

3V0-41.22 Fragenkatalog, 3V0-41.22 Zertifizierung



BONUS!!! Laden Sie die vollständige Version der ZertSoft 3V0-41.22 Prüfungsfragen kostenlos herunter:
https://drive.google.com/open?id=1qdP1vDfgIV27Fcpd2FLvgSL_dlbqchKs

Wahrscheinlich haben viele Leute Sie über die Schwierigkeiten der VMware 3V0-41.22 informiert. Aber wir ZertSoft möchten Ihnen mitteilen, wie einfach die VMware 3V0-41.22 Prüfung zu bestehen. Die VMware 3V0-41.22 Prüfungssoftware von unserem fähigen IT-Team können Sie bestimmt befriedigen. Sie brauchen nur die kostenlose Demo der VMware 3V0-41.22 probieren. Dann werden Sie unbesorgt kaufen. Wir hoffen, dass wir bei Ihrem Fortschritt im Bereich der IT helfen können!

Jeder IT-Fachmann bemüht sich darum, entweder befördert zu werden oder ein höheres Gehalt zu beziehen. Das ist der Druck unserer Gesellschaft. Wir sollen uns mit unseren Fähigkeiten beweisen. Legen Sie bitte die VMware 3V0-41.22 Zertifizierungsprüfung ab. Eigentlich ist sie nicht so schwer wie man gedacht, solange Sie geeignete Dumps wählen. Die Dumps zur VMware 3V0-41.22 Zertifizierung von ZertSoft sind die besten Dumps. Mit ihr können Sie etwas erzielen, wie Sie wollen.

>> 3V0-41.22 Fragenkatalog <<

3V0-41.22 Zertifizierung - 3V0-41.22 Prüfungsübungen

Das Expertenteam von ZertSoft hat neulich das effiziente kurzfristige Schulungsprogramm zur VMware 3V0-41.22 Zertifizierungsprüfung entwickelt. Die Kandidaten sollen an dem 20-stündigen Kurs teilnehmen, dann können sie neue Kenntnisse beherrschen und ihre ursprüngliches Wissen konsolidieren und auch die VMware 3V0-41.22 Zertifizierungsprüfung leichter als diejenigen, die viel Zeit und Energie auf die Prüfung verwendet, bestehen.

VMware Advanced Deploy VMware NSX-T Data Center 3.X 3V0-41.22 Prüfungsfragen mit Lösungen (Q15-Q20):

15. Frage

SIMULATION

Task 14

An administrator has seen an abundance of alarms regarding high CPU usage on the NSX Managers. The administrator has successfully cleared these alarms numerous times in the past and is aware of the issue. The administrator feels that the number of alarms being produced for these events is overwhelming the log files.

You need to:

* Review CPU Sensitivity and Threshold values.

Complete the requested task.

Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. This task should take approximately 5 minutes to complete.

Antwort:**Begründung:**

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To review CPU sensitivity and threshold values, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to System > Settings > System Settings > CPU and Memory Thresholds.

You will see the current values for CPU and memory thresholds for NSX Manager, NSX Controller, and NSX Edge. These values determine the percentage of CPU and memory usage that will trigger an alarm on the NSX Manager UI.

You can modify the default threshold values by clicking Edit and entering new values in the text boxes. For example, you can increase the CPU threshold for NSX Manager from 80% to 90% to reduce the number of alarms for high CPU usage. Click Save to apply the changes.

You can also view the historical data for CPU and memory usage for each component by clicking View Usage History. You can select a time range and a granularity level to see the usage trends and patterns over time

16. Frage

Task 11

upon testing the newly configured distributed firewall policy for the Boston application. it has been discovered that the Boston-Web virtual machines can be "pinged" via ICMP from the main console. Corporate policy does not allow pings to the Boston VMs.

You need to:

* Troubleshoot ICMP traffic and make any necessary changes to the Boston application security policy.

Complete the requested task.

Notes: Passwords are contained in the user_readme.txt. This task is dependent on Task 5.

Antwort:**Begründung:**

See the Explanation part of the Complete Solution and step by step instructions.

Explanation

To troubleshoot ICMP traffic and make any necessary changes to the Boston application security policy, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is

<https://<nsx-manager-ip-address>>.

Navigate to Security > Distributed Firewall and select the firewall policy that applies to the Boston application. For example, select Boston-web-Application.

Click Show IPsec Statistics and view the details of the firewall rule hits and logs. You can see which rules are matching the ICMP traffic and which actions are taken by the firewall.

If you find that the ICMP traffic is allowed by a rule that is not intended for it, you can edit the rule and change the action to Drop or Reject. You can also modify the source, destination, or service criteria of the rule to make it more specific or exclude the ICMP traffic.

If you find that the ICMP traffic is not matched by any rule, you can create a new rule and specify the action as Drop or Reject. You can also specify the source, destination, or service criteria of the rule to match only the ICMP traffic from the main console to the Boston web VMs.

After making the changes, click Publish to apply the firewall policy.

Verify that the ICMP traffic is blocked by pinging the Boston web VMs from the main console again. You should see a message saying "Request timed out" or "Destination unreachable".

17. Frage

SIMULATION

Task 5

You are asked to configure a micro-segmentation policy for a new 3-tier web application that will be deployed to the production environment.

You need to:

• Configure Tags with the following configuration detail:

Tag Name	Member
Boston	Boston-web-01a, Boston-web-02a, Boston-app-01a, Boston-db-01a
Boston-Web	Boston-web-01a, Boston-web-02a
Boston-App	Boston-app-01a
Boston-DB	Boston-db-01a

• Configure Security Groups (use tags to define group criteria) with the following configuration detail:

Boston
Boston Web-Servers
Boston App-Servers
Boston DB-Servers

• Configure the Distributed Firewall Exclusion List with the following configuration detail:

Virtual Machine:

• Configure Policy & DFW Rules with the following configuration detail:

Policy Name:	Boston-Web-Application
Applied to:	Boston
New Services:	TCP-8443, TCP-3051

• Policy detail:

Rule Name	Source	Destination	Service	Action
Any-to-Web	Any	Boston Web-Servers	HTTP,HTTPS	ALLOW
Web-to-App	Boston Web-Servers	Boston App-Servers	TCP-8443	ALLOW
App-to-DB	Boston App-Servers	Boston DB-Servers	TCP-3051	ALLOW

Notes:

Passwords are contained in the user_readme.txt. Do not wait for configuration changes to be applied in this task as processing may take some time. The task steps are not dependent on one another. Subsequent tasks may require completion of this task. This task should take approximately 25 minutes to complete.

Antwort:

Begründung:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

Step-by-Step Guide

Creating Tags and Security Groups

First, log into the NSX-T Manager GUI and navigate to Inventory > Tags to create tags like "BOSTON-Web" for web servers and assign virtual machines such as BOSTON-web-01a and BOSTON-web-02 a. Repeat for "BOSTON-App" and "BOSTON-DB" with their respective VMs. Then, under Security > Groups, create security groups (e.g., "BOSTON Web-Servers") based on these tags to organize the network logically.

Excluding Virtual Machines

Next, go to Security > Distributed Firewall > Exclusion List and add the "core-A" virtual machine to exclude it from firewall rules, ensuring it operates without distributed firewall restrictions.

Defining Custom Services

Check Security > Services for existing services. If "TCP-9443" and "TCP-3051" are missing, create them by adding new services with the protocol TCP and respective port numbers to handle specific application traffic.

Setting Up the Policy and Rules

Create a new policy named "BOSTON-Web-Application" under Security > Distributed Firewall > Policies. Add rules within this policy:

Allow any source to "BOSTON Web-Servers" for HTTP/HTTPS.

Permit "BOSTON Web-Servers" to "BOSTON App-Servers" on TCP-9443.

Allow "BOSTON App-Servers" to "BOSTON DB-Servers" on TCP-3051. Finally, save and publish the policy to apply the changes.

This setup ensures secure, segmented traffic for the 3-tier web application, an unexpected detail being the need to manually create custom services for specific ports, enhancing flexibility.

Survey Note: Detailed Configuration of Micro-Segmentation Policy in VMware NSX-T Data Center 3.x This note provides a comprehensive guide for configuring a micro-segmentation policy for a 3-tier web application in VMware NSX-T Data Center 3.x, based on the task requirements. The process involves creating tags, security groups, excluding specific virtual machines, defining custom services, and setting up distributed firewall policies. The following sections detail each step, ensuring a thorough understanding for network administrators and security professionals.

Background and Context

Micro-segmentation in VMware NSX-T Data Center is a network security technique that logically divides the data center into distinct security segments, down to the individual workload level, using network virtualization technology. This is particularly crucial for a 3-tier web application, comprising web, application, and database layers, to control traffic and enhance security. The task

specifies configuring this for a production environment, with notes indicating passwords are in user_readme.txt and no need to wait for configuration changes, as processing may take time.

Step-by-Step Configuration Process

Step 1: Creating Tags

Tags are used in NSX-T to categorize virtual machines, which can then be grouped for policy application. The process begins by logging into the NSX-T Manager GUI, accessible via a web browser with admin privileges. Navigate to Inventory > Tags, and click "Add Tag" to create the following:

Tag name: "BOSTON-Web", assigned to virtual machines BOSTON-web-01a and BOSTON-web-02a.

Tag name: "BOSTON-App", assigned to BOSTON-app-01a.

Tag name: "BOSTON-DB", assigned to BOSTON-db-01a.

This step ensures each tier of the application is tagged for easy identification and grouping, aligning with the attachment's configuration details.

Step 2: Creating Security Groups

Security groups in NSX-T are logical constructs that define membership based on criteria like tags, enabling targeted policy application. Under Security > Groups, click "Add Group" to create:

Group name: "BOSTON Web-Servers", with criteria set to include the "BOSTON-Web" tag

Group name: "BOSTON App-Servers", with criteria set to include the "BOSTON-App" tag

Group name: "BOSTON DB-Servers", with criteria set to include the "BOSTON-DB" tag

This step organizes the network into manageable segments, facilitating the application of firewall rules to specific tiers.

Step 3: Excluding "core-A" VM from Distributed Firewall

The distributed firewall (DFW) in NSX-T monitors east-west traffic between virtual machines. However, certain VMs, like load balancers or firewalls, may need exclusion to operate without DFW restrictions. Navigate to Security > Distributed Firewall > Exclusion List, click "Add", select "Virtual Machine", and choose "core-A". Click "Save" to exclude it, ensuring it bypasses DFW rules, as per the task's requirement.

Step 4: Defining Custom Services

Firewall rules often require specific services, which may not be predefined. Under Security > Services, check for existing services "TCP-9443" and "TCP-3051". If absent, create them:

Click "Add Service", name it "TCP-9443", set protocol to TCP, and port to 9443.

Repeat for "TCP-3051", with protocol TCP and port 3051.

This step is crucial for handling application-specific traffic, such as the TCP ports mentioned in the policy type (TCP-9443, TCP-3051), ensuring the rules can reference these services.

Step 5: Creating the Policy and Rules

The final step involves creating a distributed firewall policy to enforce micro-segmentation. Navigate to Security > Distributed Firewall > Policies, click "Add Policy", and name it "BOSTON-Web-Application". Add a section, then create the following rules:

Rule Name: "Any-to-Web"

Source: Any (select "Any" or IP Address 0.0.0.0/0)

Destination: "BOSTON Web-Servers" (select the group)

Service: HTTP/HTTPS (predefined service)

Action: Allow

Rule Name: "Web-to-App"

Source: "BOSTON Web-Servers"

Destination: "BOSTON App-Servers"

Service: TCP-9443 (custom service created earlier)

Action: Allow

Rule Name: "App-to-DB"

Source: "BOSTON App-Servers"

Destination: "BOSTON DB-Servers"

Service: TCP-3051 (custom service created earlier)

Action: Allow

After defining the rules, click "Save" and "Publish" to apply the policy. This ensures traffic flows as required: any to web servers for HTTP/HTTPS, web to app on TCP-9443, and app to database on TCP-3051, while maintaining security through segmentation.

Additional Considerations

The task notes indicate no need to wait for configuration changes, as processing may take time, and steps are not dependent, suggesting immediate progression is acceptable. Passwords are in user_readme.txt, implying the user has necessary credentials. The policy order is critical, with rules processed top-to-bottom, and the attachment's "Type: TCP-9443, TCP-3051" likely describes the services used, not affecting the configuration steps directly.

Table: Summary of Configuration Details

Component

Details

Tags

BOSTON-Web (BOSTON-web-01a, BOSTON-web-02a), BOSTON-App (BOSTON-app-01a), BOSTON-DB (BOSTON-

db-01a) Security Groups BOSTON Web-Servers (tag BOSTON-Web), BOSTON App-Servers (tag BOSTON-App), BOSTON DB-Servers (tag BOSTON-DB) DFW Exclusion List Virtual Machine: core-A Custom Services TCP-9443 (TCP, port 9443), TCP-3051 (TCP, port 3051) Policy Name BOSTON-Web-Application Firewall Rules Any-to-Web (Any to Web-Servers, HTTP/HTTPS, Allow), Web-to-App (Web to App-Servers, TCP-9443, Allow), App-to-DB (App to DB-Servers, TCP-3051, Allow) This table summarizes the configuration, aiding in verification and documentation.

Unexpected Detail

An unexpected aspect is the need to manually create custom services for TCP-9443 and TCP-3051, which may not be predefined, highlighting the flexibility of NSX-T for application-specific security policies.

Conclusion

This detailed process ensures a robust micro-segmentation policy, securing the 3-tier web application by controlling traffic between tiers and excluding specific VMs from DFW, aligning with best practices for network security in VMware NSX-T Data Center 3.x.

18. Frage

SIMULATION

Task 9

TO prepare for Virtual machine migration from VLAN-backed port groups to an overlay segment in NSX, a test bridge has been configured. The bridge is not functioning, and the -Bridge-VM- is not responding to ICMP requests from the main console.

You need to:

* Troubleshoot the configuration and make necessary changes to restore access to the application.

Complete the requested task.

Notes: Passwords are contained in the user_readme.txt. This task is not dependent on another. This task should take approximately 15 minutes to complete.

Antwort:

Begründung:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To troubleshoot the bridge configuration and restore access to the application, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to Networking > Segments and select the overlay segment that is bridged to the VLAN-backed port group. For example, select Web-01 segment that you created in Task 2.

Click Bridge > Set and verify the configuration details of the bridge. Check for any discrepancies or errors in the parameters such as bridge name, bridge ID, VLAN ID, edge node, etc.

If you find any configuration errors, click Edit and modify the parameters accordingly. Click Save to apply the changes.

If you do not find any configuration errors, check the connectivity and firewall rules between the overlay segment and the VLAN-backed port group. You can use ping or traceroute commands from the NSX Edge CLI or the vSphere Web Client to test the connectivity. You can also use show service bridge command to check the status of the bridge service on the NSX Edge.

If you find any connectivity or firewall issues, resolve them by adjusting the network settings or firewall rules on the NSX Edge or the vSphere Distributed Switch.

After resolving the issues, verify that the bridge is functioning and the Bridge-VM is responding to ICMP requests from the main console. You can also check the MAC addresses learned by the bridge on both sides of the network using show service bridge mac command on the NSX Edge CLI.

19. Frage

SIMULATION

Task 12

An issue with the Tampa web servers has been reported. You would like to replicate and redirect the web traffic to a network monitoring tool outside Of the NSX-T environment to further analyze the traffic.

You are asked to configure traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic using this detail:

Session Name:	Network-Monitor-01
Network Appliance Name / Group:	NM-01
Direction:	Bi Directional
TCP/IP Stack:	Default
Encapsulation Type:	GRE

Complete the requested configuration.

Notes: Passwords are contained in the user_readme.txt. This task is not dependent on other tasks. This task should take approximately 10 minutes to complete.

Antwort:

Begründung:

See the Explanation part of the Complete Solution and step by step instructions Explanation:

To configure traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic, you need to follow these steps:

Log in to the NSX Manager UI with admin credentials. The default URL is <https://<nsx-manager-ip-address>>.

Navigate to Networking > Segments and select the Tampa web overlay segment that you want to replicate the traffic from. For example, select Web-01 segment that you created in Task 2.

Click Port Mirroring > Set > Add Session and enter a name and an optional description for the port mirroring session. For example, enter Tampa-Web-Monitoring.

In the Direction section, select Bi-directional as the direction from the drop-down menu. This will replicate both ingress and egress traffic from the source to the destination.

In the Source section, click Set and select the VMs or logical ports that you want to use as the source of the traffic. For example, select Web-VM-01 and Web-VM-02 as the source VMs. Click Apply.

In the Destination section, click Set and select Remote L3 SPAN as the destination type from the drop-down menu. This will allow you to replicate the traffic to a remote destination outside of the NSX-T environment.

Enter the IP address of the destination device where you have installed the network monitoring software, such as 10.10.10.200.

Select an existing service profile from the drop-down menu or create a new one by clicking New Service Profile. A service profile defines the encapsulation type and other parameters for the replicated traffic.

Optionally, you can configure advanced settings such as TCP/IP stack, snap length, etc., for the port mirroring session.

Click Save and then Close to create the port mirroring session.

You have successfully configured traffic replication to the monitoring software for your Tampa web overlay segments with bi-directional traffic using NSX-T Manager UI.

20. Frage

.....

Wenn Sie ZertSoft wählen, können Sie 100% die Prüfung bestehen. Nach den Veränderungen der Prüfungsthemen der VMware 3V0-41.22 aktualisieren wir auch ständig unsere Schulungsunterlagen und bieten neue Prüfungsinhalte. ZertSoft bietet Ihnen rund um die Uhr kostenlosen Online-Service. Falls Sie in der VMware 3V0-41.22 Zertifizierungsprüfung durchfallen, zahlen wir Ihnen die gesamte Summe zurück.

3V0-41.22 Zertifizierung: <https://www.zertsoft.com/3V0-41.22-pruefungsfragen.html>

Es gibt viele Lernmaterialien für echte Prüfung auf dem Markt; Sie werden den Unterschied nach dem Demo Probieren unserer 3V0-41.22 exams4sure pdf erkennen, Aber wie kann man VMware 3V0-41.22 Prüfung bestehen und das Zertifikat erhalten, Wenn Sie ZertSoft 3V0-41.22 Zertifizierung, können Sie Erfolg erzielen, ZertSoft stellt den an der 3V0-41.22 Zertifizierungsprüfung Teilnehmenden die neuesten und genauen Prüfungsfragen und Antworten zur Verfügung.

Man kann sagen, dass der Taoismus und die Chuchi-Literatur neue 3V0-41.22 Prüfungsübungen Produkte sind, die der Kultur des alten China hinzugefügt wurden, Nein, sagte er, tut mir leid, ich habe kein Geld.

Es gibt viele Lernmaterialien für echte Prüfung 3V0-41.22 auf dem Markt; Sie werden den Unterschied nach dem Demo Probieren unserer 3V0-41.22 exams4sure pdf erkennen, Aber wie kann man VMware 3V0-41.22 Prüfung bestehen und das Zertifikat erhalten?

3V0-41.22: Advanced Deploy VMware NSX-T Data Center 3.X Dumps & PassGuide 3V0-41.22 Examen

Wenn Sie ZertSoft, können Sie Erfolg erzielen, ZertSoft stellt den an der 3V0-41.22 Zertifizierungsprüfung Teilnehmenden die neuesten und genauen Prüfungsfragen und Antworten zur Verfügung.

Die Prüfungsfragen von 3V0-41.22 Studienführer sind umfassend und enthält die neue Schwerpunkte.

- 3V0-41.22 Prüfung 3V0-41.22 Schulungsunterlagen 3V0-41.22 Prüfung Suchen Sie auf ► www.zertpruefung.ch ◀ nach 3V0-41.22 und erhalten Sie den kostenlosen Download mühelos 3V0-41.22 Prüfung
- 3V0-41.22 Zertifizierungsprüfung 3V0-41.22 Schulungsunterlagen 3V0-41.22 Testing Engine Suchen Sie auf ⇒ www.itzert.com ⇐ nach ► 3V0-41.22 und erhalten Sie den kostenlosen Download mühelos 3V0-41.22 Prüfungssimulationen

