# 350-701최신업데이트시험덤프 & 350-701합격보장가능시험



그리고 Fast2test 350-701 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=1tNv0KUkxHbPMOjNy0wosa4Ld4a20JRZu

Fast2test의 Cisco 350-701덤프로Cisco 350-701시험준비를 하면 시험패스는 간단한 일이라는걸 알게 될것입니다. Cisco 350-701덤프는 최근Cisco 350-701시험의 기출문제모음으로 되어있기에 적중율이 높습니다.시험에서 떨어지면 덤프비용 전액 환불해드리기에 우려없이 덤프를 주문하셔도 됩니다.

시스코 350-701 자격증 시험은 네트워크 보안 전문가로서 자신의 전문성을 입증하고자 하는 IT 전문가들에게 중요한 자격증입니다. 이 자격증은 전 세계에서 인정되며, IT 산업에서 높은 존경을 받습니다. 자격증 시험의 준비는 네트워크 보안 기술을 구현하고 관리하는 데 광범위한 연구 및 실무 경험이 필요합니다. 자격증 소지자는 조직의 네트워크를 안전하게 보호하고 위협과 공격으로부터 방어하는 데 필요한 기술과 지식을 갖추고 있습니다.

Cisco 350-701 인증 시험은 사이버 보안 분야에서 지식과 기술을 향상시키려는 IT 전문가를 위한 것입니다. 이 인증 시험은 사이버 보안 분야에 대한 전문 지식을 검증하고 전문 개발에 대한 귀하의 헌신을 보여주는 훌륭한 방법입니다. 인증은 전 세계적으로 인정되며 업계의 IT 전문가가 많이 인기를 얻고 있습니다.

**>> 350-701최신 업데이트 시험덤프 <<**

## 350-701합격보장 가능 시험, 350-701최신 시험대비자료

Cisco 350-701시험패스는 어려운 일이 아닙니다. Fast2test의 Cisco 350-701 덤프로 시험을 쉽게 패스한 분이 헤아릴 수 없을 만큼 많습니다. Cisco 350-701덤프의 데모를 다운받아 보시면 구매결정이 훨씬 쉬워질것입니다. 하루 빨리 덤프를 받아서 시험패스하고 자격증 따보세요.

## 최신 CCNP Security 350-701 무료샘플문제 (Q299-Q304):

**질문 # 299**
Drag and drop the solutions from the left onto the solution's benefits on the right.

정답：

설명：

질문 # 300
An engineer is trying to decide whether to use Cisco Umbrella, Cisco CloudLock, Cisco Stealthwatch, or Cisco AppDynamics Cloud Monitoring for visibility into data transfers as well as protection against data exfiltration Which solution best meets these requirements?

- A. Cisco Stealthwatch
- B. Cisco AppDynamics Cloud Monitoring
- C. Cisco Umbrella
- D. Cisco CloudLock

정답： **D**

설명：
Cisco CloudLock is a cloud-native cloud access security broker (CASB) that helps you move to the cloud safely. It protects your cloud users, data, and apps. CloudLock's simple, open, and automated approach uses APIs to manage the risks in your cloud app ecosystem. With CloudLock you can more easily combat data breaches while meeting compliance regulations1.
Cisco CloudLock provides the following features that meet the requirements of visibility into data transfers as well as protection against data exfiltration:
* User security: Cloudlock uses advanced machine learning algorithms to detect anomalies based on multiple factors. It also identifies activities outside allowed countries and spots actions that seem to take place at impossible speeds across distances1.
* Data security: Cloudlock's data loss prevention (DLP) technology continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies as well as highly tunable custom policies. It also supports inline and out-of-band data inspection and blocking capabilities to protect sensitive data12.
* App security: The Cloudlock Apps Firewall discovers and controls cloud apps connected to your corporate environment. You can see a crowd-sourced Community Trust Rating for individual apps, and you can ban or allowlist them based on risk1.
The other solutions do not provide the same level of visibility and protection as Cisco CloudLock:
* Cisco Umbrella is a cloud-delivered network security service that provides DNS-layer security, secure web gateway, cloud-delivered firewall, cloud access security broker, and threat intelligence3. It does not offer data security features such as DLP, data inspection, and data blocking4.
* Cisco AppDynamics Cloud Monitoring is a cloud-native application performance management solution that helps you monitor, troubleshoot, and optimize your cloud applications. It does not offer user security, data security, or app security features as a CASB solution.
* Cisco Stealthwatch is a network traffic analysis solution that provides visibility and threat detection across your network, endpoints, and cloud. It does not offer data security features such as DLP, data inspection, and data blocking.
3: Cisco Umbrella Packages - Cisco Umbrella 1: Cisco Cloudlock - Cisco 2: Cisco Cloudlock Cisco Cloudlock: Secure Cloud Data 4: Easy to Deploy & Simple to Manage CASB Solution - Cisco Umbrella :
Cisco AppDynamics Cloud Monitoring : Cisco Stealthwatch - Cisco

질문 # 301
Drag and drop the capabilities of Cisco Firepower versus Cisco AMP from the left into the appropriate category on the right.

정답：

설명：

질문 # 302
DRAG DROP
Drag and drop the Firepower Next Generation Intrusion Prevention System detectors from the left onto the correct definitions on the right.
Select and Place:

정답：

## 질문 # 303

Which two activities can be done using Cisco DNA Center? (Choose two)

- A. DHCP
- B. DNS
- C. Design
- D. Provision
- E. Accounting

## 정답：C,D

설명：

Explanation Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html Cisco DNA Center has four general sections aligned to IT workflows:

Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site.

Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need.

Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task.

The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups.

Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous

streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work.

The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Explanation Cisco DNA Center has four general sections aligned to IT workflows: Design: Design your network for consistent configurations by device and by site. Physical maps and logical topologies help provide quick visual reference. The direct import feature brings in existing maps, images, and topologies directly from Cisco Prime Infrastructure and the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM), making upgrades easy and quick. Device configurations by site can be consolidated in a "golden image" that can be used to automatically provision new network devices. These new devices can either be pre-staged by associating the device details and mapping to a site. Or they can be claimed upon connection and mapped to the site. Policy: Translate business intent into network policies and apply those policies, such as access control, traffic routing, and quality of service, consistently over the entire wired and wireless infrastructure. Policy-based access control and network segmentation is a critical function of the Cisco Software-Defined Access (SDAccess) solution built from Cisco DNA Center and Cisco Identity Services Engine (ISE). Cisco AI Network Analytics and Cisco Group-Based Policy Analytics running in the Cisco DNA Center identify endpoints, group similar endpoints, and determine group communication behavior. Cisco DNA Center then facilitates creating policies that determine the form of communication allowed between and within members of each group. ISE then activates the underlying infrastructure and segments the network creating a virtual overlay to follow these policies consistently. Such segmenting implements zero-trust security in the workplace, reduces risk, contains threats, and helps verify regulatory compliance by giving endpoints just the right level of access they need. Provision: Once you have created policies in Cisco DNA Center, provisioning is a simple drag-and-drop task. The profiles (called scalable group tags or "SGTs") in the Cisco DNA Center inventory list are assigned a policy, and this policy will always follow the identity. The process is completely automated and zero-touch. New devices added to the network are assigned to an SGT based on identity-greatly facilitating remote office setups. Assurance: Cisco DNA Assurance, using AI/ML, enables every point on the network to become a sensor, sending continuous streaming telemetry on application performance and user connectivity in real time. The clean and simple dashboard shows detailed network health and flags issues. Then, guided remediation automates resolution to keep your network performing at its optimal with less mundane troubleshooting work. The outcome is a consistent experience and proactive optimization of your network, with less time spent on troubleshooting tasks. Reference: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/dna-center/nb-06-dna-center-so-cte-en.html


## 질문 # 304

......

2026 Fast2test 최신 350-701 PDF 버전 시험 문제집과 350-701 시험 문제 및 답변 무료 공유:
https://drive.google.com/open?id=1tNv0KUkxHbPMOjNy0wosa4Ld4a20JRZu