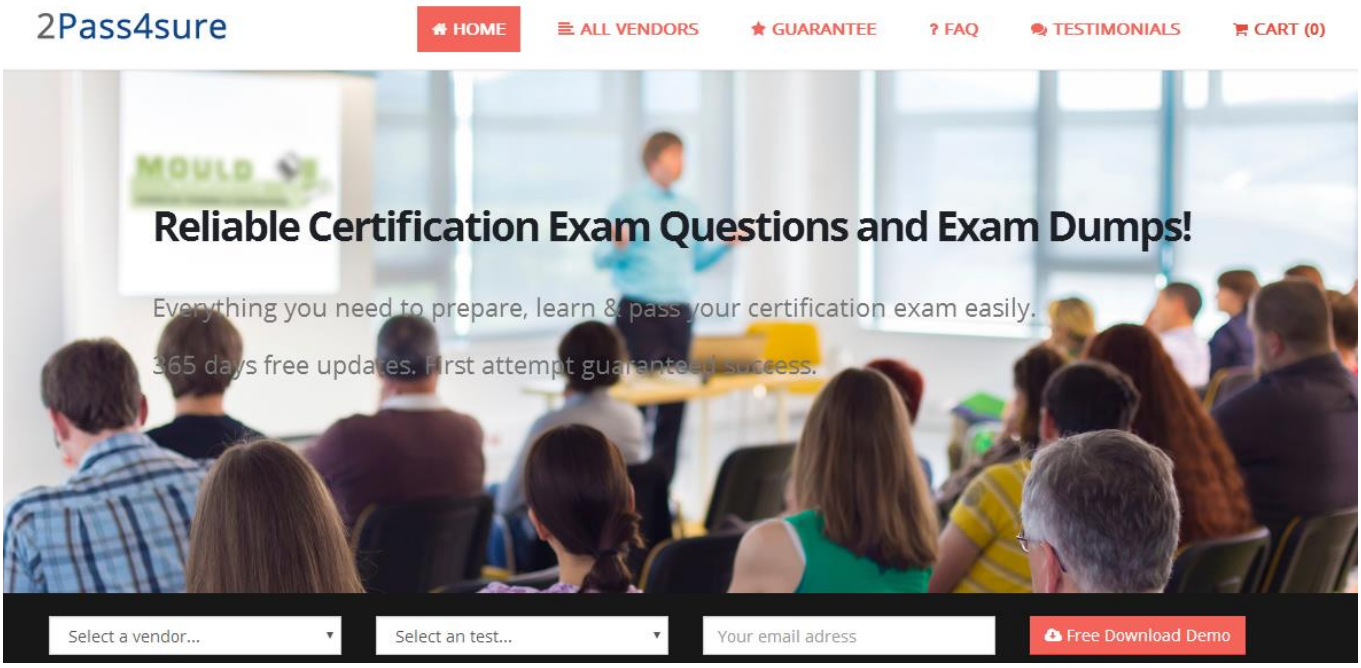
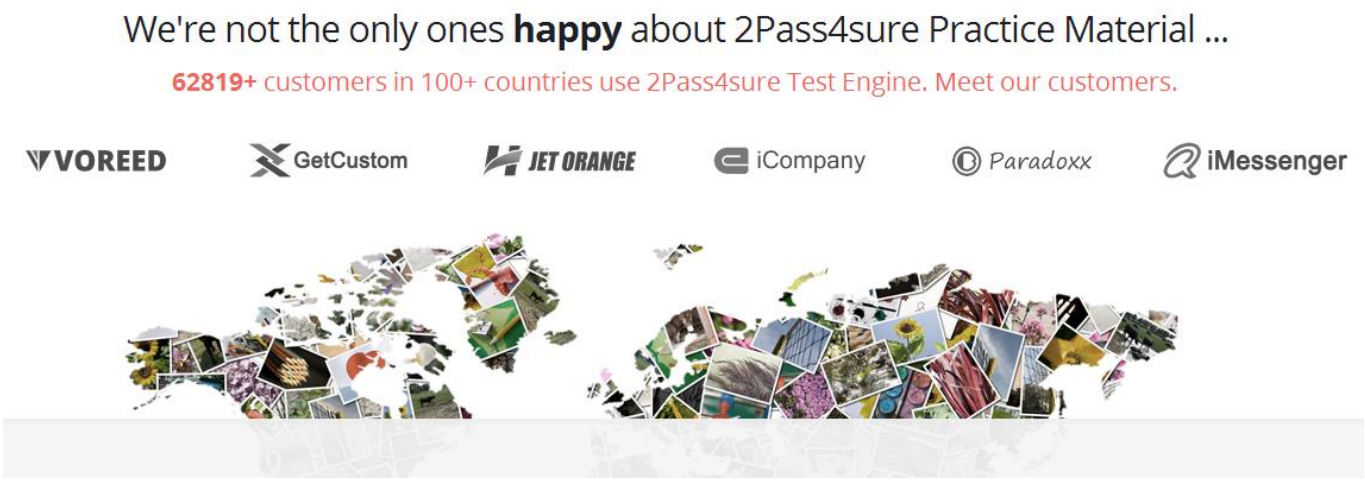
2Pass4sure





http://www.2pass4sure.com/

Reliable Certification Exam Questions and Exam Dumps - 2Pass4sure

Exam : **2V0-41.23-JPN**

Title : VMware NSX 4.x Professional (2V0-41.23日本語版)

Vendor : VMware

Version : DEMO

QUESTION NO: 1
サポートされている 2 つのホスト スイッチ モードは何ですか? (2つお選びください。)
A. DPDK データパス
B. 拡張データパス
C. オーバーレイ データパス
D. 安全なデータパス
E. 標準データパス
Answer: B E
Explanation:
The host switch modes determine how the NSX network and security stack is allocated on the underlying host CPU or DPU. There are two supported host switch modes: Enhanced Datapath and Standard Datapath1. Enhanced Datapath mode leverages the DPU to offload the NSX datapath processing from the host CPU, while Standard Datapath mode uses the host CPU for the NSX datapath processing1. DPDK Datapath, Overlay Datapath, and Secure Datapath are not valid host switch modes for NSX 4.x. References: NSX Features

QUESTION NO: 2
vmnic リンクのステータスがダウンしているかどうかを確認するために使用できる 2 つの CLI コマンドはどれですか? (2つお選びください。)
A. esxcfg-nics -1
B. ネットワーク NIC リスト以外
C. esxcli ネットワーク vswitch dvs wmare リスト
D. esxcfg-vmknic -1
E. esxcfg-vmsvc/get.network
Answer: A B
Explanation:
esxcfg-nics -l and esxcli network nic list are two CLI commands that can be used to see the vmnic link status on an ESXi host. Both commands display information such as the vmnic name, driver, link state, speed, and duplex mode. The link state can be either Up or Down, indicating whether the vmnic is connected or not. For example, the output of esxcfg-nics -l can look like this:
Name PCI Driver Link Speed Duplex MAC Address MTU Description
vmnic0 0000:02:00.0 igbn Up 1000Mbps Full 00:50:56:01:2a:3b 1500 Intel Corporation I350 Gigabit Network Connection vmnic1 0000:02:00.1 igbn Down 0Mbps Half 00:50:56:01:2a:3c 1500 Intel Corporation I350 Gigabit Network Connection

QUESTION NO: 3
ローカル ユーザーの認証ポリシーを変更するために使用される NSX CLI コマンドはどれですか?
A. cli タイムアウトを設定します
B. 認証ポリシーの最小パスワード長を取得します
C. 強化ポリシーの設定
D. 認証ポリシーを設定します
Answer: D

Explanation:
According to the VMware NSX Documentation4, the set auth-policy command is used to change the authentication policy settings for local users, such as password length, lockout period, and maximum authentication failures. The other commands are either used to view the authentication policy settings (B), change the CLI session timeout (A), or change the hardening policy settings .

QUESTION NO: 4
NSX Manager の syslog を表示する CLI コマンドはどれですか?
A. ログファイル auth.lag を取得します
B. /var/log/syslog/syslog.log
C. ログ マネージャーのフォローを表示
D. ログファイルの syslog を取得します
Answer: D
Explanation:
According to the VMware NSX CLI Reference Guide, this CLI command shows the syslog messages on the NSX Manager node. You can use this command to view the system logs for troubleshooting or monitoring purposes.
The other options are either incorrect or not available for this task. get log-file auth.log is a CLI command that shows the authentication logs on the NSX Manager node, not the syslog messages. /var/log/syslog/syslog.log is not a CLI command, but a file path that may contain syslog messages on some Linux systems, but not on the NSX Manager node. show log manager follow is not a valid CLI command, as there is no show log command or manager option in the NSX CLI.
NSX Cli command
get log-file <fiilename>
get log-file <filename> follow
Below are commonly used log files, there are many more log files
get log-file <auth.log | controller | controller-error | http.log | kern.log | manager.log | node-mgmt.log | policy.log | syslog> [follow]
use [follow] to continuing monitor
Example: get log-file syslog follow
get log-file syslog

QUESTION NO: 5
NSX 管理者は、異なるセグメントに存在するアプリ仮想マシンと DB
仮想マシン間の接続を検証するためにどの TraceFlow トラフィック
タイプを使用する必要がありますか?
A. マルチキャスト
B. ユニキャスト
C. エニーキャスト
D. ブロードキャスト
Answer: B
Explanation:
Unicast is the traffic type that an NSX administrator should use for validating connectivity

between App and DB virtual machines that reside on different segments. According to the VMware documentation1, unicast traffic is the traffic type that is used to send a packet from one source to one destination. Unicast traffic is the most common type of traffic in a network, and it is used for applications such as web browsing, email, file transfer, and so on2. To perform a traceflow with unicast traffic, the NSX administrator needs to specify the source and destination IP addresses, and optionally the protocol and related parameters1. The traceflow will show the path of the packet across the network and any observations or errors along the way3. The other options are incorrect because they are not suitable for validating connectivity between two specific virtual machines. Multicast traffic is the traffic type that is used to send a packet from one source to multiple destinations simultaneously2. Multicast traffic is used for applications such as video streaming, online gaming, and group communication4. To perform a traceflow with multicast traffic, the NSX administrator needs to specify the source IP address and the destination multicast IP address1. Broadcast traffic is the traffic type that is used to send a packet from one source to all devices on the same subnet2. Broadcast traffic is used for applications such as ARP, DHCP, and network discovery. To perform a traceflow with broadcast traffic, the NSX administrator needs to specify the source IP address and the destination MAC address as FF:FF:FF:FF:FF:FF1. Anycast traffic is not a valid option, as it is not supported by NSX Traceflow. Anycast traffic is a traffic type that is used to send a packet from one source to the nearest or best destination among a group of devices that share the same IP address. Anycast traffic is used for applications such as DNS, CDN, and load balancing.

QUESTION NO: 6
ステートフル アクティブ/アクティブ SNAT を有効にする前に、NSX 環境で構成する必要がある設定は次のうちどれですか?
A. アクティブ/スタンバイ モードの Tier-1 ゲートウェイ
B. 分散専用モードの Tier-1 ゲートウェイ
C. NSX Edge アップリンクのインターフェイス グループ
D. NSX Edge アップリンクのパンティング トラフィック グループ
Answer: C
Explanation:
To enable stateful active-active SNAT on a Tier-0 or Tier-1 gateway, you must configure an Interface Group for the NSX Edge uplinks. An Interface Group is a logical grouping of NSX Edge interfaces that belong to the same failure domain. A failure domain is a set of NSX Edge nodes that share the same physical network infrastructure and are subject to the same network failures. By configuring an Interface Group, you can ensure that the stateful services are distributed across different failure domains and can recover from network failures1

QUESTION NO: 7
トラフィックが通過するルート パスに影響を与えるために使用できる 2 つの有効な BGP 属性は何ですか? (2つお選びください。)
A. AS パスの先頭に追加
B. BFD
C. コスト
D. MED

Answer: A D
* AS-Path Prepend: This attribute allows you to prepend one or more AS numbers to the AS path of a route, making it appear longer and less preferable to other BGP routers. You can use this attribute to manipulate the inbound traffic from your BGP peers by advertising a longer AS path for some routes and a shorter AS path for others .
* MED: This attribute stands for Multi-Exit Discriminator and allows you to specify a preference value for a route among multiple exit points from an AS. You can use this attribute to manipulate the outbound traffic to your BGP peers by advertising a lower MED value for some routes and a higher MED value for others .

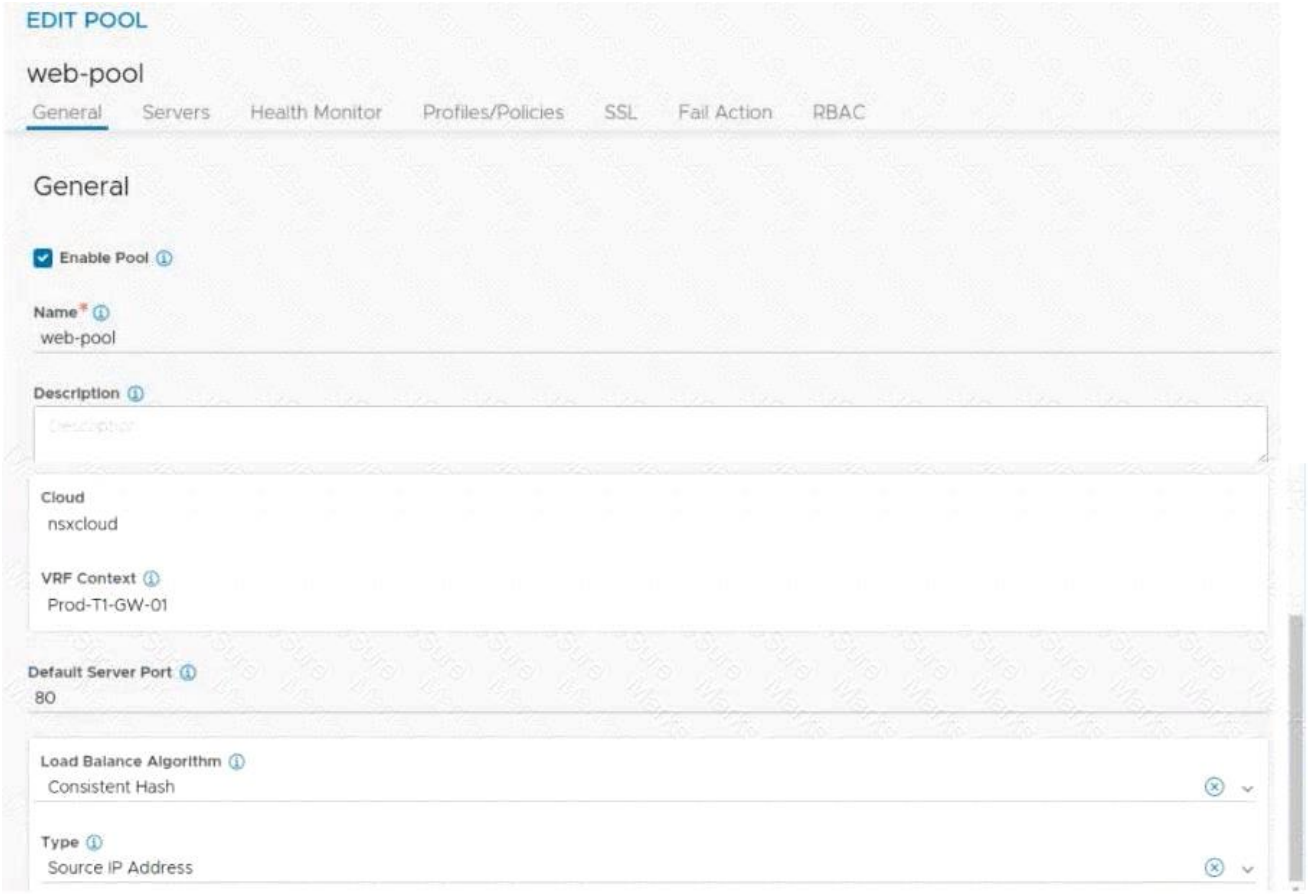
QUESTION NO: 8
セキュリティ管理者は、特定のアプリケーションのドメイン名に基づいてファイアウォールルールを構成する必要があります。
管理者は分散ファイアウォール ルールのどのフィールドを設定しますか?
A. プロフィール
B. サービス
C. ポリシー
D. ソース
Answer: A
Explanation:
To configure a firewall rule based on the domain name of a specific application, the administrator needs to use the Profile field in a distributed firewall rule. The Profile field allows the administrator to select a context profile that contains one or more attributes for filtering traffic. One of the attributes that can be used is Domain (FQDN) Name, which specifies the fully qualified domain name of the application. For example, if the administrator wants to filter traffic to *.office365.com, they can create a context profile with the Domain (FQDN) Name attribute set to *.office365.com and use it in the Profile field of the firewall rule.
References:
* Filtering Specific Domains (FQDN/URLs)
* FQDN Filtering

QUESTION NO: 9
組織の IT セキュリティ コンプライアンス要件の一部として、NSX Manager を 2FA (2 要素認証) 用に構成する必要があります。
統合を構成する前に、NSX 管理者は何を準備する必要がありますか? ○
A. Active Directory LDAP と OAuth クライアントの統合が追加されました
B. OAuth クライアントが追加された VMware Identity Manager
C. Active Directory LDAP と ADFS の統合
D. NSX を Web アプリケーションとして追加した VMware Identity Manager
Answer: B
Explanation:
To configure NSX Manager for two-factor authentication (2FA), an NSX administrator must have VMware Identity Manager (vIDM) with an OAuth Client added. vIDM provides identity management services and supports various 2FA methods, such as VMware Verify, RSA

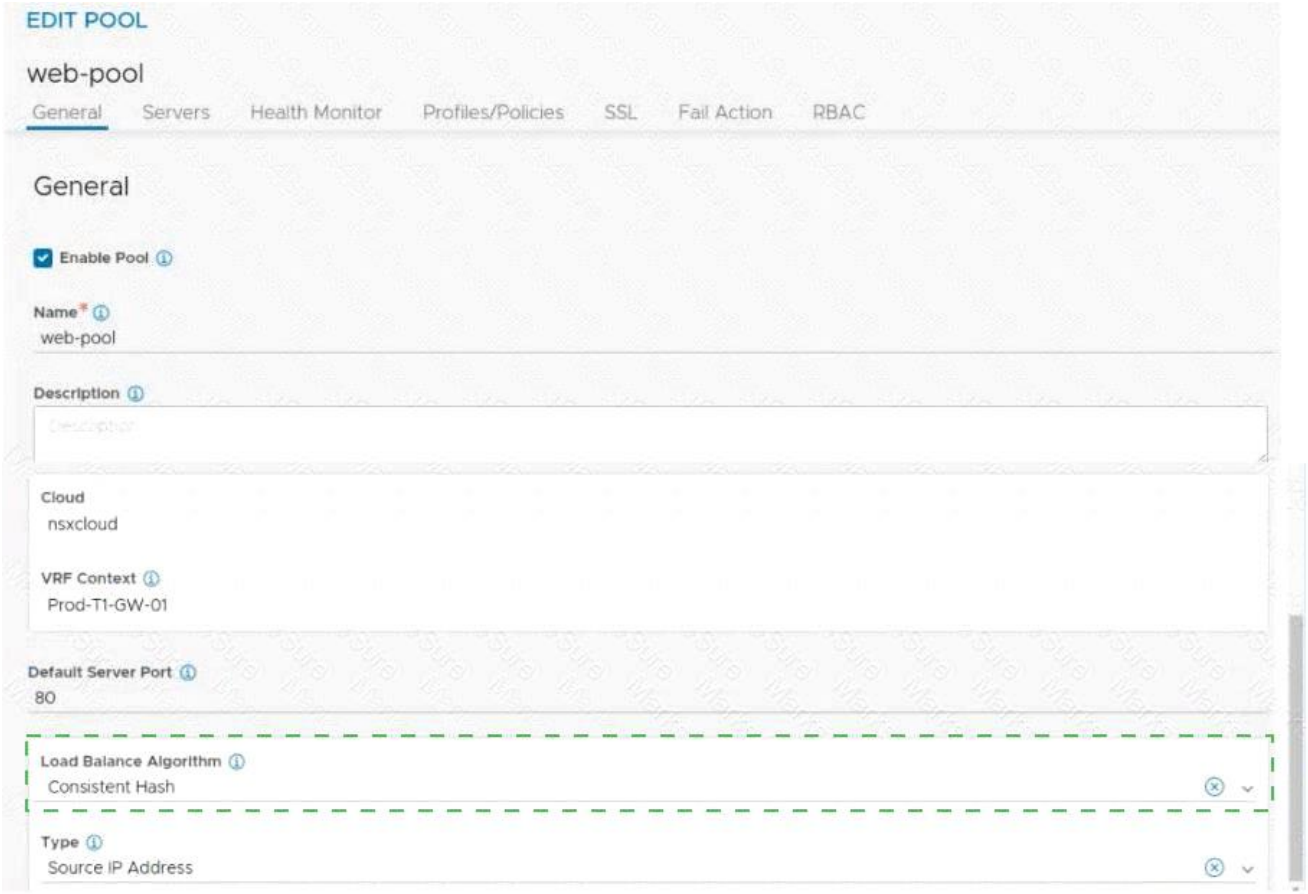
SecurID, and RADIUS. An OAuth Client is a configuration entity in vIDM that represents an application that can use vIDM for authentication and authorization. NSX Manager must be registered as an OAuth Client in vIDM before it can use
2FA. References: : VMware NSX-T Data Center Installation Guide, page 19. : VMware NSX-T Data Center Administration Guide, page 102. : VMware Blogs: Two-Factor Authentication with VMware NSX-T

QUESTION NO: 10
管理者は、ネットワーク イントロスペクションのサービス挿入を構成しています。
ネットワーク イントロスペクションを構成できる 2 つの場所はどれですか?
(2つお選びください。)
A. Host pNIC
B. Partner SVM
C. Tier-0 gateway
D. Tier-1 gateway
E. Edge Node
Answer: A B
Explanation:
Network Introspection is a service insertion feature that allows third-party network security services to monitor and analyze the traffic between virtual machines. Network Introspection can be configured on the host pNIC or on the partner SVM, depending on the type of service and the deployment model. The host pNIC configuration is used for services that require traffic redirection from the physical network to the service virtual machine. The partner SVM configuration is used for services that require traffic redirection from the virtual network to the service virtual machine. Network Introspection cannot be configured on the Tier-0 or Tier-1 gateways, as they are not part of the data plane where the service insertion occurs. Network Introspection also cannot be configured on the edge node, as it is a logical construct that hosts the Tier-0 and Tier-1 gateways. References: Distributed Service Insertion, NSX Securing "Anywhere" Part IV

QUESTION NO: 11
展示を参照してください。
管理者は、Web サーバー間でトラフィックを再分散するように NSX Advanced Load Balancer を構成しました。
ただし、リクエストは 1 つのサーバーにのみ送信されます
問題を解決するには、次のプール構成設定のうちどれを調整する必要がありますか?画像をクリックして正解をマークしてください。



Answer:



Explanation:

Load Balancing Algorithm
You specify the following parameters during the creation of a server pool:
* Name: A unique name for the server pool.
* Cloud: The cloud connector details for the NSX environment.
* VRF Context: Virtual Routing Framework (VRF) is a method to isolate traffic in a system. VRF is also called a route domain in the load balancer community. A global VRF context is created by default. Network administrators might create custom VRF contexts to isolate traffic between different tenants or subsets.
* Default Server Port: New connections to servers will use this destination service port. The default port is 80.
* Load-balancing algorithm: The selected load-balancing algorithm controls how the incoming connections are distributed among the servers in the pool.
* Tier-1 gateway (logical router): Specify the Tier-1 gateway that you want to attach the server pool to. This value matches the Tier-1 gateway specified for the virtual service and VIP.