

Exam Questions 2V0-41.23

VMware NSX 4.x Professional

<https://www.2passeasy.com/dumps/2V0-41.23/>



NEW QUESTION 1

An NSX administrator is troubleshooting a connectivity issue with virtual machines running on an ESXi transport node. Which feature in the NSX UI shows the mapping between the virtual NIC and the host's physical adapter?

- A. Port Mirroring
- B. Switch Visualization
- C. Activity Monitoring
- D. IPFIX

Answer: B

Explanation:

According to the VMware NSX Documentation, Switch Visualization is a feature in the NSX UI that shows the mapping between the virtual NIC and the host's physical adapter for virtual machines running on an ESXi transport node. You can use Switch Visualization to view details such as port ID, MAC address, VLAN ID, IP address, MTU, port state, port speed, port type, and port group for each virtual NIC and physical adapter.
<https://docs.vmware.com/en/VMware-NSX/4.1/installation/GUID-55E5C735-18AD-43F8-9BE5-F75D5B8C6E>

NEW QUESTION 2

A company security policy requires all users to log into applications using a centralized authentication system. Which two authentication, authorization, and accounting (AAA) systems are available when integrating NSX with VMware Identity Manager? (Choose two.)

- A. RADIUS 2.0
- B. Keycloak Enterprise
- C. RSA SecurID
- D. LDAP and OpenLDAP based on Active Directory (AD)
- E. SecureDAP

Answer: CD

Explanation:

NSX supports two types of authentication, authorization, and accounting (AAA) systems when integrating with VMware Identity Manager: RSA SecurID and LDAP and OpenLDAP based on Active Directory (AD). RSA SecurID is a two-factor authentication system that uses a token-based approach to verify the identity of users. LDAP and OpenLDAP based on AD are directory services that store and manage user information and credentials. Both systems can be used to provide centralized authentication for users who want to access applications in an NSX environment.
<https://blogs.vmware.com/networkvirtualization/2017/11/remote-user-authentication-and-rbac-with-nsx-t.html>

NEW QUESTION 3

Where in the NSX UI would an administrator set the time attribute for a time-based Gateway Firewall rule?

- A. The option to set time-based rule is a clock icon in the rule.
- B. The option to set time-based rule is a field in the rule itself.
- C. There is no option in the NSX UI.
- D. It must be done via command line interface.
- E. The option to set time-based rule is a clock icon in the policy.

Answer: D

Explanation:

According to the VMware documentation¹, the clock icon appears on the firewall policy section that you want to have a time window. By clicking the clock icon, you can create or select a time window that applies to all the rules in that policy section. The other options are incorrect because they either do not exist or are not related to the time-based rule feature. There is no option to set a time-based rule in the rule itself, as it is a policy-level setting. There is also an option to set a time-based rule in the NSX UI, so it does not require using the command line interface.
<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-8572496E-A60E-48C3-A016-4A081AC8>

NEW QUESTION 4

Where does an administrator configure the VLANs used in VRF Lite? (Choose two.)

- A. segment connected to the Tier-1 gateway
- B. uplink trunk segment
- C. downlink interface of the default Tier-0 gateway
- D. uplink interface of the VRF gateway
- E. uplink interface of the default Tier-0 gateway

Answer: BD

Explanation:

According to the VMware NSX Documentation, these are the two places where you need to configure the VLANs used in VRF Lite:

- Uplink trunk segment: This is a segment that connects a tier-0 gateway to a physical network using multiple VLAN tags. You need to configure the VLAN IDs for each VRF on this segment.
- Uplink interface of the VRF gateway: This is an interface that connects a VRF gateway to an uplink trunk segment using a specific VLAN tag. You need to configure the VLAN ID for each VRF on this interface.

NEW QUESTION 5

An NSX administrator is treating a NAT rule on a Tier-0 Gateway configured in active-standby high availability mode. Which two NAT rule types are supported for this configuration? (Choose two.)

- A. Reflexive NAT
- B. Destination NAT
- C. 1:1 NAT
- D. Port NAT
- E. Source NAT

Answer: BE

Explanation:

According to the VMware NSX Documentation, these are two NAT rule types that are supported for a tier-0 gateway configured in active-standby high availability mode. NAT stands for Network Address Translation and is a feature that allows you to modify the source or destination IP address of a packet as it passes through a gateway.

- Destination NAT: This rule type allows you to change the destination IP address of a packet from an external IP address to an internal IP address. You can use this rule type to provide access to your internal servers from external networks using public IP addresses.
- Source NAT: This rule type allows you to change the source IP address of a packet from an internal IP address to an external IP address. You can use this rule type to provide access to external networks from your internal servers using public IP addresses.

NEW QUESTION 6

Sort the rule processing steps of the Distributed Firewall. Order responses from left to right.

If the packet matches source, destination, service, profile and applied to fields, apply the action defined.	If the rule table action is allow, create an entry in the connection table and forward the packet.	Packet arrives at dvfilter connection table, if matching entry in the table, process the packet.	If the rule table action is reject or deny, take that action.	If connection table has no match, compare the packet to the rule table.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The correct order of the rule processing steps of the Distributed Firewall is as follows:

- Packet arrives at vfilter connection table. If matching entry in the table, process the packet.
- If connection table has no match, compare the packet to the rule table.
- If the rule table action is allow, create an entry in the connection table and forward the packet.
- If the rule table action is reject or deny, take that action.

This order is based on the description of how the Distributed Firewall works in the web search results¹. The first step is to check if there is an existing connection entry for the packet in the vfilter connection table, which is a cache of flow entries for rules with an allow action. If there is a match, the packet is processed according to the connection entry. If there is no match, the packet is compared to the rule table, which contains all the security policy rules. The rules are evaluated from top to bottom until a match is found. The match criteria include source, destination, service, profile and applied to fields. The action defined by the matching rule is applied to the packet. The action can be allow, reject or deny. If the action is allow, a new connection entry is created for the packet and the packet is forwarded to its destination. If the action is reject or deny, the packet is dropped and an ICMP message or a TCP reset message is sent back to the source.

NEW QUESTION 7

Which CLI command is used for packet capture on the ESXi Node?

- A. tcpdump
- B. debug
- C. pktcap-uw
- D. set capture

Answer: C

Explanation:

According to the VMware Knowledge Base, this CLI command is used for packet capture on the ESXi node. pktcap-uw stands for Packet Capture User World and is a tool that allows you to capture packets from various points in the network stack of an ESXi host. You can use this tool to troubleshoot network issues or analyze traffic flows.

The other options are either incorrect or not available for this task. tcpdump is not a valid CLI command for packet capture on the ESXi node, as it is a tool that runs on Linux systems, not on ESXi hosts. debug is not a valid CLI command for packet capture on the ESXi node, as it is a generic term that describes the process of finding and fixing errors, not a specific tool or command. set capture is not a valid CLI command for packet capture on the ESXi node, as it does not exist in the ESXi CLI.

NEW QUESTION 8

Which three of the following describe the Border Gateway Routing Protocol (BGP) configuration on a Tier-0 Gateway? (Choose three.)

- A. Can be used as an Exterior Gateway Protocol.
- B. It supports a 4-byte autonomous system number.
- C. The network is divided into areas that are logical groups.
- D. EIGRP Is disabled by default.
- E. BGP is enabled by default.

Answer: ABD

Explanation:

- * A. Can be used as an Exterior Gateway Protocol. This is correct. BGP is a protocol that can be used to exchange routing information between different autonomous systems (AS). An AS is a network or a group of networks under a single administrative control. BGP can be used as an Exterior Gateway Protocol (EGP) to connect an AS to other ASes on the internet or other external networks¹
- * B. It supports a 4-byte autonomous system number. This is correct. BGP supports both 2-byte and 4-byte AS numbers. A 2-byte AS number can range from 1 to 65535, while a 4-byte AS number can range from 65536 to 4294967295. NSX supports both 2-byte and 4-byte AS numbers for BGP configuration on a Tier-0 Gateway²
- * C. The network is divided into areas that are logical groups. This is incorrect. This statement describes OSPF, not BGP. OSPF is another routing protocol that operates within a single AS and divides the network into areas to reduce routing overhead and improve scalability. BGP does not use the concept of areas, but rather uses attributes, policies, and filters to control the routing decisions and traffic flow³
- * D. FIGRP Is disabled by default. This is correct. FIGRP stands for Fast Interior Gateway Routing Protocol, which is an enhanced version of IGRP, an obsolete routing protocol developed by Cisco. FIGRP is not supported by NSX and is disabled by default on a Tier-0 Gateway.
- * E. BGP is enabled by default. This is incorrect. BGP is not enabled by default on a Tier-0 Gateway. To enable BGP, you need to configure the local AS number and the BGP neighbors on the Tier-0 Gateway using the NSX Manager UI or API.

To learn more about BGP configuration on a Tier-0 Gateway in NSX, you can refer to the following resources:

- VMware NSX Documentation: Configure BGP ¹
- VMware NSX 4.x Professional: BGP Configuration
- VMware NSX 4.x Professional: BGP Troubleshooting

NEW QUESTION 9

Which choice is a valid insertion point for North-South network introspection?

- A. Guest VM vNIC
- B. Partner SVM
- C. Tier-0 gateway
- D. Host Physical NIC

Answer: C

Explanation:

A valid insertion point for North-South network introspection is Tier-0 gateway. North-South network introspection is a service insertion feature that allows third-party network services to be integrated with NSX. North-South network introspection enables traffic redirection from the uplink of an NSX Edge node to a service chain that consists of one or more service profiles¹. The Tier-0 gateway is the logical router that connects the NSX Edge node to the physical network and provides North-South routing and network services².

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-D5933474-34A2-4DCE-AE9B-A82FF33>

NEW QUESTION 10

What are two functions of the Service Engines in NSX Advanced Load Balancer? (Choose two.)

- A. It collects real-time analytics from application traffic flows.
- B. It stores the configuration and policies related to load-balancing services.
- C. It performs application load-balancing operations.
- D. It deploys web servers to perform load-balancing operations.
- E. It provides a user interface to perform configuration and management tasks.

Answer: CE

Explanation:

The Service Engines in NSX Advanced Load Balancer are VM-based applications that handle all data plane operations by receiving and executing instructions from the Controller. The Service Engines perform the following functions:

- They perform application load-balancing operations for all client- and server-facing network interactions. They support various load-balancing algorithms, health monitors, SSL termination, and persistence profiles.
 - They provide a user interface to perform configuration and management tasks. The user interface is accessible through a web browser or a REST API. The user interface allows the user to create and modify virtual services, pools, health monitors, policies, analytics, and other load-balancing settings
- <https://docs.vmware.com/en/VMware-Telco-Cloud-Platform/3.0/vmware-telco-cloud-reference-architecture-gui>

NEW QUESTION 10

An architect receives a request to apply distributed firewall in a customer environment without making changes to the network and vSphere environment. The architect decides to use Distributed Firewall on VDS.

Which two of the following requirements must be met in the environment? (Choose two.)

- A. vCenter 8.0 and later
- B. NSX version must be 3.2 and later
- C. NSX version must be 3.0 and later
- D. VDS version 6.6.0 and later

Answer: BD

Explanation:

Distributed Firewall on VDS is a feature of NSX-T Data Center that allows users to install Distributed Security for vSphere Distributed Switch (VDS) without the need to deploy an NSX Virtual Distributed Switch (N-VDS). This feature provides NSX security capabilities such as Distributed Firewall (DFW), Distributed IDS/IPS, Identity Firewall, L7 App ID, FQDN Filtering, NSX Intelligence, and NSX Malware Prevention. To enable this feature, the following requirements must be met in the environment:

- The NSX version must be 3.2 and later¹. This is the minimum version that supports Distributed Security for VDS.
- The VDS version must be 6.6.0 and later¹. This is the minimum version that supports the NSX host preparation operation that activates the DFW with the default rule set to allow.

References:

- Overview of NSX IDS/IPS and NSX Malware Prevention

NEW QUESTION 11

Which troubleshooting step will resolve an error with code 1001 during the configuration of a time-based firewall rule?

- A. Reinstalling the NSX VIBs on the ESXi host.
- B. Restarting the NTPservice on the ESXi host.
- C. Changing the lime zone on the ESXi host.
- D. Reconfiguring the ESXi host with a local NTP server.

Answer: B

Explanation:

According to the web search results, error code 1001 is related to a time synchronization issue between the ESXi host and the NSX Manager. This can cause problems when configuring a time-based firewall rule, which requires the ESXi host and the NSX Manager to have the same time zone and NTP server settings . To resolve this error, you need to restart the NTP service on the ESXi host to synchronize the time with the NSX Manager. You can use the following command to restart the NTP service on the ESXi host:

```
/etc/init.d/ntpd restart
```

The other options are not valid solutions for this error. Reinstalling the NSX VIBs on the ESXi host will not fix the time synchronization issue. Changing the time zone on the ESXi host may cause more discrepancies with the NSX Manager. Reconfiguring the ESXi host with a local NTP server may not be compatible with the NSX Manager's NTP server.

NEW QUESTION 16

Which two are requirements for FQDN Analysis? (Choose two.)

- A. The NSX Edge nodes require access to the Internet to download category and reputation definitions.
- B. ESXi control panel requires access to the Internet to download category and reputation definitions.
- C. The NSX Manager requires access to the Internet to download category and reputation definitions.
- D. A layer 7 gateway firewall rule must be configured on the Tier-1 gateway uplink.
- E. A layer 7 gateway firewall rule must be configured on the Tier-0 gateway uplink.

Answer: AD

Explanation:

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-C5CD87FD-8095-49F3-97CE-E606AB89>

NEW QUESTION 20

Which CLI command shows syslog on NSX Manager?

- A. get log-file auth.lag
- B. /var/log/syslog/syslog.log
- C. show log manager follow
- D. get log-file syslog

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
```

NEW QUESTION 22

Which command on ESXi is used to verify the Local Control Plane connectivity with Central Control Plane?

- A)

```
esxcli network ip connection list | grep netcpa
```
- B)

```
esxcli network ip connection list | grep 1234
```
- C)

```
esxcli network ip connection list | grep ccpd
```
- D)

```
esxcli network ip connection list | grep 1235
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: B

Explanation:

According to the web search results, the command that is used to verify the Local Control Plane (LCP) connectivity with Central Control Plane (CCP) on ESXi is get control-cluster status. This command displays the status of the LCP and CCP components on the ESXi host, such as the LCP agent, CCP client, CCP server, and CCP connection. It also shows the IP address and port number of the CCP server that the LCP agent is connected to. If the LCP agent or CCP client are not running or not connected, it means that there is a problem with the LCP connectivity .

NEW QUESTION 25

Which of the two following characteristics about NAT64 are true? (Choose two.)

- A. NAT64 is stateless and requires gateways to be deployed in active-standby mode.
- B. NAT64 is supported on Tier-1 gateways only.
- C. NAT64 is supported on Tier-0 and Tier-1 gateways.
- D. NAT64 requires the Tier-1 gateway to be configured in active-standby mode.
- E. NAT64 requires the Tier-1 gateway to be configured in active-active mode.

Answer: CD

Explanation:

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-69604E49-BC8B-4777-BFD8-B98F8D1F>

NEW QUESTION 28

An administrator has a requirement to have consistent policy configuration and enforcement across NSX instances. What feature of NSX fulfills this requirement?

- A. Load balancer
- B. Federation
- C. Multi-hypervisor support
- D. Policy-driven configuration

Answer: B

Explanation:

Federation is a feature of NSX that allows the administrator to manage multiple NSX instances with a single pane of glass view, create gateways and segments that span one or more locations, and configure and enforce firewall rules consistently across locations¹. Federation provides centralized policy management for security and networking services for all locations and pushes it down to NSX Local Managers at the respective sites for enforcement¹. Federation also enables disaster recovery and workload mobility scenarios by providing consistent network and security policies across different sites¹. References: 1: NSX Federation - VMware Docs(<https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.2/administration/GUID-D5B6DC79-6733-44>)

NEW QUESTION 30

Which VPN type must be configured before enabling a L2VPN?

- A. Route-based IPsec VPN
- B. Policy based IPsec VPN
- C. SSL-based IPsec VPN
- D. Port-based IPsec VPN

Answer: A

Explanation:

According to the VMware NSX Documentation, this VPN type must be configured before enabling a L2VPN. L2VPN stands for Layer 2 VPN and is a feature that allows you to extend your layer 2 network across different sites using an IPsec tunnel. Route-based IPsec VPN is a VPN type that uses logical router ports to establish IPsec tunnels between sites.

<https://docs.vmware.com/en/VMware-NSX/4.1/administration/GUID-86C8D6BB-F185-46DC-828C-1E1876B8>

NEW QUESTION 34

As part of an organization's IT security compliance requirement, NSX Manager must be configured for 2FA (two-factor authentication). What should an NSX administrator have ready before the integration can be configured? O

- A. Active Directory LDAP integration with OAuth Client added
- B. VMware Identity Manager with an OAuth Client added
- C. Active Directory LDAP integration with ADFS
- D. VMware Identity Manager with NSX added as a Web Application

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

NEW QUESTION 37

An NSX administrator wants to create a Tier-0 Gateway to support equal cost multi-path (ECMP) routing. Which failover detection protocol must be used to meet this requirement?

- A. Bidirectional Forwarding Detection (BFD)
- B. Virtual Router Redundancy Protocol (VRRP)
- C. Beacon Probing (BP)
- D. Host Standby Router Protocol (HSRP)

Answer: A

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, BFD is a failover detection protocol that provides fast and reliable detection of link failures between two routing devices. BFD can be used with ECMP routing to monitor the health of the ECMP paths and trigger a route change in case of a failure¹². BFD is supported by both BGP and OSPF routing protocols in NSX-T3. BFD can also be configured with different timers to achieve different detection times³.

NEW QUESTION 38

Which three selections are capabilities of Network Topology? (Choose three.)

- A. Display how the different NSX components are interconnected.
- B. Display the uplink configured on the Tier-0 Gateways.
- C. Display how the Physical components are interconnected.
- D. Display the VMs connected to Segments.
- E. Display the uplinks configured on the Tier-1 Gateways.

Answer: ABD

Explanation:

According to the VMware NSX Documentation, these are three of the capabilities of Network Topology, which is a graphical representation of your network infrastructure in NSX:

- Display how the different NSX components are interconnected: You can use Network Topology to view how your segments, gateways, routers, firewalls, load balancers, VPNs, and other NSX components are connected and configured in your network.
- Display the uplink configured on the Tier-0 Gateways: You can use Network Topology to view the uplink interface and segment that connect your tier-0 gateways to your physical network. You can also view the VLAN ID and IP address of the uplink interface.
- Display the VMs connected to Segments: You can use Network Topology to view the VMs that are attached to your segments. You can also view the IP address and MAC address of each VM.

NEW QUESTION 42

How is the RouterLink port created between a Tier-1 Gateway and Tier-0 Gateway?

- A. Manually create a Logical Switch and connect to both Tier-1 and Tier-0 Gateways.
- B. Automatically created when Tier-1 is created.
- C. Manually create a Segment and connect to both Tier-1 and Tier-0 Gateways.
- D. Automatically created when Tier-1 is connected with Tier-0 from NSX UI.

Answer: D

Explanation:

According to the VMware NSX 4.x Professional documents and tutorials, a RouterLink port is a logical port that connects a Tier-1 gateway to a Tier-0 gateway. This port is automatically created when a Tier-1 gateway is associated with a Tier-0 gateway from the NSX UI or API. The RouterLink port enables routing between the two gateways and carries all the routing protocols and traffic. There is no need to manually create a logical switch or segment for this purpose¹.

NEW QUESTION 43

When running nsxcli on an ESXi host, which command will show the Replication mode?

- A. get logical-switch <Local-Switch-UUID> status
- B. get logical-switch <Logical-Switch-UUID>
- C. get logical-switches
- D. get logical-switch status

Answer: B

NEW QUESTION 44

Which statement is true about an alarm in a Suppressed state?

- A. An alarm can be suppressed for a specific duration in seconds.
- B. An alarm can be suppressed for a specific duration in days.
- C. An alarm can be suppressed for a specific duration in minutes.
- D. An alarm can be suppressed for a specific duration in hours.

Answer: D

Explanation:

The answer is D. An alarm can be suppressed for a specific duration in hours.

According to the VMware NSX documentation, an alarm can be in one of the following states: Open, Acknowledged, Suppressed, or Resolved¹².

An alarm in a Suppressed state means that the status reporting for this alarm has been disabled by the user for a user-specified duration¹²
When a user moves an alarm into a Suppressed state, they are prompted to specify the duration in hours. After the specified duration passes, the alarm state reverts to Open. However, if the system determines the condition has been corrected, the alarm state changes to Resolved¹³
To learn more about how to manage alarm states in NSX, you can refer to the following resources:

- VMware NSX Documentation: Managing Alarm States 1
- VMware NSX Documentation: View Alarm Information 2
- VMware NSX Intelligence Documentation: Manage NSX Intelligence Alarm States 3 <https://docs.vmware.com/en/VMware-NSX-Intelligence/1.2/user-guide/GUID-EBD3C5A8-F9AB-4A22-BA40->

NEW QUESTION 46

An administrator has been tasked with implementing the SSL certificates for the NSX Manager Cluster VIP. Which is the correct way to implement this change?

- A. Send an API call to `https://<nsx-mgr>/api/v1/cluster/api-certificate? action=set_cluster_certificate&certificate_id=<certificate_id>`
B. Send an API call to `https://<nsx-mgr>/api/v1/node/services/http? action=apply_certificate&certificate_id=<certificate_id>`
C. SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate vip install<certificate_id>`
D. SSH as admin into the NSX manager with the cluster VIP IP and run `nsxcli cluster certificate node install <certificate_id>`

Answer: A

Explanation:

<https://docs.vmware.com/en/VMware-Validated-Design/5.0.1/com.vmware.vvd.sddc-nsxt-domain-deploy.doc/G>

NEW QUESTION 51

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 2V0-41.23 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 2V0-41.23 Product From:

<https://www.2passeasy.com/dumps/2V0-41.23/>

Money Back Guarantee

2V0-41.23 Practice Exam Features:

- * 2V0-41.23 Questions and Answers Updated Frequently
- * 2V0-41.23 Practice Questions Verified by Expert Senior Certified Staff
- * 2V0-41.23 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 2V0-41.23 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year