

NSE8_812 Exam Collection | Reliable NSE8_812 Exam Question



BONUS!!! Download part of DumpStillValid NSE8_812 dumps for free: <https://drive.google.com/open?id=1FFDs8nZRnV6guHivB7DF9uiZbFy3lq3B>

The NSE8_812 study material provided by DumpStillValid can make you enjoy a boost up in your career and help you get the NSE8_812 certification easily. The 99% pass rate can ensure you get high scores in the actual test. In order to benefit more candidates, we often give some promotion about our NSE8_812 Pdf Files. You will get the most valid and best useful NSE8_812 study material with a reasonable price. Besides, you will enjoy the money refund policy in case of failure.

Fortinet NSE8_812 certification exam is a written exam that is designed to validate the skills and knowledge of network security professionals who work with Fortinet products and solutions. NSE8_812 exam is intended for those who have a strong understanding of network security concepts and who have experience with Fortinet solutions. Passing NSE8_812 Exam is an important milestone for those who want to demonstrate their expertise in network security and to advance their careers in this field.

>> NSE8_812 Exam Collection <<

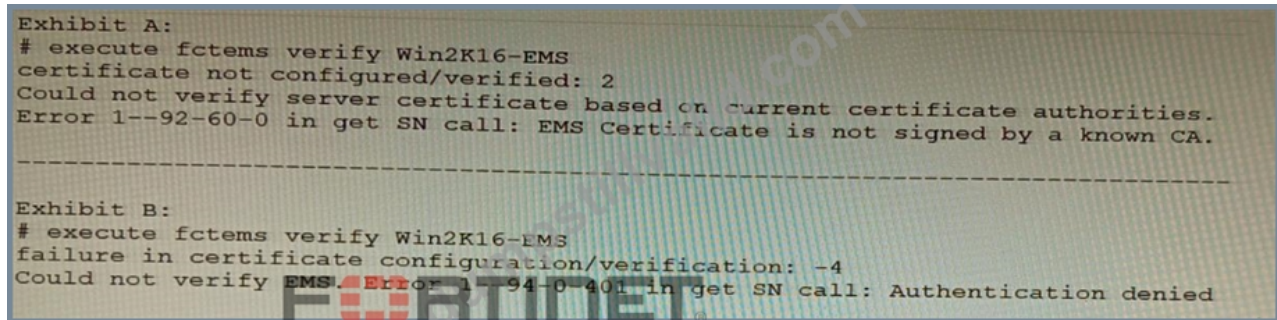
Reliable NSE8_812 Exam Question | NSE8_812 Detailed Study Plan

Our NSE8_812 study materials' developers to stand in the perspective of candidate, fully consider their material basis and actual levels of knowledge, formulated a series of scientific and reasonable learning mode, meet the conditions for each user to tailor their learning materials. What's more, our NSE8_812 Study Materials are cheap and cheap, and we buy more and deliver more. The more customers we buy, the bigger the discount will be. In order to make the user a better experience to the superiority of our NSE8_812 study materials.

Fortinet NSE 8 - Written Exam (NSE8_812) Sample Questions (Q31-Q36):

NEW QUESTION # 31

Refer to the exhibit.



```
Exhibit A:
# execute fctems verify Win2K16-EMS
certificate not configured/verified: 2
Could not verify server certificate based on current certificate authorities.
Error 1--92-60-0 in get SN call: EMS Certificate is not signed by a known CA.

-----

Exhibit B:
# execute fctems verify Win2K16-EMS
failure in certificate configuration/verification: -4
Could not verify EMS. Error 1--94-0-401 in get SN call: Authentication denied
```

The exhibit shows two error messages from a FortiGate root Security Fabric device when you try to configure a new connection to a FortiClient EMS Server.

Referring to the exhibit, which two actions will fix these errors? (Choose two.)

- A. Authorize the root FortiGate on the FortiClient EMS
- B. Verify that the CRL is accessible from the root FortiGate
- C. Install a new known CA on the Win2K16-EMS server.
- D. Export and import the FortiClient EMS server certificate to the root FortiGate.

Answer: A,B

Explanation:

A is correct because the error message "The CRL is not accessible" indicates that the root FortiGate cannot access the CRL for the FortiClient EMS server. Verifying that the CRL is accessible will fix this error.

D is correct because the error message "The FortiClient EMS server is not authorized" indicates that the root FortiGate is not authorized to connect to the FortiClient EMS server. Authorizing the root FortiGate on the FortiClient EMS server will fix this error. The other options are incorrect. Option B is incorrect because exporting and importing the FortiClient EMS server certificate to the root FortiGate will not fix the CRL error. Option C is incorrect because installing a new known CA on the Win2K16-EMS server will not fix the authorization error.

References:

Troubleshooting FortiClient EMS connectivity | FortiClient / FortiOS 7.0.0 - Fortinet Document Library
Authorizing FortiGates with FortiClient EMS | FortiClient / FortiOS 6.4.8 - Fortinet Document Library

NEW QUESTION # 32

Refer to the exhibits.

The exhibits show a diagram of a requested topology and the base IPsec configuration.

A customer asks you to configure ADVPN via two internet underlays. The requirement is that you use one interface with a single IP address on DC FortiGate.

In this scenario, which feature should be implemented to achieve this requirement?

- A. Change advpn2 to IKEv1
- B. Use peer-id
- C. Use local-id
- D. Use network-overlay id

Answer: D

Explanation:

A is correct because using network-overlay id allows you to configure multiple ADVPN tunnels on a single interface with a single IP address on the DC FortiGate. This is explained in the FortiGate Administration Guide under ADVPN > Configuring ADVPN > Configuring ADVPN on the hub. References: <https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn>
<https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/978793/advpn/978794/configuring-advpn>

NEW QUESTION # 33

Refer to the exhibit.



What is happening in this scenario?

- A. The user status changed at FortiClient EMS to off-net.
- B. The user is authenticating against a FortiGate Captive Portal.
- C. The user is authenticating against an IdP.
- C. The user has not authenticated on their external browser.

Answer: C

NEW QUESTION # 34

A customer wants to use the FortiAuthenticator REST API to retrieve an SSO group called SalesGroup. The following API call is being made with the 'curl' utility:

```
curl -k -v -u "admin:zeyDZXmP6GbKcerqdWWEYNTnH2TaXc-5Htp2dAVS" -X PUT -d '{"name":"SalesGroup"}' -H 'Content-Type: application/json' https://10.10.10.12/api/v1/ssogroup/100/
```

Which two statements correctly describe the expected behavior of the FortiAuthenticator REST API? (Choose two.)

- A. The syntax is incorrect because the API call needs the get method.
- B. Only users with the "Full permission" role can access the REST API
- C. This API call will fail because it requires that API version 2
- D. If the REST API web service access key is lost, it cannot be retrieved and must be changed.

Answer: A,C

Explanation:

To retrieve an SSO group called SalesGroup using the FortiAuthenticator REST API, the following issues need to be fixed in the API call:

* The API version should be v2, not v1, as SSO groups are only supported in version 2 of the REST API.

* The HTTP method should be GET, not POST, as GET is used to retrieve information from the server, while POST is used to create or update information on the server. Therefore, a correct API call would look like this: curl -X GET -H "Authorization: Bearer <token>" https://fac.example.com/api/v2/sso

/groups/SalesGroup References: <https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution-guide/927310/introduction>

<https://docs.fortinet.com/document/fortiauthenticator/6.4.1/rest-api-solution-guide/927311/sso-groups>

NEW QUESTION # 35

You want to use the MTA adapter feature on FortiSandbox in an HA-Cluster. Which statement about this solution is true?

- A. The MTA adapter is only available in the primary node.
- B. The configuration is different than on a standalone device.

- Answer: A**

The MTA adapter feature on FortiSandbox is a feature that allows FortiSandbox to act as a mail transfer agent (MTA) that can receive, inspect, and forward email messages from external sources. The MTA adapter feature can be used to integrate FortiSandbox with third-party email security solutions that do not support direct integration with FortiSandbox, such as Microsoft Exchange Server or Cisco Email Security Appliance (ESA). The MTA adapter feature can also be used to enhance email security by adding an additional layer of inspection and filtering before delivering email messages to the final destination. The MTA adapter feature can be enabled on FortiSandbox in an HA-Cluster, which is a configuration that allows two FortiSandbox units to synchronize their settings and data and provide high availability and load balancing for sandboxing services. However, one statement about this solution that is true is that the MTA adapter is only available in the primary node. This means that only one FortiSandbox unit in the HA-Cluster can act as an MTA and receive email messages from external sources, while the other unit acts as a backup node that can take over the MTA role if the primary node fails or loses connectivity. This also means that only one IP address or FQDN can be used to configure the external sources to send email messages to the FortiSandbox MTA, which is the IP address or FQDN of the primary node. Reference: <https://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/mail-transfer-agent-mta> <https://docs.fortinet.com/document/fortisandbox/3.2.0/administration-guide/19662/high-availability-ha>

• • • • •

Reliable NSE8 812 Exam Question: https://www.dumpstillvalid.com/NSE8_812-prep4sure-review.html

- [illegible]

myportal.utt.edu.tt, www.stes.tyc.edu.tw, pct.edu.pk, mindlearn.nathjiiti.in, www.stes.tyc.edu.tw, compassionate.training,
Disposable vapes

DOWNLOAD the newest DumpStillValid NSE8_812 PDF dumps from Cloud Storage for free: <https://drive.google.com/open?id=1FFDs8nZRnV6guHivB7DF9uiZbFy3lq3B>