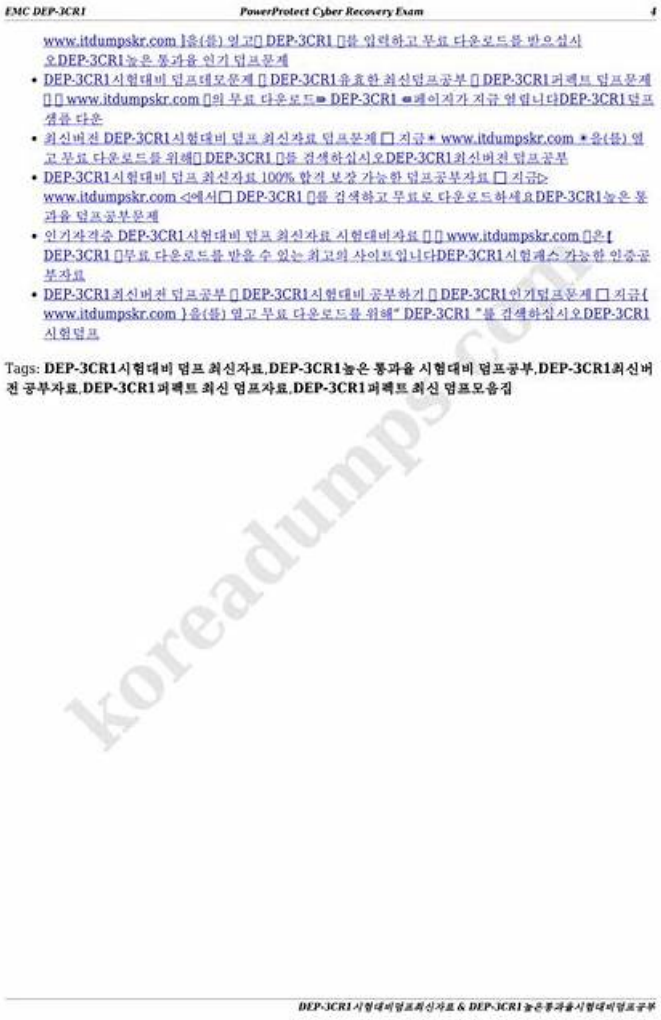
350-101시험대비덤프공부자료, 350-101최고품질인증시험기출자료


EMC DEP-3CR1 PowerProtect Cyber Recovery Exam 4

www.itdumpskr.com }을(를) 엽고□ DEP-3CR1 □를 입력하고 무료 다운로드를 받으십시오DEP-3CR1높은 통과율 인기 덤프문제

- DEP-3CR1시험대비 덤프데모문제 □ DEP-3CR1유효한 최신덤프공부 □ DEP-3CR1퍼펙트 덤프문제 □□ www.itdumpskr.com □의 무료 다운로드▶ DEP-3CR1 ◀페이지가 지금 열립니다DEP-3CR1덤프샘플 다운
- 최신버전 DEP-3CR1시험대비 덤프 최신자료 덤프문제 □ 지금 * www.itdumpskr.com *을(를) 엽고 무료 다운로드를 위해□ DEP-3CR1 □를 검색하십시오DEP-3CR1최신버전 덤프공부
- DEP-3CR1시험대비 덤프 최신자료 100% 합격 보장 가능한 덤프공부자료 □ 지금▷ www.itdumpskr.com ◁에서□ DEP-3CR1 □를 검색하고 무료로 다운로드하세요DEP-3CR1높은 통과율 덤프공부문제
- 인기자격증 DEP-3CR1시험대비 덤프 최신자료 시험대비자료 □□ www.itdumpskr.com □은[DEP-3CR1 □무료 다운로드를 받을 수 있는 최고의 사이트입니다DEP-3CR1시험패스 가능한 인증공부자료
- DEP-3CR1최신버전 덤프공부 □ DEP-3CR1시험대비 공부하기 □ DEP-3CR1인기덤프문제 □ 지금{ www.itdumpskr.com }을(를) 엽고 무료 다운로드를 위해" DEP-3CR1 "를 검색하십시오DEP-3CR1시험덤프

Tags: DEP-3CR1시험대비 덤프 최신자료,DEP-3CR1높은 통과율 시험대비 덤프공부,DEP-3CR1최신버전 공부자료,DEP-3CR1퍼펙트 최신 덤프자료,DEP-3CR1퍼펙트 최신 덤프모음집

DEP-3CR1시험대비덤프최신자료 & DEP-3CR1높은통과율시험대비덤프공부

KoreaDumps는 여러분이 빠른 시일 내에Cisco 350-101인증시험을 효과적으로 터득할 수 있는 사이트입니다.Cisco 350-101인증 자격증은 일상생활에 많은 개변을 가져올 수 있는 시험입니다.Cisco 350-101인증 자격증을 소지한 자들은 당연히 없는 자들보다 연봉이 더 높을 거고 승진기회도 많아지며 IT업계에서의 발전도 무궁무진합니다.

Cisco 350-101인증시험을 패스하려면 시험대비자료선택은 필수입니다. 우리KoreaDumps에서는 빠른 시일 내에 Cisco 350-101관련 자료를 제공할 수 있습니다. KoreaDumps의 전문가들은 모두 경험도 많고, 그들이 연구자료는 실제시험의 문제와 답과 거이 일치합니다. KoreaDumps 는 인증시험에 참가하는 분들한테 편리를 제공하는 사이트이며,여러분들이 시험패스에 도움을 줄 수 있는 사이트입니다.

>> 350-101시험대비 덤프공부자료 <<

350-101최고품질 인증시험 기출자료 - 350-101시험패스 가능 덤프자료

Cisco 350-101인증시험은 현재IT인사들 중 아주 인기 잇는 인증시험입니다.Cisco 350-101시험패스는 여러분의 하시는 일과 생활에서 많은 도움을 줄뿐만 아니라 중요한 건 여러분의IT업계에서의 자기만의 자리를 지키실 수 잇습니다.이렇게 좋은 시험이니 많은 분들이 응시하려고 합니다,하지만 패스 율은 아주 낮습니다.

Cisco 350-101 시험요강:

주제	소개
주제 1	• Wireless Network Implementation: Covers Cisco wireless deployment architectures (Fabric, Mesh, Local, Cloud), physical infrastructure setup, and configuring management access for APs, WLCs, and dashboards.
주제 2	• Automation and AI: Covers Python scripting basics, NETCONF • YANG, wireless API interpretation, and AI-driven analytics, operations, and radio resource management within Catalyst Center.
주제 3	• RF Fundamentals: Covers the behavior of radio waves, how RF signals are measured and interpreted, the mathematics behind RF calculations, and the characteristics of Wi-Fi antennas.
주제 4	• Wireless Monitoring and Management: Covers network maintenance tasks, client monitoring configuration, troubleshooting client connectivity issues, and integrating with external devices and platforms.
주제 5	• Client Connectivity Configuration: Covers configuring authentication both on and off the controller, setting up client connectivity across different operating systems, roaming behavior, and wireless guest network configuration.

최신 CCIE Wireless 350-101 무료샘플문제 (Q14-Q19):

질문 # 14
A business is deploying Cisco Catalyst 9100 APs managed by Catalyst 9800 WLCs. The IT team needs policies that adapt based on user identity and device posture and also provide visibility into device activity and location. Which configuration meets these requirements?

- A. Integrate Cisco ISE for identity-based policies and omit mobile device management and location services.
- B. Configure Cisco Catalyst Center assurance for visibility and apply static per-service set identifier virtual LAN assignments without Cisco ISE integration.
- C. Integrate Cisco Catalyst Center with Cisco ISE for policy control, add mobile device management for posture checks, and use Cisco Spaces for location visibility.
- D. Use Cisco Catalyst 9800 ACLs combined with mobile device management integration without Catalyst Center or Catalyst Spaces.

정답：C

설명:
To enforce adaptive policies based on user identity, device posture, and provide comprehensive visibility into device activity and location, Cisco recommends integrating Cisco Catalyst Center, Cisco ISE, and Cisco Spaces. Cisco ISE provides identity-based access control and posture assessment, allowing dynamic policy enforcement for users and devices. Mobile device management integration further extends posture checks for endpoint compliance. Cisco Catalyst Center enables real-time assurance and monitoring of network performance, device activity, and service health, while Cisco Spaces provides location analytics and visibility of client devices across the wireless environment. Option B relies solely on ACLs and MDM, which cannot provide full network-wide visibility or context-aware policy enforcement. Option C enables visibility via Catalyst Center but lacks dynamic identity and posture-based policies because it omits ISE integration. Option D integrates ISE but neglects device posture and location visibility, failing to meet all requirements. The combination in Option A ensures that adaptive policies can respond to real-time user and device conditions, enforce compliance, and provide actionable insights for network operations. Reference topics:Wireless Monitoring and Management - Catalyst Center assurance, Cisco ISE integration, mobile device posture, Cisco Spaces location analytics.

질문 # 15
What is a feature of an RTS frame in the context of 802.11 frame types?

- A. It applies spectral mask for transmission.
- B. It provides navigation updates for roaming clients.
- C. It compresses frames for bandwidth savings.
- D. It requests permission to send data on a channel.

정답：D

설명：
An RTS frame is an 802.11control frameused in the Request to Send/Clear to Send exchange. Cisco identifies RTS as a Request to Send frame and explains that 802.11 control frames assist in delivering data frames between stations. Cisco further states that the RTS/CTS function is optional, helps reduce collisions when hidden stations are associated to the same access point, and that a station sends an RTS frame as the first phase before transmitting a data frame.
Therefore, option B is correct because the RTS frame requests access to the wireless medium before data transmission. If the receiving station or AP replies with CTS, nearby stations defer transmission based on the duration information, reducing collision probability. This is especially relevant in hidden-node environments where two clients can hear the AP but cannot hear each other. Option A refers to RF spectral-mask compliance, which is a physical-layer regulatory concept. Option C confuses NAV behavior with roaming; RTS/CTS may influence virtual carrier sensing, not client roaming updates. Option D is unrelated because frame compression is not an RTS function. Reference topics:802.11 frame types, control frames, RTS/CTS, CSMA/CA, hidden-node mitigation, and medium reservation.

질문 # 16

```
configure terminal
hostname 9800-L
ip domain name yourdomain.com
crypto key generate rsa
Choose the size of the key modulus in the range of 512 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [1024]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

aaa new-model
aaa authentication login default local
username admin priv 15 password YourPassword
```


Refer to the exhibit. An engineer is preparing a Cisco 9800-L WLC for deployment in a sensitive area. Only encrypted remote management via SSH is allowed, and all other VTY access methods must be disabled. The
9800-L WLC will be part of a larger deployment, and an external audit will check for any unencrypted management protocols. According to the requirements, only SSH is allowed for remote CLI sessions. Which set of commands must be executed to complete the Cisco IOS XE CLI configuration on the WLC?

- A. line vty 0 97transport input sshlogin authentication defaultexit
- B. line vty 0 97transport sshlogin authentication default
- C. line vty 0 97no transport input telnetlogin authentication default
- D. line vty disable 0 97transport preferred sshlogin authentication defaultexit

정답：A

설명：
The correct configuration is option C because Cisco IOS XE restricts inbound protocols on VTY lines with thetransport inputcommand. Cisco's Catalyst 9800 best-practice guidance states that administrators should confirm SSH is enabled and Telnet is disabled for better controller security, and that the Catalyst 9800 follows standard Cisco IOS XE behavior for enabling or disabling Telnet and SSH. Cisco IOS XE SSH documentation explicitly showsline vty line_number [ending_line_number]followed bytransport input ssh, and explains that this prevents non-SSH Telnet connections, limiting access to SSH only.
The existing exhibit already includes the SSH prerequisites: hostname, domain name, RSA key generation, AAA new-model, a default login method using local credentials, and a local privileged user. The missing VTY configuration must therefore apply that default AAA login list to the VTY lines withlogin authentication defaultand restrict inbound transport to SSH. Cisco AAA documentation confirms thatlogin authentication defaultapplies the configured default authentication list to the line or set of lines. Option A is incomplete and does not explicitly permit SSH. Option B uses invalid syntax. Option D omits the requiredinputkeyword. Reference topics:Catalyst 9800 secure management, VTY access control, SSH, Telnet hardening, AAA login authentication, and

IOS XE device administration.

질문 # 17
Exhibit:

Refer to the exhibit. An organization wants to use Cisco Spaces for location analytics, and an engineer is setting up the Cisco Catalyst 9800 WLC to send location data. The Spaces connector has already been configured and is operational on the WLC. The engineer must now configure the controller to forward telemetry data to the correct Spaces cloud endpoint using TLS to complete the integration. Which CLI command must be added to the box in the code?

- A. profile spaces-profile ip address 198.51.100.10 receiver tls-native
- B. receiver protocol tls-native profile spaces-profile ip address 198.51.100.10 57555
- C. receiver ip address 198.51.100.10 57555 protocol tls-native profile spaces-profile
- D. profile spaces-profile receiver 198.51.100.10 57555 protocol tls-native

정답： C

설명：
The correct command isreceiver ip address 198.51.100.10 57555 protocol tls-native profile spaces- profilebecause it matches the Cisco IOS XE model-driven telemetry subscription syntax used on Catalyst
9800 controllers. Cisco documents the receiver statement under telemetry ietf subscription as receiver ip address ip-address receiver-port protocol protocol profile name, and describes it as the command that configures the receiver IP address, port, protocol, and profile for telemetry notifications.
In the exhibit, the subscription already defines the telemetry feed: encode-tdl encoding, a native stream, the TDL URI for ewlc/wlan_config, the WLC source address, and an on-change update policy. What is missing is the collector destination. For Cisco Spaces or Catalyst Center-style integrations, the WLC must know where to export telemetry and which secure transport profile to use. Cisco troubleshooting examples for Catalyst
9800 telemetry use the same command structure: receiver ip address X.X.X.X 25103 protocol tls-native profile ... under the telemetry subscription.
Options A, B, and D are invalid because they reorder the CLI keywords. IOS XE telemetry configuration is parser-order sensitive: the command begins with receiver ip address, followed by the receiver port, then protocol, then profile. Reference topic:Wireless Monitoring and Management - Catalyst 9800 streaming telemetry, Cisco Spaces integration, TLS transport, and telemetry receiver configuration.

질문 # 18
Which process is managed by Ministry of Internal Affairs and Communications in Japan?

- A. RF technical standards
- B. customer onboarding documentation
- C. manufacturing batch inspection
- D. supplier chain evaluation

정답： A

설명：
The correct answer isRF technical standards. In Japan, wireless LAN and other radio equipment must operate under national RF regulatory requirements controlled by the Ministry of Internal Affairs and Communications, commonly referenced as MIC. TELEC, a registered certification body in Japan, states that specified radio equipment such as wireless LAN equipment used in Japan must conform to technical regulations regulated by MIC, and that radio equipment conformity certification validates conformance to the technical standards under Japan's Radio Act.
This aligns directly with Cisco wireless regulatory-domain behavior. Cisco's Catalyst 9800 country-code documentation explains

that APs use legal frequencies approved for their regulatory domain, and for Japan regulatory-domain devices, Japan country codes must be configured so the controller and APs operate within permitted channel and power constraints. Cisco also states that country codes are assigned and verified on APs or wireless controllers to ensure regulatory compliance for wireless operation. Manufacturing batch inspection, customer onboarding, and supplier-chain evaluation are not RF spectrum regulatory functions. Reference topics:RF Fundamentals - regulatory domains, country codes, channel legality, transmit-power limits, and wireless compliance.

질문 # 19

.....