Valid Exam 350-701 Blueprint & New Soft 350-701 Simulations

2025 Latest TestSimulate 350-701 PDF Dumps and 350-701 Exam Engine Free Share: https://drive.google.com/open?id=1UB5yz-8VmPFpcctSV7z_6o952mwdPGB-

We are always on the way to be better for we can't be satisfied to be the best on the 350-701 exam questions. We are trying to apply the most latest technologies to the compiling and designing on the 350-701 learning guide. With these innovative content and displays, our company is justified in claiming for offering unique and unmatched 350-701 Study Material to certifications candidates. And you won't regret for your choice if you buy our 350-701 practice engine.

Cisco 350-701 SCOR: Job Roles and Salaries

When you complete the Cisco 350-701 exam and get the CCIE Security or CCNP Security certifications, you will be positioned to benefit from vast employment opportunities that are available worldwide. Some of the job roles you can apply for with these certificates include:

- Security Engineer
- Systems Engineer
- Network Administrator
- Network Engineer
- Network Designer

With any of these certifications, you will also be able to get decent pay. For instance, according to PayScale, the average salary that a certified individual with CCIE Security can earn is $126,896 per year, while the average remuneration of the CCNP Security certificate holder amounts to $112,674 per annum.

>> Valid Exam 350-701 Blueprint <<

Valid Exam 350-701 Blueprint & Free PDF Quiz Cisco Realistic New Soft Implementing and Operating Cisco Security Core Technologies Simulations

We consider the actual situation of the test-takers and provide them with high-quality 350-701 learning materials at a reasonable price. Choose the 350-701 test guide absolutely excellent quality and reasonable price, because the more times the user buys the 350-701 test guide, the more discounts he gets. In order to make the user's whole experience smoother, we also provide a thoughtful package of services. Once users have any problems related to the 350-701 learning questions, our staff will help solve them as soon as possible.

Cisco Implementing and Operating Cisco Security Core Technologies Sample Questions (Q308-Q313):

NEW QUESTION # 308

A network engineer must configure a Cisco ESA to prompt users to enter two forms of information before gaining access The Cisco ESA must also join a cluster machine using preshared keys What must be configured to meet these requirements?

- A. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA CLI
- B. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA CLI.
- C. Enable two-factor authentication through a RADIUS server and then join the cluster by using the Cisco ESA GUI
- D. Enable two-factor authentication through a TACACS+ server and then join the cluster by using the Cisco ESA GUI.

Answer: B

Explanation:
Two-factor authentication is a security feature that requires users to provide two forms of information before gaining access to the Cisco ESA. The two factors are usually something the user knows, such as a password, and something the user has, such as a token or a code. Two-factor authentication can be enabled for specific user roles on the Cisco ESA through a RADIUS server, which is an external authentication server that supports the Remote Authentication Dial-In User Service (RADIUS) protocol. The RADIUS server can generate and validate the second factor for the users, such as a one-time password (OTP) or a time-based one- time password (TOTP). To enable two-factor authentication through a RADIUS server, the network engineer must configure the RADIUS server settings on the Cisco ESA, and assign the user roles that require two- factor authentication to use the RADIUS server as the authentication source. This can be done on the System Administration > Users page in the web interface, or by using the userconfig command in the CLI12.
A cluster is a group of Cisco ESAs that share the same configuration information and can be managed centrally. A cluster can provide increased reliability, flexibility, and scalability for the email security system.
To join a cluster, a Cisco ESA must have the same AsyncOS version as the other cluster members, and must use a pre-shared key to authenticate with the cluster leader. The pre-shared key is a secret passphrase that is configured on the cluster leader and must be entered on the joining appliance. To join a cluster by using the Cisco ESA CLI, the network engineer must use the clusterconfig command, which allows the engineer to create a new cluster, join an existing cluster, or leave a cluster. The clusterconfig command also allows the engineer to specify the communication port and the hostname or IP address of the cluster leader. If the Cisco ESA has enabled two-factor authentication, the network engineer must also use the clusterconfig > prepjoin command to configure the pre-shared key before joining the cluster34.
Therefore, option A is the correct answer, and the other options are incorrect. Option B is incorrect because the cluster configuration options must be done via the CLI on the Cisco ESA and cannot be created or joined in the GUI. Option C is incorrect because the Cisco ESA does not support TACACS+ as an external authentication source, only LDAP and RADIUS. Option D is incorrect because it also uses TACACS+, which is not supported by the Cisco ESA. References :=
* User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) - Distributing Administrative Tasks
* User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) - External Authentication
* Configure an Email Security Appliance (ESA) Cluster
* User Guide for AsyncOS 14.0 for Cisco Secure Email Gateway - GD (General Deployment) - Centralized Management

NEW QUESTION # 309
Refer to the exhibit.

What does the number 15 represent in this configuration?

- A. access list that identifies the SNMP devices that can access the router
- B. number of possible failed attempts until the SNMPv3 user is locked out
- C. interval in seconds between SNMPv3 authentication attempts
- D. privilege level for an authorized user to this router

Answer: A

Explanation:
The syntax of this command is shown below:
snmp-server group [group-name {v1 | v2c | v3 [auth | noauth | priv]}] [read read-view] [write write-view] [notify notify-view] [access access-list] The command above restricts which IP source addresses are allowed to access SNMP functions on the router. You could restrict SNMP access by simply applying an interface ACL to block incoming SNMP packets that don't come from trusted servers. However, this would not be as effective as using the global SNMP commands shown in this recipe. Because you can apply this method once for the whole router, it is much simpler than applying ACLs to block SNMP on all interfaces separately. Also, using interface ACLs would block not only SNMP packets intended for this router, but also may stop SNMP packets that just happened to be passing through on their way to some other destination device.

NEW QUESTION # 310
Based on the NIST 800-145 guide, which cloud architecture may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises?

- A. hybrid cloud
- B. community cloud
- C. private cloud
- D. public cloud

Answer: B

Explanation:
According to the NIST 800-145 guide1, a community cloud is a cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. A community cloud is different from a hybrid cloud, which is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). A private cloud is a cloud infrastructure that is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. A public cloud is a cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. References := Some possible references are:
1: NIST SP 800-145, The NIST Definition of Cloud Computing, 1 2: Evaluation of Cloud Computing Services Based on NIST SP 800-145, 3 3: What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, 6

NEW QUESTION # 311
What are two rootkit types? (Choose two)

- A. user mode
- B. buffer mode
- C. virtual
- D. registry
- E. bootloader

Answer: B,E

NEW QUESTION # 312
Using Cisco Cognitive Threat Analytics, which platform automatically blocks risky sites, and test unknown sites for hidden advanced threats before allowing users to click them?

- A. Cisco Enterprise Security Appliance (ESA)
- B. Cisco Advanced Stealthwatch Appliance (ASA)
- C. Cisco Identity Services Engine (ISE)
- D. Cisco Web Security Appliance (WSA)

Answer: D

Explanation:
Cisco Web Security Appliance (WSA) is the platform that automatically blocks risky sites, and tests unknown sites for hidden advanced threats before allowing users to click them, using Cisco Cognitive Threat Analytics.
Cisco Cognitive Threat Analytics is a cloud-based solution that reduces the time to discovery of threats operating inside the network by analyzing web traffic and detecting anomalous behavior. Cisco WSA integrates with Cisco Cognitive Threat Analytics to provide enhanced web security and breach detection.
Cisco WSA can also leverage other Cisco security solutions, such as Cisco Umbrella, Cisco Advanced Malware Protection (AMP), and Cisco Talos Intelligence Group, to provide comprehensive web security. References:
* Cisco Web Security Appliance (WSA)

* Cisco Cognitive Threat Analytics At-a-Glance
* Introducing Cisco Cognitive Threat Analytics
* Implementing and Operating Cisco Security Core Technologies (SCOR) - Module 3: Cloud and Content Security

NEW QUESTION # 313
.....

After so many years' development, our 350-701 exam torrent is absolutely the most excellent than other competitors, the content of it is more complete, the language of it is more simply. Once you use our 350-701 latest dumps, you will save a lot of time. High effectiveness is our great advantage. After twenty to thirty hours' practice, you are ready to take the real 350-701 Exam Torrent. The results will never let you down. You just need to wait for obtaining the certificate.