' a suspected hardware issue is not a valid diagnostic method and could create interference.

NEW QUESTION: 30

A NOC engineer notices that UEs in a cell are triggering handovers to a neighboring cell and then quickly handing back, repeating this cycle (a 'ping-pong' pattern). Which parameter adjustment is most likely to help reduce this behavior?

- A.** Increasing the handover event hysteresis and/or time-to-trigger values for the relevant measurement event between the two cells
- B.** Disabling the neighbor relation between the two cells entirely
- C.** Increasing the PCI value of one of the two cells
- D.** Reducing the channel bandwidth of both cells

Answer: (SHOW ANSWER)

Ping-pong handovers occur when a UE repeatedly hands over back and forth between two cells, often because the signal levels of both cells are very close to each other near the cell boundary, causing the handover trigger condition to be met in alternating directions in quick succession. Handover events (such as an A3 event, where a neighbor's signal

becomes a defined offset better than the serving cell) include configurable hysteresis and time-to-trigger parameters. Increasing the hysteresis margin requires a more substantial and sustained signal difference before a handover is triggered, while increasing the time-to-trigger requires the condition to be met for a longer continuous duration before the measurement report is sent. Both adjustments reduce sensitivity to short-term signal fluctuations, directly addressing ping-ponging.

Disabling the neighbor relation would prevent legitimate handovers entirely, harming mobility performance; changing PCI values or bandwidth does not address the underlying signal-level trigger sensitivity that causes ping-pong behavior.

NEW QUESTION: 31

NetAct shows an AirScale gNB as 'Connection Lost' although there has been no reported power outage at the site. What should the NOC engineer check FIRST?

- A. RF unit VSWR readings
- B. IP connectivity/transport link between NetAct and the site (routing, firewall, backhaul status)
- C. Cell Physical Cell Identity (PCI) configuration
- D. Antenna electrical tilt settings

Answer: B (LEAVE A REPLY)

A complete loss of O and M connectivity status in NetAct, without an associated power loss, most commonly indicates a problem in the IP path between the management system and the site - such as a backhaul

/transport link failure, a routing misconfiguration, a firewall rule change, or a fault on the site router or switch. Standard remote troubleshooting methodology follows a layered, 'isolate before escalate' approach:

confirm basic transport and IP reachability first (for example, checking link status, ping/traceroute results to the site's O and M address) before investigating radio-related items. RF unit VSWR, PCI configuration, and antenna tilt are radio-domain parameters that would not cause a total O and M connectivity loss, and checking them first would waste time and delay resolution. Verifying the transport path quickly narrows the fault domain and determines whether the issue can be resolved remotely or requires field dispatch.

Valid NRN-522 Dumps shared by Actual4test.com for Helping Passing NRN-522 Exam! Actual4test.com now offer the **newest NRN-522 exam dumps**, the Actual4test.com NRN-522 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NRN-522 dumps with Test Engine here: https://www.actual4test.com/NRN-522_examcollection.html (122 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 32

A NOC engineer is considering performing a remote factory reset on a base station as a troubleshooting step for a persistent issue. What is the most significant risk of this action if performed without proper preparation?

- A. A factory reset has no effect on the unit's configuration and is therefore always safe to perform
- B. A factory reset may erase the unit's current configuration, requiring a full restoration from backup (or re-commissioning) to return the site to its operational state
- C. A factory reset automatically creates a new backup of the current configuration before proceeding
- D. A factory reset only affects the unit's physical LED indicators and has no impact on service

Answer: B (LEAVE A REPLY)

A factory reset typically returns a network element to its default, out-of-the-box configuration state, which generally means erasing the unit's current operational configuration - including cell parameters, neighbor relations, and other site-specific provisioning. If performed without first ensuring a verified, complete configuration backup is available, this action can leave the site without the configuration needed to resume normal operation, requiring a time-consuming restoration from backup or, in the worst case, a full re-commissioning process involving significant manual effort. Given this risk, a factory reset is generally considered a last-resort troubleshooting action, used only when less drastic remote troubleshooting steps have been exhausted, and only after confirming that a usable backup exists and that the operational impact (likely requiring an extended outage for the affected cells) is acceptable and properly scheduled. The action does not automatically create its own backup, nor is its impact limited to cosmetic indicators - it directly affects the unit's operational state.

NEW QUESTION: 33

Before granting a new NOC engineer remote access credentials to production AirScale sites, what should be verified according to Nokia's operational security practices?

- A. That the engineer owns a personal mobile phone
- B. That the engineer has completed required training and is assigned a role matching their responsibilities under the least-privilege principle
- C. That the engineer holds physical keys to all site cabinets
- D. That the engineer's account has unrestricted access to all NetAct modules by default

Answer: B (LEAVE A REPLY)

Before a new NOC engineer is granted credentials to access live production AirScale sites, operational security practice requires confirming the individual has completed the appropriate training for the tools, procedures, and risks involved, and that their account is provisioned with a role matching their actual job responsibilities, following the least-privilege principle of granting only the access necessary to perform assigned tasks. This

minimizes the risk of accidental or unauthorized actions on a live network by inexperienced or over-privileged users. Owning a personal mobile phone or holding physical site keys relate to unrelated personal or facility-access matters and have no bearing on logical access provisioning for remote OAM systems. Granting unrestricted access to all NetAct modules by default directly contradicts least-privilege principles, increases organizational risk, and is explicitly the kind of practice operational security guidelines aim to prevent.

NEW QUESTION: 34

A base station has the necessary software installed to support a new advanced scheduling feature, but the feature remains inactive. The NOC engineer is informed that a license-related step is required. What is the most likely explanation?

- A.** The feature requires a software downgrade before it can be used
- B.** Many advanced features require a valid license key to be activated in addition to having the supporting software installed, separating software capability from commercial entitlement
- C.** The feature can only be activated by physically replacing the baseband module
- D.** The feature will activate automatically once the next scheduled software upgrade occurs, regardless of licensing

Answer: B (LEAVE A REPLY)

In many telecom equipment vendors' licensing models, including Nokia's, having the software capability to support a feature installed on the base station is necessary but not always sufficient for that feature to be operational. Many advanced or optional features require a corresponding license key to be applied and activated, which represents the commercial entitlement to use that capability. This separation allows operators to purchase and activate features incrementally as needed, without requiring different software builds for different feature sets. A NOC engineer encountering an inactive feature with the correct software already installed should verify the license status for that feature and, if needed, coordinate with the appropriate team to apply or activate the required license. This is unrelated to software downgrades, hardware replacement, or waiting for a future software upgrade - none of which would resolve a licensing gap, since the underlying software already supports the feature.

NEW QUESTION: 35

After a remote configuration change causes unexpected cell behavior, and the automatic fallback mechanism does not fully resolve the issue, what is the most appropriate next step for the NOC engineer?

- A.** Restore the affected network element's configuration from the most recent verified pre-change backup
- B.** Permanently decommission the affected cell
- C.** Apply a completely different, unrelated configuration template to the cell
- D.** Wait indefinitely without taking action, since the issue will eventually self-correct

Answer: A (LEAVE A REPLY)

When a configuration change leads to unexpected behavior and any automatic fallback does not fully restore normal operation, the appropriate recovery action is to restore the affected network element's configuration from the most recent verified backup taken before the change was applied. This returns the element to its known-working state, addressing the immediate service impact while the root cause of the unexpected behavior from the new configuration can be investigated separately, outside of the live production environment if needed. This is precisely why taking and verifying a pre-change backup is emphasized as a best practice - it provides exactly this kind of recovery option.

Decommissioning the cell is a drastic and disproportionate response to a configuration issue; applying an unrelated template introduces further uncertainty and risk; and taking no action prolongs any service degradation unnecessarily, which is inconsistent with the NOC's responsibility to restore service promptly.

NEW QUESTION: 36

The PLMN ID broadcast by a 5G cell is composed of which two elements, and what is its primary function?

- A.** Cell ID and Tracking Area Code - used to route handovers between cells
- B.** Mobile Country Code (MCC) and Mobile Network Code (MNC) - used by UEs to identify and select the correct operator's network
- C.** PCI and frequency band - used to determine cell transmit power
- D.** IP address and VLAN ID - used for OandM transport routing

Answer: B (LEAVE A REPLY)

The Public Land Mobile Network Identity (PLMN ID) is composed of a Mobile Country Code (MCC), which identifies the country in which the network operates, and a Mobile Network Code (MNC), which identifies the specific mobile network operator within that country. This combination is broadcast by every cell as part of its system information and is used by UEs during network selection and registration to confirm they are camping on a cell belonging to their home operator or an authorized roaming partner. Correct PLMN configuration is fundamental: an incorrect PLMN ID would cause UEs belonging to that operator to treat the cell as unsuitable, preventing any subscribers from camping on it. This is entirely separate from Cell ID/TAC (used for tracking and identification within a network), PCI (used for physical-layer cell identification), and transport-layer addressing such as IP/VLAN configuration, which serve different operational purposes.

NEW QUESTION: 37

Why is it considered a best practice to verify the integrity of a configuration or software backup file shortly after it is created, rather than assuming the backup process completed successfully?

- A.** Because a backup that appears to have completed without verification could be incomplete or corrupted, and this would only be discovered when it is needed for a restore - at which point recovery options become severely limited
- B.** Because backup verification automatically improves the cell's KPI performance
- C.** Because verification is required by NetAct before any alarms can be displayed for the element
- D.** Because unverified backups cause the base station to continuously restart

Answer: A (LEAVE A REPLY)

A backup operation reporting a successful completion status does not always guarantee that the resulting backup file is complete, uncorrupted, and usable for a future restore - issues such as interrupted transfers, storage errors, or partial writes can sometimes occur without being immediately obvious. The critical risk is that such problems are often only discovered at the moment a restore is actually needed - typically during a recovery from a failed upgrade or configuration change - at which point the absence of a usable backup severely limits recovery options and can significantly extend an outage. For this reason, verifying backup integrity (for example, through checksum validation, file size checks, or test restores where feasible) shortly after creation is considered a best practice, ensuring that if a restore is ever needed, the backup can be relied upon. Backup verification has no relationship to KPI performance, alarm display functionality, or causing repeated restarts - its sole purpose is to confirm the backup's usability for recovery.

NEW QUESTION: 38

During a remote piloting activity, the NOC engineer and field engineer are unable to bring a replaced RF unit into service despite following standard verification and troubleshooting steps, and a hardware fault on the new unit itself is suspected. What is the most appropriate next step?

- A.** Continue indefinitely repeating the same remote troubleshooting steps without involving any other teams
- B.** Escalate the issue to the next-level support team or vendor technical assistance, providing documented details of the steps already performed, the symptoms observed, and the suspected hardware fault, to support further diagnosis or part replacement
- C.** Instruct the field engineer to discard the new unit and leave the site without further communication
- D.** Permanently delete the cell's configuration from NetAct to resolve the issue

Answer: B (LEAVE A REPLY)

When standard remote troubleshooting and on-site verification steps have been exhausted and a hardware fault on the newly installed unit itself is suspected, continuing to repeat the same steps is unlikely to be productive and delays resolution. The appropriate next step is to escalate the issue to the next level of support

- which may be a specialized technical support team or the equipment vendor's technical assistance center - providing clear documentation of what steps have already been

performed, the specific symptoms observed (such as particular alarm codes or link status indications), and the basis for suspecting a hardware fault on the new unit. This documentation allows the receiving team to avoid repeating already-completed steps and to focus on deeper diagnosis, which may lead to confirming a defective unit and arranging a further replacement. Leaving the site without resolution or communication abandons the activity in an incomplete state, and deleting the cell's configuration would not address a suspected hardware defect and would create additional, unnecessary recovery work.

NEW QUESTION: 39

During a Site Acceptance Test (SAT) for a newly commissioned 5G site, what is the NOC team's typical role?

- A.** To physically inspect the antenna mounting hardware for structural compliance
- B.** To remotely verify that the site is visible and manageable from centralized OandM systems, that cells come into service correctly, that no unexpected alarms are present, and that initial performance indicators are within expected ranges
- C.** To negotiate the commercial contract terms for the site's construction
- D.** To install the physical RF cabling between the antenna and the baseband unit

Answer: B (LEAVE A REPLY)

During a Site Acceptance Test for a newly commissioned site, the NOC team's role centers on remote verification from the centralized operations perspective, complementing the field team's physical inspection and commissioning activities. This typically includes confirming that the new site and its cells are visible, reachable, and manageable through centralized tools such as NetAct (confirming O and M connectivity is correctly established), verifying that all expected cells come into service without configuration errors, checking that no unexpected or unresolved alarms are present that would indicate an incomplete or faulty installation, and reviewing initial performance indicators (such as successful connection attempts and basic KPI reporting) to confirm the site is functioning as intended before it is accepted into normal operation.

Physical inspections of mounting hardware, cabling installation, and commercial/contractual matters fall outside the NOC's remote operational role and are handled by field engineering, construction, and commercial teams respectively.

NEW QUESTION: 40

Over a period of several weeks, a NOC team observes that a particular cell's average PRB utilization during the busy hour has steadily increased from 60% to consistently above 85%, even though no faults or configuration issues have been identified. What is the most appropriate action based on this trend?

- A.** Ignore the trend since no active alarms are present
- B.** Immediately lock the cell to prevent further load increase
- C.** Flag the cell for capacity planning review, as the trend suggests the cell may require additional capacity to maintain performance

D. Reduce the cell's transmit power to discourage new connections

Answer: C (LEAVE A REPLY)

A steady upward trend in busy-hour PRB utilization over multiple weeks, in the absence of faults or configuration changes, is a classic indicator of organic traffic growth gradually consuming available capacity. While the cell may still be performing acceptably at 85% utilization, continuing this trend risks crossing into the congestion range (typically above 90%) where accessibility and throughput KPIs begin to degrade. The appropriate response is proactive: flagging the cell for capacity planning review allows engineers to evaluate options such as adding carriers, adjusting load balancing parameters, or planning sectorization before performance actually suffers. Ignoring the trend risks a reactive, customer-impacting outcome once congestion thresholds are crossed. Locking the cell or reducing transmit power would actively degrade service for existing users and is not an appropriate response to a capacity trend - these actions would be counterproductive and harm the very users the network is meant to serve.

NEW QUESTION: 41

Which Nokia centralized network management system is primarily used by NOC and technical support personnel to monitor, configure, and manage AirScale 5G base stations remotely from an Operations Center?

A. NetAct

B. NetGuard Security Management

C. CloudBand

D. Nokia Digital Automation Cloud

Answer: A (LEAVE A REPLY)

NetAct is Nokia's centralized Operations Support System (OSS) and is the primary platform used by NOC and technical support teams to manage AirScale 5G base stations from a centralized Operations Center. It integrates Fault Management (FM), Configuration Management (CM), Performance Management (PM), and Software Management (SWM) modules into a single environment, allowing engineers to monitor alarms, push configuration changes, review KPI dashboards, and manage software lifecycle activities across the entire RAN estate without visiting individual sites. While element-level tools such as BTS Site Manager exist for local diagnostics on a single base station, NetAct is the day-to-day platform for remote, network-wide operations. NetGuard focuses on security analytics, CloudBand on NFV infrastructure orchestration, and Nokia Digital Automation Cloud targets private wireless deployments, so none of these serve as the primary RAN operations management system referenced in remote operations procedures.

NEW QUESTION: 42

For security segmentation, NOC personnel typically do not connect directly from their workstations to production AirScale base stations. Instead, they first authenticate to an intermediate, hardened host. What is this intermediate host commonly called?

- A. Jump server / bastion host
- B. Edge router
- C. Load balancer
- D. DNS server

Answer: [\(SHOW ANSWER\)](#)

A jump server (also called a bastion host) is an intermediate, hardened system that NOC personnel must authenticate to before establishing management sessions, such as SSH or NetAct client connections, to production base stations. This design reduces the attack surface of the network because production elements only need to accept management connections originating from a small number of tightly controlled, monitored hosts, rather than from every individual engineer's workstation across potentially varied locations and security postures. Jump servers also provide a natural point for enforcing multi-factor authentication, centralized session logging, and periodic access reviews. An edge router forwards traffic between networks but is not an access-control checkpoint for engineer sessions. A load balancer distributes traffic across multiple servers for performance/availability, and a DNS server resolves hostnames to IP addresses - neither performs the security gatekeeping function described.

NEW QUESTION: 43

What is the function of cell reselection priority parameters configured for idle-mode UEs across different frequency layers (e.g., 5G vs. 4G, or different 5G bands)?

- A. They determine which UEs are allowed to register on the network at all
- B. They guide idle-mode UEs toward preferred frequency layers or cells, influencing which layer a UE camps on when multiple suitable options are available
- C. They define the maximum transmit power for each frequency layer
- D. They determine the encryption keys used for signaling on each frequency layer

Answer: [B \(LEAVE A REPLY\)](#)

Cell reselection priority parameters are broadcast to idle-mode UEs and inform them how to prioritize different frequency layers (such as a 5G band versus an LTE band, or multiple 5G bands) when more than one suitable cell is available for camping. By assigning higher reselection priority to certain layers, an operator can influence idle-mode UE distribution - for example, encouraging UEs to camp on a 5G layer where available to ensure faster initial access to 5G services, or directing UEs away from a layer that is being prepared for maintenance. These parameters work alongside reselection thresholds and timers that prevent excessive reselection (ping-ponging) between layers. They do not control network registration eligibility (which depends on subscription and PLMN matching), transmit power limits (a separate RF parameter), or encryption key management (a security function handled through different mechanisms), but they play an important role in idle-mode load distribution and user experience from the moment a device wakes up.

NEW QUESTION: 44

Why does NetAct support configuring automatic notifications, such as email or SMS, for Critical severity alarms to NOC personnel?

- A.** To eliminate the need for any live alarm monitoring dashboard
- B.** To ensure timely awareness of severe issues even when staff are not actively watching the FM dashboard, supporting faster initial response
- C.** To automatically resolve the underlying fault condition
- D.** To reduce the total number of alarms the network generates

Answer: B ([LEAVE A REPLY](#))

NetAct supports configuring automatic notifications, such as email or SMS alerts, to be sent to designated NOC personnel when alarms of a certain severity - commonly Critical - are raised. This ensures severe issues are brought to the attention of responsible engineers promptly, even if no one is actively viewing the live FM dashboard at that exact moment, helping reduce the time between a fault occurring and corrective action beginning. This notification mechanism complements, rather than replaces, the FM dashboard, which remains necessary for detailed investigation, alarm correlation across the network, and ongoing monitoring of all severity levels. It does not automatically fix any underlying fault - it is purely an awareness mechanism - and has no effect on how many alarms the network actually generates, which is determined by real fault conditions and configured alarm definitions/thresholds, not by notification settings.

NEW QUESTION: 45

What is the purpose of a NetAct configuration/network audit tool in remote operations?

- A.** To physically inspect equipment cabinets at the site
- B.** To compare deployed parameter values on live elements against a defined reference/baseline configuration and report deviations
- C.** To measure electrical power consumption at the site
- D.** To generate customer-facing marketing reports

Answer: ([SHOW ANSWER](#))

A NetAct configuration (network) audit tool compares the parameter values currently deployed on live network elements against a defined reference or baseline configuration - sometimes called a golden configuration or template - and reports any deviations or inconsistencies found. This is highly valuable for remote operations because it can detect unauthorized or accidental configuration changes, configuration drift following maintenance activities, or sites that failed to receive an intended bulk update correctly, all without requiring a physical site visit. It directly supports standard provisioning workflows by allowing engineers to confirm that planned configuration changes were applied correctly and consistently across all targeted base stations. The tool does not perform physical inspection of cabinets (a field activity), does not measure power consumption (handled by environmental/equipment monitoring functions), and is not used to produce marketing material - its scope is strictly configuration verification within the OAM domain.

NEW QUESTION: 46

A NOC engineer reviewing UE measurement reports notices that two physically adjacent 5G cells are broadcasting the identical Physical Cell Identity (PCI), causing UEs to receive ambiguous reference signals.

What is this condition called, and what is the appropriate remote corrective action?

- A.** This is PCI confusion, and it should be resolved by adjusting the cells' reference signal power
- B.** This is a PCI collision, and it should be resolved by reassigning a unique PCI value to one of the conflicting cells
- C.** This is PCI confusion, and the only remedy is to delete the neighbor relation between the two cells
- D.** This is a normal configuration and requires no action, since PCI values can be safely reused on adjacent cells

Answer: B (LEAVE A REPLY)

A PCI collision occurs when two neighboring (geographically adjacent or mutually visible) cells are configured with the same Physical Cell Identity, causing UEs to be unable to reliably distinguish between them based on their synchronization and reference signals. This leads to degraded reference signal measurements, failed handovers, and potential interference between the two cells' signals. This is distinct from PCI confusion, where two non-adjacent cells that share a PCI are both neighbors of a third common cell, creating ambiguity during handover target selection even though the two same-PCI cells are not directly adjacent. The correct remediation for a PCI collision is a PCI replanning exercise, reassigning one of the conflicting cells to a unique PCI value that avoids both direct reuse with its neighbors and problematic modulo relationships that affect reference signal sequences. This is typically performed remotely via configuration management without requiring a site visit.

Valid NRN-522 Dumps shared by Actual4test.com for Helping Passing NRN-522 Exam! Actual4test.com now offer the **newest NRN-522 exam dumps**, the Actual4test.com NRN-522 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NRN-522 dumps with Test Engine here: https://www.actual4test.com/NRN-522_examcollection.html (122 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 47

An 'Equipment Over-Temperature' alarm is raised at a remote site. Besides checking the cooling system itself, what else should a NOC engineer review related to this alarm?

- A.** The cell's configured Physical Cell Identity (PCI)

B. Whether a cabinet door-open, fan failure, or HVAC/air-conditioning fault alarm is also present, indicating a broader environmental issue

C. The handover success rate KPI

D. The NetAct software license expiry date

Answer: ([SHOW ANSWER](#))

An 'Equipment Over-Temperature' alarm indicates internal temperature monitoring has detected conditions exceeding safe operating limits, which can lead to performance throttling or automatic protective shutdown of the affected hardware. Beyond inspecting the cooling system itself, a NOC engineer should check whether related environmental alarms are also present at the site, such as a cabinet door-open alarm (which disrupts climate control), a fan failure alarm, or an HVAC/air-conditioning fault alarm for the shelter or cabinet.

These correlated alarms often explain an over-temperature condition by pointing to a broader site environmental issue rather than an isolated equipment defect, helping correctly scope the response (for example, escalating an environmental/facilities issue rather than treating it purely as a RAN equipment fault).

The cell's PCI value, handover success rate, and NetAct license expiry date are entirely unrelated to thermal conditions and would not assist in diagnosing this alarm.

NEW QUESTION: 48

After a field engineer physically replaces a Remote Electrical Tilt (RET) antenna actuator, what remote verification should the NOC engineer perform to confirm the new unit is properly integrated?

A. Confirm the new RET device is detected and communicating correctly over the AISG bus, and verify that its tilt position can be read and adjusted as expected

B. Confirm the RET unit's color matches the previous unit

C. Confirm the RET unit has the same serial number as the unit it replaced

D. Confirm the RET unit is broadcasting on the correct NR-ARFCN

Answer: **A** ([LEAVE A REPLY](#))

Remote Electrical Tilt (RET) units are Antenna Line Devices (ALDs) that communicate with the base station over the Antenna Interface Standards Group (AISG) bus. After a physical RET replacement, the appropriate remote verification is to confirm that the new device is discovered on the AISG bus, that it is communicating correctly with the base station's controller, and that its current tilt position can be read remotely and that tilt adjustment commands are correctly applied and reflected back. This confirms both the physical connectivity (cabling/bus communication) and functional operability (motor and position feedback) of the replaced unit.

The unit's color is irrelevant to functional verification, and while serial number changes are expected with replacement (a new unit will naturally have a different serial number, which should simply be recorded for inventory purposes), it is not itself a functional check. NR-

ARFCN relates to radio carrier frequency configuration and has no relationship to RET device verification.

NEW QUESTION: 49

A cell repeatedly raises and clears 'Cell Unavailable' alarms. Performance data shows PRB utilization dropping to zero during exactly the same periods. Which area should be investigated FIRST as the likely root cause?

- A.** NetAct user interface display/theme settings
- B.** Possible transport link instability, loss of synchronization reference, or unexpected hardware resets affecting the cell during those periods
- C.** The make and model of subscriber handsets in the area
- D.** The operator's billing system

Answer: B (LEAVE A REPLY)

When a cell repeatedly raises and clears 'Cell Unavailable' alarms, and PRB utilization simultaneously drops to zero during exactly those same intervals, this pattern strongly indicates the cell is genuinely going out of service intermittently, rather than a display or reporting artifact. The investigation should focus on causes capable of producing repeated, short-duration outages: transport link instability (brief link flaps causing loss of the cell's connectivity), loss of synchronization reference (particularly significant for TDD 5G, where sync loss can force a cell to stop transmitting to avoid interference), or unexpected hardware resets/restarts of the baseband or radio unit, potentially linked to environmental issues such as overheating or power fluctuations.

NetAct UI theme settings, subscriber handset models, and the billing system are entirely unrelated to RAN service availability and would not explain this correlated alarm and KPI pattern. Correlating alarm timing with PM data and environmental/transport alarms is a key NOC diagnostic technique.

NEW QUESTION: 50

A 'High VSWR' (Voltage Standing Wave Ratio) alarm is raised on an RF unit's antenna branch. What does this alarm typically indicate a problem with?

- A.** The NetAct server's storage capacity
- B.** The antenna, feeder cable, or RF connector on that branch
- C.** The core network's mobility management function
- D.** The operator's subscriber billing database

Answer: B (LEAVE A REPLY)

Voltage Standing Wave Ratio (VSWR) measures how efficiently RF energy transmitted by the radio unit is delivered into the antenna system versus being reflected back due to an impedance mismatch. A High VSWR alarm indicates a significant mismatch on a particular antenna branch or port, commonly caused by issues such as a damaged or loose feeder cable connection, a faulty or improperly seated RF connector, moisture

/water ingress into a connector, or physical damage to an antenna element. This is a radio-frequency hardware issue on the affected branch and is entirely unrelated to NetAct server storage, core network mobility functions, or billing systems. For NOC engineers, a persistent High VSWR alarm typically signals that a field visit may be needed to inspect and repair the physical RF connections or replace damaged hardware on that antenna line, since it is a physical-layer condition not resolvable through remote configuration alone.

NEW QUESTION: 51

What is the AISG bus used for in the context of antenna line device management?

- A.** It is the main fiber optic link carrying CPRI/eCPRI traffic between the baseband and RF units
- B.** It is a standardized communication interface that allows the base station to communicate with and control Antenna Line Devices such as RET units and Tower Mounted Amplifiers (TMAs)
- C.** It is the OandM IP network used to connect the site to NetAct
- D.** It is the power supply cable providing DC power to the baseband unit

Answer: B (LEAVE A REPLY)

The Antenna Interface Standards Group (AISG) bus is a standardized communication interface (typically layered over RS-485 and sometimes carried over the same coaxial feeder cable as the RF signal, using a technique that separates the control signal from the RF) that enables the base station's control unit to discover, communicate with, and control Antenna Line Devices (ALDs) mounted on or near the antenna - most commonly Remote Electrical Tilt (RET) actuators and Tower Mounted Amplifiers (TMAs). Through the AISG bus, the system can remotely query device status, read sensor data such as current tilt position, and send control commands such as tilt adjustments or TMA gain settings. This is entirely distinct from the CPRI

/eCPRI fiber links carrying baseband-to-RF digital radio signals, the O and M IP network connecting the site to centralized management systems like NetAct, or the DC power distribution supplying equipment - each of which serves a different, non-overlapping function within the site's overall infrastructure.

NEW QUESTION: 52

Within NetAct, which functional module is primarily responsible for planning, distributing, and activating software packages across base stations?

- A.** Fault Management (FM)
- B.** Performance Management (PM)
- C.** Software Management (SWM)
- D.** Configuration Management (CM)

Answer: (SHOW ANSWER)

The Software Management (SWM) module within NetAct is the centralized functional area responsible for the end-to-end software lifecycle of base stations and other network

elements, including planning software deployment campaigns, distributing (downloading) software packages to target network elements, scheduling and triggering activation, and monitoring the success or failure of these operations across potentially large numbers of sites. This is distinct from Fault Management (FM), which handles alarms and fault conditions; Performance Management (PM), which handles KPI and counter-based performance data; and Configuration Management (CM), which handles parameter and configuration provisioning. While these modules may interact - for example, a software activation might generate alarms visible in FM, or a software change might necessitate subsequent configuration adjustments via CM - the core responsibility for managing software packages, versions, and activation campaigns rests specifically with SWM, making it the primary tool a NOC engineer would use for software lifecycle activities.

NEW QUESTION: 53

A NOC engineer 'acknowledges' an active alarm in NetAct FM. What does this action signify?

- A. The underlying fault has been automatically repaired
- B. The alarm has been seen and is being handled, helping avoid duplicated investigation by other team members
- C. The affected base station will automatically reboot
- D. The alarm record is permanently deleted from the system

Answer: B (LEAVE A REPLY)

Acknowledging an alarm in NetAct FM is an administrative action that marks the alarm as having been seen and taken ownership of by an engineer, without changing the underlying fault condition itself. In a NOC environment where multiple engineers or shifts monitor shared alarm lists, acknowledgement communicates that someone is already aware of and working on the issue, helping to avoid duplicated troubleshooting effort and providing a basic accountability trail for follow-up. It does not automatically resolve or repair the underlying fault - the alarm will only clear once the actual condition causing it is resolved, whether automatically by the network recovering or through engineer intervention. Acknowledgement also does not cause the base station to reboot, and acknowledged alarms remain visible in the active list (not deleted) until the underlying condition clears, at which point they typically move to the alarm history.

NEW QUESTION: 54

What is the role of the Managed Object Model (MOM) in Nokia's RAN configuration management framework?

- A. It defines the physical cabling diagram for a base station site
- B. It defines the structured hierarchy of configurable objects (such as network elements, cells, and their parameters) that configuration management tools operate on
- C. It is a list of all active and historical alarms for a network element
- D. It is the software package used to upgrade base station firmware

Answer: B (LEAVE A REPLY)

The Managed Object Model (MOM) defines the structured, hierarchical representation of all configurable entities within the network - such as network elements, their subordinate functional units, cells, and the individual parameters associated with each object - along with the relationships between them. Configuration management tools, including NetAct CM applications, rely on the MOM to know what objects exist, what parameters each object type supports, valid value ranges, and how objects relate to one another (for example, a cell object existing as a child of a baseband equipment object). Understanding the MOM is important for NOC engineers performing configuration changes, since it determines where a given parameter resides within the object hierarchy and what other objects or parameters might be affected by a change. The MOM is a configuration management construct and is unrelated to physical cabling documentation, alarm history (a fault management function), or software upgrade packages (a software lifecycle management function).

NEW QUESTION: 55

What is the primary function of the AirScale System Module within an AirScale Base Transceiver Station (BTS)?

- A.** RF amplification and antenna interfacing
- B.** Baseband processing, control-plane functions, and OandM connectivity, supporting multiple radio technologies under Single RAN
- C.** Providing power supply for the macro cabinet only
- D.** Generating the GPS satellite timing signal

Answer: B (LEAVE A REPLY)

The AirScale System Module is the central baseband processing unit of the AirScale BTS. It hosts digital baseband processing for the deployed radio technologies, handles control-plane functions, and provides the O and M interface that NetAct and remote engineers use for configuration, fault, and performance management.

Under Nokia's Single RAN architecture, the same System Module hardware can support 2G, 3G, 4G, and 5G concurrently, with the active technology mix determined by software and licensing rather than separate dedicated hardware. RF amplification and the physical antenna interface are performed by separate AirScale Radio (RF) modules, not the System Module. The System Module is not a power supply for the cabinet, and while it receives external timing/synchronization references such as GNSS for network synchronization, it does not itself generate GPS satellite signals.

NEW QUESTION: 56

How is the Cell Availability KPI typically calculated for a reporting period, and what does this KPI primarily reflect?

- A.** (Total successful handovers / total handover attempts) x 100 - reflects mobility performance

- B.** $(\text{Total time the cell was in service} / \text{total time in the period}) \times 100$ - reflects how much of the period the cell was able to carry traffic
- C.** $(\text{Total downlink throughput} / \text{total uplink throughput}) \times 100$ - reflects traffic balance
- D.** $(\text{Total active alarms} / \text{total cleared alarms}) \times 100$ - reflects fault management efficiency

Answer: (SHOW ANSWER)

Cell Availability is an Availability-category KPI that measures the proportion of a given reporting period during which a cell was operationally able to carry traffic - that is, unlocked, in service, and not blocked by a fault. It is calculated as the ratio of the time the cell was actually available to the total duration of the reporting period, expressed as a percentage. Periods of planned maintenance (administrative locking) are sometimes excluded or tracked separately from unplanned outages, depending on operator reporting policy, since the two have different operational implications. This KPI is critical for service level agreement (SLA) reporting and for identifying cells with recurring stability issues such as repeated automatic resets, hardware faults, or transport outages. It is distinct from throughput-based, handover-based, or alarm-count-based ratios, which belong to other KPI categories and answer different operational questions.

Valid NRN-522 Dumps shared by Actual4test.com for Helping Passing NRN-522 Exam! Actual4test.com now offer the **newest NRN-522 exam dumps**, the Actual4test.com NRN-522 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com NRN-522 dumps with Test Engine here: https://www.actual4test.com/NRN-522_examcollection.html (122 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)