NSE5_FSW_AD-7.6 Deutsch Prüfungsfragen & NSE5_FSW_AD-7.6 Prüfungsfrage

Außerdem sind jetzt einige Teile dieser EchteFrage NSE5_FSW_AD-7.6 Prüfungsfragen kostenlos erhältlich: https://drive.google.com/open?id=15OALtZZUjDCHAEtJXARiy7A3LmR-mqWM

EchteFrage kann Ihnen nicht nur die ausgezeichnete Prüfungsunterlagen zur Fortinet NSE5_FSW_AD-7.6 Zertifizierung sondern auch guten Service bieten. Kaufen Sie EchteFrage Dumps, bekommen Sie einjährige kostlose Aktualisierung von EchteFrage. Damit können Sie immer die neuesten Fortinet NSE5_FSW_AD-7.6 Prüfungsfragen besitzen. Falls Sie dieFortinet NSE5_FSW_AD-7.6 Prüfung nicht ausgereicht hätten, gibt EchteFrage Ihnen voll Geld zurück. Und dann machen Sie sich keine Sorge. Wir EchteFrage sind sehr zuversichtlich für unsere Dumps. Glauben Sie bitten auch an uns. Verpassen Sie bitte nicht EchteFrage zu Ihrem Erfolg. Wenn Sie das ignorieren, verlieren die Chance für einen einmaligen Erfolg.

Fortinet NSE5_FSW_AD-7.6 Exam Syllabus Topics:

Section	Objectives
FortiSwitch concepts	- Configure VLANs using FortiSwitch - Configure switch ports, split port, and available transceivers - Configure switching and routing on FortiSwitch - Use QoS and LLDP-MED on FortiSwitch - Configure STP to prevent network loops - Configure the ports required for stack deployment
Layer 2 control and security	- Use ACLs, security profiles, and VLAN security mechanisms on FortiSwitch - Use port security options on FortiSwitch - Use filtering and antispoofing techniques on FortiSwitch
Deployment and management	- Configure and provision FortiSwitch - Deploy FortiSwitch supported deployment topologies - Deploy and configure FortiSwitch in a multi-tenancy environment
Monitoring and troubleshooting	- Troubleshoot FortiLink issues - Use packet capturing methods to monitor and troubleshoot traffic issues - Interpret system logs, monitor port statistics, and diagnose connectivity issues - Use tools to view and extract network information from FortiSwitch

>> NSE5_FSW_AD-7.6 Deutsch Prüfungsfragen <<

Fortinet NSE5_FSW_AD-7.6 Prüfungsfrage & NSE5_FSW_AD-7.6 Vorbereitungsfragen

Die Fortinet NSE5_FSW_AD-7.6 Zertifizierungsprüfung ist heutztage sehr beliebt. EchteFrage wird Ihnen helfen, die NSE5_FSW_AD-7.6 Prüfung zu bestehen, und bietet Ihnen einen einjährigen kostenlosen Update-Service. Dann wählen Sie doch EchteFrage, um Ihren Traum zu verwirklichen. Um Erfolg zu erringen, ist Ihnen weise, EchteFrage zu wählen. Wählen Sie EchteFrage, Sie werden der nächste IT-Elite sein.

Fortinet NSE 5 - FortiSwitch 7.6 Administrator NSE5_FSW_AD-7.6 Prüfungsfragen mit Lösungen (Q11-Q16):

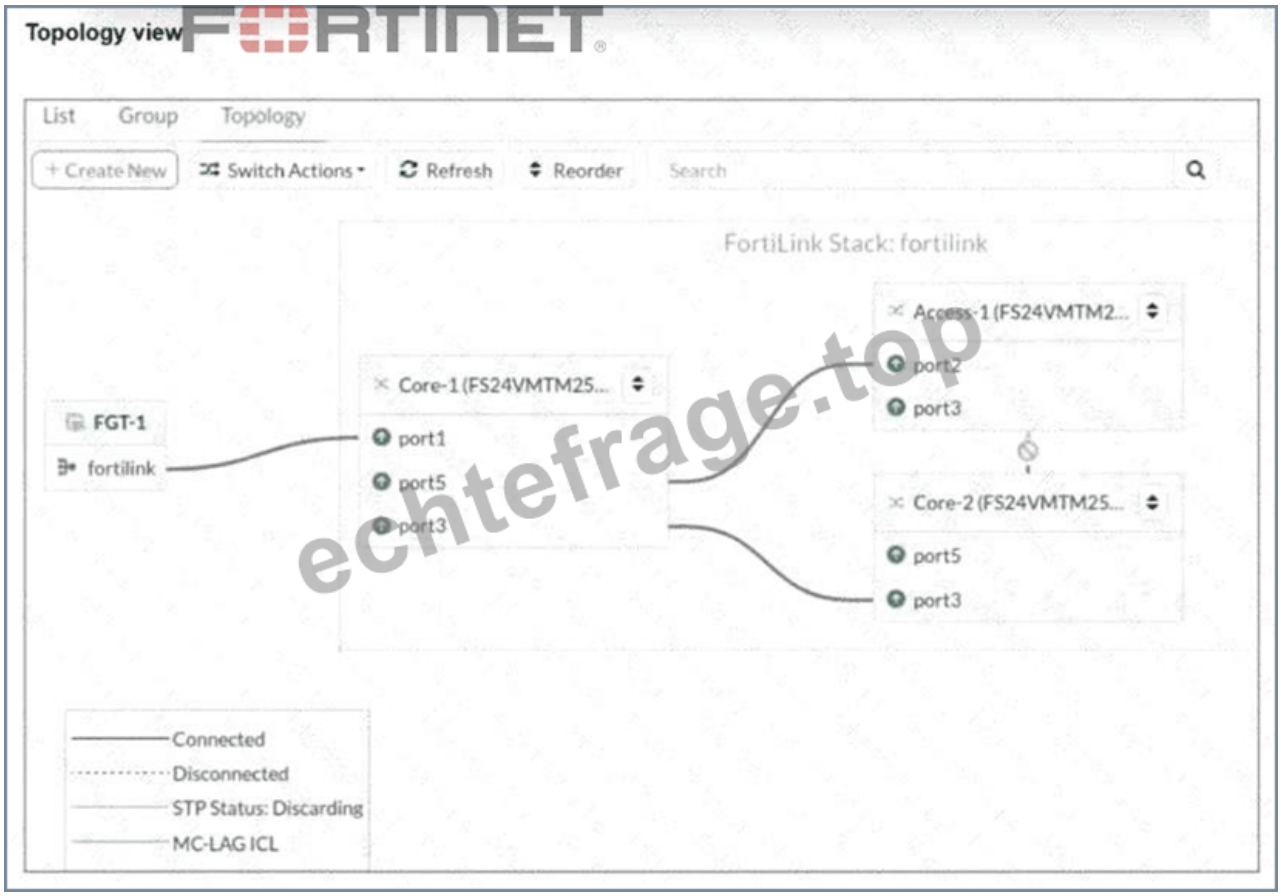
11. Frage
In which two ways can you assign a FortiSwitch port to a VDOM using a multi-tenancy setup? (Choose two answers)

- A. Switch the FortiLink interface to the target VDOM.
- B. Assign the switch port to a VLAN on FortiGate and perform VDOM mapping.
- C. Create a virtual port pool on the FortiGate CLI.
- D. Assign a port to a VDOM directly on the managed FortiSwitch.

Antwort: B,C

Begründung:
According to theFortiOS 7.6 Administration Guideand theFortiSwitch 7.6 Study Guide, multi-tenancy in a FortiLink-managed environment allows a central FortiGate to partition a managed FortiSwitch fabric so that different ports can belong to different Virtual Domains (VDOMs). This is essential for Managed Service Providers (MSPs) who need to isolate client traffic at the hardware layer.
The documentation identifies two primary methods for achieving this assignment:
* Assign to a VLAN and Perform VDOM Mapping (Option A):This is the most common method. The administrator creates a VLAN on the FortiLink interface and assigns it to a specific VDOM on the FortiGate. By assigning a physical FortiSwitch port to that specific VLAN, the port's traffic is logically terminated within the target VDOM. TheVDOM mappingensures that the switch-controller identifies which VDOM "owns" the traffic originating from that specific port/VLAN combination.
* Create a Virtual Port Pool (Option B):For more advanced multi-tenancy, administrators can use the FortiGate CLI to create aVirtual Port Pool. This feature allows the FortiGate to "pool" physical switch ports and present them as logical resources that can be distributed across various VDOMs. This method provides greater flexibility in resource allocation without requiring the entire FortiLink interface to be moved.
Regarding the incorrect options:Option Cis incorrect because in a managed environment, the FortiSwitch CLI is not used for VDOM assignments; all orchestration must happen from the FortiGate.Option Dis incorrect because while you can move a FortiLink interface to a VDOM, this would move theentireswitch management and all its ports to that VDOM, which does not support a multi-tenant setup where different ports need to reside in different VDOMs.

12. Frage
Refer to the exhibit.



You just connected three FortiSwitch devices:Core-1,Core-2, andAccess-1. Core-1 and Core-2 both connect to Access-1 for redundancy. All switches are managed by FortiGate, which uses port4 as the FortiLink interface. After you enable the uplink ports on Core-2, you notice that port3 on Access-1 enters the Discarding STP state. What is the most likely cause of this behavior? (Choose one answer)

- A. FortiGate is not running Spanning Tree Protocol (STP) on the FortiLink interface.
- B. Bridge Protocol Data Unit (BPDU) Guard is enabled, which shuts down the port after it receives BPDUs.
- C. Core-2 has the lowest bridge priority.
- D. Access-1 is not authorized by FortiGate.

Antwort: C

Begründung:
According to theFortiSwitchOS 7.6 Administration Guideand theFortiLink 7.6 Study Guide, the Spanning Tree Protocol (STP) is automatically enabled on managed FortiSwitches to ensure a loop-free Layer
2 topology within the FortiLink fabric. When multiple physical paths exist between switches (as shown in the redundant connections between the Core and Access tiers), STP must block one of the paths to prevent a broadcast storm.
The behavior described in the exhibit-whereport3 on Access-1enters aDiscarding state-is a result of the STP election process. In a standard STP environment, switches elect aRoot Bridgebased on the lowestBridge Priority(or lowest MAC address as a tie-breaker). Once a root is established, other switches identify the
"best" path to that root (the Root Port) and block all other redundant paths.
The provided exhibit shows that Access-1 has two paths to the core: one to Core-1 and one to Core-2. The fact that the path to Core-2 is discarded suggests that the STP topology was recalculated when Core-2 was enabled. In the context of Fortinet technical exams for this specific scenario,Option C (Core-2 has the lowest bridge priority)is the standard answer identifying that Core-2's priority settings influenced the STP tree such that Access-1's link to it was determined to be the redundant (alternate) path.
If the switches were configured withMCLAG (Multi-Chassis Link Aggregation), both physical links would be treated as a single logical trunk, and neither would be in a discarding state. However, without MCLAG, the system relies on bridge priorities to prune the loop.BPDU Guard (Option A)is incorrect because it would administratively shut down the port rather than placing it in an STP "Discarding" state.Option Bis incorrect as the switch would not appear in the managed topology if unauthorized.

13. Frage
What type of multimode transceiver can be used to split a 40G port?

- A. SFP+ transceiver
- B. SFP transceiver
- C. QSFP+ transceiver
- D. QSFP transceiver

Antwort: C

Begründung:
QSFP+ transceiver (A): The QSFP+ (Quad Small Form-factor Pluggable Plus) transceiver is designed to handle 40G data rates and can be used to split a 40G port into multiple 10G connections. This type of transceiver supports such configurations, making it suitable for high-density applications where multiple 10G connections are derived from a single 40G port, thereby maximizing the utilization of the port and the fiber infrastructure.

14. Frage
Refer to the exhibits. An IP phone is connected to port1 of FortiSwitch Access-1. The IP phone tags its traffic with VLAN ID 20. On FortiGate, VLAN IP_Phone (VLAN ID 20) has been configured, and port1 of Access-
1 is set with VLAN 20 as the native VLAN. However, the IP phone cannot reach the network. The exhibit shows the partial VLAN configuration and the port1 configuration on Access-1.
Which configuration change must you make on FortiSwitch to allow ingress and egress traffic for the IP phone? (Choose one answer)

- A. On port1, disable the edge_port
- B. On VLAN IP_Phone, enable vlanforward
- C. On port1, add VLAN 20 to the allowed_vlans list
- D. On VLAN IP_Phone, enable l2forward

Antwort: C

Begründung:
According to theFortiSwitchOS 7.6 Administration GuideandFortiOS 7.6 FortiLink Guide, the processing of Ethernet frames on a managed FortiSwitch port depends on whether the frame is tagged or untagged upon arrival (ingress) and how the port's VLAN membership is defined.
In the provided exhibit,port1is configured with set vlan "IP_Phone" (VLAN 20) as itsnative VLAN. By definition, the native VLAN handles untagged traffic; any untagged frame arriving at the port is assigned to VLAN 20, and any egress traffic from VLAN 20 is sent out of the port without a tag. However, the scenario specifically states that theIP phone tags its traffic with VLAN ID 20.
When a FortiSwitch receives atagged frame, it checks the VLAN ID against theallowed-vlanslist configured on that port. Although VLAN 20 is the native VLAN, the exhibit shows that the port has been explicitly configured with set allowed-vlans "quarantine". This creates a restrictive filter that permits only tagged frames belonging to the "quarantine" VLAN to enter or exit the port. Because VLAN 20 (IP_Phone) is not present in the allowed-vlans list, the switch drops the tagged frames from the IP phone during ingress processing.
To resolve this, the administrator must modify theFortiSwitch port configurationby adding VLAN 20 to the allowed_vlans list (e.g., set allowed-vlans "quarantine" "IP_Phone" or set allowed-vlans-all enable). This ensures that the switch recognizes and permits tagged traffic for VLAN 20 on that physical interface. Option B is incorrect because l2forward is a Layer 3 interface setting on the FortiGate and does not address the physical port's ingress filtering logic on the switch. Disabling the edge_port (Option D) relates to Spanning Tree Protocol (STP) convergence and would not impact VLAN tag filtering.

15. Frage
Exhibit.
You need to manage three FortiSwitch devices using a FortiGate device. Two of the FortiSwitch devices initiated a reboot after the authorization process. However, the FortiSwitch device with the configuration shown in the exhibit. did not reboot All three devices completed FortiLink manage-ment authorization successfully.
Why did the FortiSwitch device shown in the exhibit not reboot to complete the authorization pro-cess?
The management mode was set to use FortiLink mode.

- A. The system time is not in-sync and is using a non-default value
- B. Switch auto-discovery is enabled.
- C. The FortiSwitch device is scheduled to reboot as part the authorization process
- D. The management mode was set to use FortiLink mode.

Antwort: D

Begründung:
Regarding the scenario where a FortiSwitch did not reboot after the authorization process while the other devices did, the most likely cause, given the configuration settings in the exhibit, is:
* The management mode was set to use FortiLink mode (Option B): If the FortiSwitch was already configured to use FortiLink for its management mode, it may not require a reboot to complete the authorization process as its management interface settings are already aligned with FortiLink requirements. This is unlike switches that might be transitioning from a standalone or another management mode, which would typically require a reboot to apply new management settings fully.
References:
FortiLink mode specifically tailors FortiSwitch to be managed via a FortiGate device, integrating its operation into the wider security fabric without needing a reboot if it is already set to this mode before authorization.
This contrasts with other management modes where transitioning to FortiLink could necessitate a system restart to initialize the new configuration.

16. Frage
.....

BONUS!!! Laden Sie die vollständige Version der EchteFrage NSE5_FSW_AD-7.6 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=15OALtZZUjDCHAEtJXARiy7A3LmR-mqWM