Exam Questions jn0-634

Security, Professional (JNCIP-SEC)

https://www.2passeasy.com/dumps/jn0-634/

NEW QUESTION 1
Which statement about transparent mode on an SRX340 is true?

A. You must reboot the device after configuring transparent mode.
B. Security policies applied to transparent mode zones require Layer 2 address matching.
C. Screens are not supported in transparent mode security zones.
D. All interfaces on the device must be configured with the ethernet-switching protocol family.

Answer: A

NEW QUESTION 2
Click the Exhibit button.

```
user@host# show security idp
idp-policy base-policy {
     rulebase-ips {
          rule R1 {
               match {
                    from-zone trust;
                    source-address any;
                    to-zone untrust;
                    destination-address any;
                    application default;
                    attacks {
                         predefined-attack-groups HTTP-Critical;
                    }
               }
               then {
                    action {
                         mark-diffserv {
                              10;
                         }
                    }
               }
          }
     }
}
```

Referring to the security policy shown in the exhibit, which two actions will happen as the packet is processed? (Choose two.)

A. It passes unmatched traffic after modifying the DSCP priority.
B. It marks and passes matched traffic with a high DSCP priority.
C. It marks and passes matched traffic with a low DSCP priority.
D. It passes unmatched traffic without modifying DSCP priority.

Answer: BD

NEW QUESTION 3
Click the Exhibit button.

```
[edit security utm]
user@host# show
custom-objects {
     url-pattern {
          allow {
               value "user@example.com";
          }
          reject {
               value "user@example.com";
          }
     }
}
feature-profile {
     anti-spam {
          address-whitelist allow;
          address-blacklist reject;
          sbl {
               profile AS {
                    sbl-default-server;
                    spam-action block;
                    custom-tag-string SPAM;
               }
          }
     }
}
```

Referring to the exhibit, which statement is true?

A. E-mails from the user@example.com address are marked with SPAM in the subject line by the spam block list server.
B. E-mails from the user@example.com address are blocked by the spam list server.
C. E-mails from the user@example.com address are blocked by the reject blacklist.
D. E-mails from the user@example.com address are allowed by the allow whitelist.

Answer: D

NEW QUESTION 4
Your manager has identified that employees are spending too much time posting on a social media site. You are asked to block user from posting on this site, but they should still be able to access any other site on the Internet.
In this scenario, which AppSecure feature will accomplish this task?

A. AppQoS
B. AppTrack
C. APpFW
D. APBR

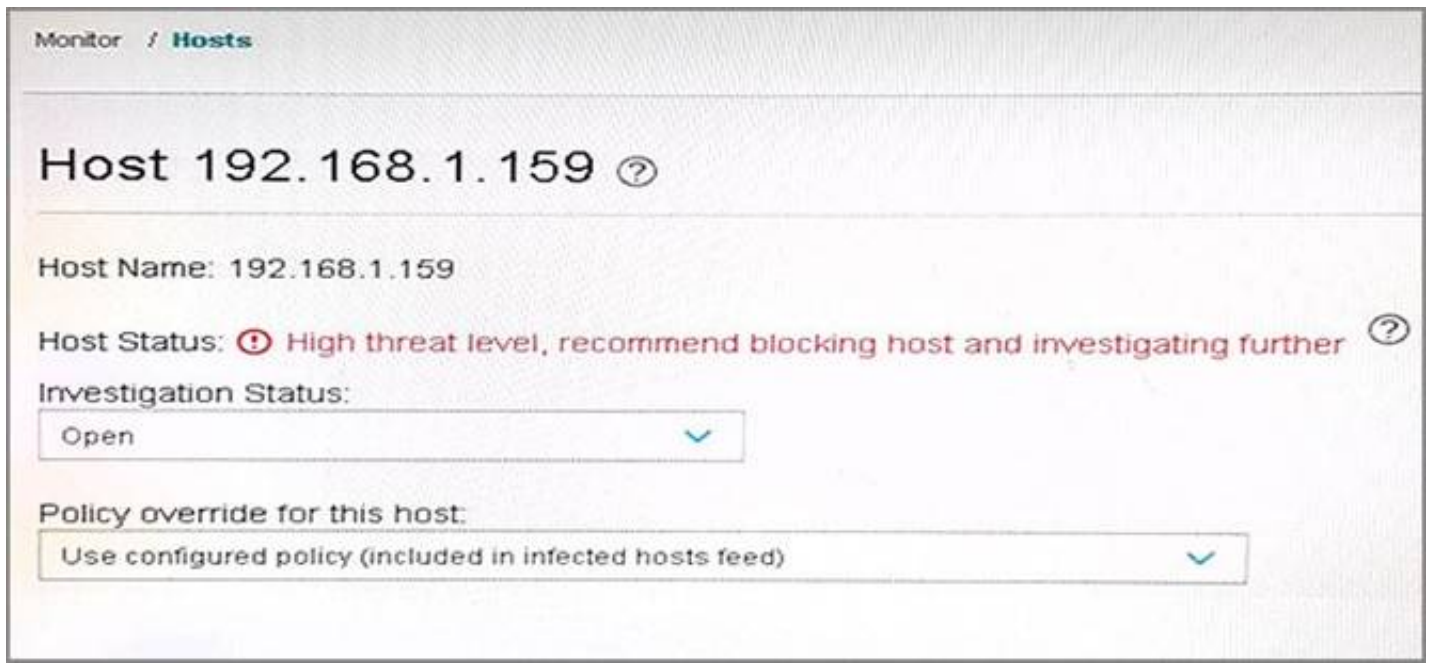
Answer: C

NEW QUESTION 5
While reviewing the Log and Reporting portion of Security Director, you find that multiple objects reference the same address. You want to use a standardized name for all of the objects.
In this scenario, how would you create a standardized object name without searching the entire policy?

A. Remove the duplicate objects.
B. Merge the duplicate objects.
C. Rename the duplicate objects.
D. Replace the duplicate objects.

Answer: B

NEW QUESTION 6
Click the Exhibit button.



Referring to the exhibit, the host has been automatically blocked from communicating on the network because a malicious file was downloaded. You cleaned the infected host and changed the investigation status to Resolved – Fixed.
What does Sky ATP do if the host then attempts to download a malicious file that would result in a threat score of 10?

A. Sky ATP does not log the connection attempt and an SRX Series device does not allow the host to communicate on the network.
B. Sky ATP logs the connection attempt and an SRX Series device does not allow the host to communicate on the network.
C. Sky ATP logs the connection attempt and an SRX Series device allows the host to communicate on the network.
D. Sky ATP does not log the connection attempt and an SRX Series device allows the host to communicate on the network.

Answer: C

NEW QUESTION 7
Click the Exhibit button.

```
[edit]
user@host# show security policies from-zone internet to-zone dmz
policy dmz-poll {
     match {
          source-address any;
          destination-address any;
          application any;
     }
     then {
          permit {
               application-services {
                    idp;
               }
          }
          log {
               session-close;
          }
     }
}

[edit]
user@host# show security idp
idp-policy idp-poll {
     rulebase-ips {
          rule r1 {
               match {
                    attacks {
                         predefined-attack-groups "HTTP All";
                    }
               }
               then {
                    action {
                         ignore-connection;
                    }
               }
          }
          rule r2 {
               match {
                    attacks {
                         predefined-attack-groups "DNS All";
                    }
               }
               then {
                    action {
                         close-server;
                    }
                    ip-action {
                         ip-notify;
                    }
               }
          }
     }
}
```

Referring to the configuration shown in the exhibit, which statement explains why traffic matching the IDP signature DNS:OVERFLOW:TOO-LONG-TCP-MSG is not being stopped by the SRX Series device?

A. The security policy dmz-pol1 has an action of permit.
B. The IDP policy idp-pol1 is not configured as active.
C. The IDP rule r2 has an ip-action value of notify.
D. The IDP rule r1 has an action of ignore-connection.

Answer: B

NEW QUESTION 8
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high available chassis cluster and are configured for IPS. There has been a node failover.
In this scenario, which two statements are true? (Choose two.)

A. The IP action table is synchronized between the chassis cluster nodes.
B. Cached SSL session ID information for existing sessions is not synchronized between nodes.
C. The IP action table is not synchronized between the chassis cluster nodes.
D. Cached SSL session ID information for existing session is synchronized between nodes.

Answer: CD

NEW QUESTION 9
After downloading the new IPS attack database, the installation of the new database fails. What caused this condition?

A. The new attack database no longer contained an attack entry that was in use.
B. The new attack database was revoked between the time it was downloaded and installed.
C. The new attack database was too large for the device on which it was being installed.
D. Some of the new attack entries were already in use and had to be deactivated before installation.

Answer: A

NEW QUESTION 10
Click the Exhibit button.

```
policy allow-all {
     match {
          source-address any;
          destination-address any;
          application any;
     }
     then {
          permit {
               application-services {
                    idp;
                    utm-policy wf-policy_websense-home;
                    application-firewall {
                         rule-set demo-tracking_1;
                    }
               }
               log {
                    session-init;
                    session-close;
               }
          }
     }
}
```

According to the policy shown in the exhibit, which application-services traffic will be processed first?

A. the application traffic matchings the IDP rules
B. the application traffic matchings the utm-policy log rule set
C. the application traffic matchings the utm-policy wf-policy_websense-home rules
D. the application traffic matchings the application-firewall rule-set demo-tracking_1 rule

Answer: A

NEW QUESTION 10
You are using the integrated user firewall feature on an SRX Series device.
Which three parameters are stored in the Active Directory authentication table? (Choose three.)

A. IP address
B. MAC address
C. group mapping
D. username
E. password

Answer: ACD

NEW QUESTION 12
Click the Exhibit button.

```
[edit security policies global policy int-FW]
user@host# show
match {
     source-address any;
     destination-address any;
     application any;
}
then {
     permit;
}

user@host> show security user-identification local-authentication-table all

user@host>
```

You have configured integrated user firewall on the SRX Series devices in your network. However, you noticed that no users can access the servers that are behind the SRX Series devices.
Referring to the exhibit, what is the problem?

A. The Kerberos service is not configured correctly on the Active Directory server.
B. There are no authentication entries in the SRX Series device for the users.

C. The security policy on the SRX Series device is configured incorrectly.
D. The SAML service is not configured correctly on the Active Directory server.

Answer: C

NEW QUESTION 14
What are three types of content that are filtered by the Junos UTM feature set? (Choose three.)

A. IMAP
B. HTTP
C. SIP
D. SSL
E. FTP

Answer: ABE

NEW QUESTION 17
Click the Exhibit button.

```
[edit]
user@host# show security application-tracking
first-update-interval 1;

[edit]
user@host# show security zones security-zone trust
tcp-rst;
host-inbound-traffic {
     system-services {
          all;
     }
}
interfaces {
     ge-0/0/2.0;
}
application-tracking;
```

Referring to the exhibit, how many AppTrack logs will be generated for an HTTP session lasting 12 minutes?

A. 4
B. 2
C. 1
D. 3

Answer: A

NEW QUESTION 21
Click the Exhibit button.

```
[edit services advanced-anti-malware policy SKY_policy1]
user@host# show
match {
     application HTTP;
     verdict-threshold 6;
}
then {
     action block;
     notification {
          log;
     }
}
inspection-profile Test_Profile;
fallback-options {
     action permit;
     notification {
          log;
     }
}
default-notification {
     log;
}
whitelist-notification {
     log;
}
blacklist-notification {
     log;
}
```

Referring to the exhibit, you have configured a Sky ATP policy to inspect user traffic. However, you have noticed that encrypted traffic is not being inspected.
In this scenario, what must you do to solve this issue?

A. Change the policy to inspect HTTPS traffic.
B. Configure the PKI feature.
C. Configure the SSL forward proxy feature.
D. Change the policy to inspect TLS traffic.

Answer: C

NEW QUESTION 23
Your network includes SRX Series devices at all headquarter, data center, and branch locations. The headquarter and data center locations use high-end SRX Series devices, and the branch locations use branch SRX Series devices. You are asked to deploy IPS on the SRX Series devices using one of the available IPS deployment modes.
In this scenario, which two statements are true? (Choose two.)

A. Inline tap mode provides enforcement.
B. Inline tap mode can be used at all locations.
C. Integrated mode can be used at all locations.
D. Integrated mode provides enforcement.

Answer: CD

NEW QUESTION 27
Click the Exhibit button.

```
[edit]
user@host# show interfaces ge-0/0/4
unit 0 {
     family ethernet-switching {
          interface-mode access;
          vlan {
               members SV;
          }
     }
}

[edit]
user@host# show interfaces ge-0/0/5
unit 0 {
     family ethernet-switching {
          interface-mode access;
          vlan {
               members SV;
          }
     }
}

[edit]
user@host# show vlans
SV {
     vlan-id 101;
}

[edit]
user@host# show security forwarding-options
secure-wire {
     access-sw {
          interface [ ge-0/0/4 ge-0/0/5 ];
     }
}

[edit]
user@host# commit
[edit security forwarding-options secure-wire access-sw]
     'interface ge-0/0/4'
          Interface name ge-0/0/4 is not valid
[edit security forwarding-options secure-wire access-sw]
     'interface ge-0/0/4'
          Error: two and only two logical interfaces are required for a
secure-wire
error: configurartion check-out failed
```

You are trying to implement secure wire on your SRX Series device. However, you are receiving the commit error shown in the exhibit.
What must you do to solve the problem?

A. Add the correct logical units to the interfaces in the secure wire.
B. Put the ge-0/0/4 and ge-0/0/5 interfaces in separate secure wires.
C. Change the Ethernet switching mode from access to trunk for the ge-0/0/4 and ge-0/0/5 interfaces.
D. Add the ge-0/0/4 and ge-0/0/5 interfaces to the SV VLAN.

Answer: A

NEW QUESTION 31
Which browser is supported by Security Director with Logging and Reporting?

A. Firefox
B. Agora
C. PowerBrowser
D. Mosaic

Answer: A

NEW QUESTION 34
Click the Exhibit button.

```
[edit]
user@host# show interfaces
ge-0/0/3 {
     unit 0 {
          family inet {
               address 10.1.1.1/24;
          }
     }
}
ge-0/0/4 {
     unit 0 {
          family ethernet-switching {
               interface-mode access;
               vlan;
                    members SV;
               }
          }
     }
}
ge-0/0/5 {
     unit 0 {
          family ethernet-switching {
               interface-mode access;
               vlan {
                    members SV;
               }
          }
     }
}
irb {
     unit 0 {
          family inet {
               address 172.20.101.101/24;
          }
     }
}

[edit]
user@host# show vlans
SV {
     vlan-id 101;
     13-interface irb.0;
}

[edit]
user@host# show security zones security-zone L2
interfaces {
     irb.0;
}

[edit]
user@host# show security polciies

[edit]
user@host#

[edit]
user@host# run show ethernet-switching global-information
Global Configuration:

MAC aging interval       : 300
MAC learning             : Enabled
MAC statistics           : Disabled
MAC limit Count          : 65535
MAC limit hit            : Disabled
MAC packet action drop   : Disabled
LE aging time            : 1200
LE VLAN aging time       : 1200
Global Mode              : Transparent bridge
```

Two hosts on the same subnet are connected to an SRX340 using interfaces ge-0/0/4 and ge-0/0/5. The two hosts can communicate with each other, but they cannot communicate with hosts outside of their subnet. Referring to the exhibit, which three actions would you take to solve this problem? (Choose three.)

A. Add the ge-0/0/4 and ge-0/0/5 interfaces to the L2 zone.
B. Remove the irb.0 interface from the L2 zone.
C. Set the SRX340 to Ethernet switching mode.
D. Configure a security policy to permit the traffic.
E. Reboot the SRX340.

Answer: CDE

NEW QUESTION 36
You are creating an IPS policy with multiple rules. You want traffic that matches rule 5 to silently be dropped, along with any future packets that match the appropriate attributes of the incoming traffic.
In this scenario, which ip-action parameter should you use?

A. ip-block
B. ip-close
C. log-create
D. timeout

Answer: A

NEW QUESTION 40
You have been notified by your colocation provider that your infrastructure racks will no longer be adjacent to each other.
In this scenario, which technology would you use to secure all Layer 2 and Layer 3 traffic between racks?

A. IPsec
B. GRE
C. 802.1BR
D. MACsec

Answer: D

NEW QUESTION 41
Which IDP rule configuration will send an RST to any new session that meets the action criteria?

A. ip-action block
B. action close-client-and-server
C. ip-action close
D. action drop-connection

Answer: C

NEW QUESTION 43
Using content filtering on an SRX Series device, which three types of HTTP content are able to be blocked? (Choose three.)

A. PDF files
B. ZIP files
C. Java applets
D. Active X
E. Flash

Answer: BCD

NEW QUESTION 44
A customer has recently deployed a next-generation firewall, sandboxing software, cloud access security brokers (CASB), and endpoint protection.
In this scenario, which tool would provide the customer with additional attack prevention?

A. Junos Space Cross Provisioning Platform
B. Contrail
C. Security Director Policy Enforcer
D. Network Director Inventory Manager

Answer: C

NEW QUESTION 45
To which three UTM components would the custom-objects parameter apply? (Choose three.)

A. Sky ATP
B. antispam
C. content filtering
D. antivirus
E. Web filtering

Answer: BCE

NEW QUESTION 47
SRX Series devices with AppSecure support which three custom signatures? (Choose three.)

A. MAC address-based mapping
B. latency detection mapping
C. IP protocol-based mapping
D. ICMP-based mapping
E. Layer 7-based signatures

Answer: CDE

NEW QUESTION 49
Which two statements about enabling MACsec using static CAK security mode keys are true? (Choose two.)

A. CAK secures the data plane traffic.
B. SAK secures the data plane traffic.
C. SAK secures the control plane traffic.
D. CAK secures the control plane traffic.

Answer: BD

NEW QUESTION 50
You need to add all of the sites in the domain example.com to urllist2. You decide to use wildcards to account for any changes made to the domain in the future. In this scenario, which two commands would you use to meet this requirement? (Choose two.)

A. set custom-objects url-pattern urllist2 value http://*.example.com
B. set custom-objects url-pattern urllist2 value http://*example.com
C. set custom-objects url-pattern urllist2 value http://*.example.???
D. set custom-objects url-pattern urllist2 value http://*.example.*

Answer: AC

NEW QUESTION 51
Which two statements about the integrated user firewall feature of the Junos OS are true? (Choose two.)

A. The maximum number of supported active directory servers is ten.
B. IPv6 addresses are not supported.
C. The maximum number of supported active directory servers is five.
D. IPv6 addresses are supported.

Answer: AB

NEW QUESTION 52
Which feature of Sky ATP is deployed with Software-Defined Secure Networks?

A. zero-day threat mitigation
B. software image snapshot support
C. device inventory management
D. service redundancy daemon configuration support

Answer: A

NEW QUESTION 56
Click the Exhibit button.

```
user@host# show security advance-policy-based-routing
profile profile1 {
     rule rule-app1 {
          match {
               dynamic-application junos:HTTP;
          }
          then {
               routing-instance R1;
          }
     }
     rule rule-app2 {
          match {
               dynamic-application junos:junos:web:social-networking;
          }
          then {
               routing-instance R2;
          }
     }
     rule rule-app3 {
          match {
               dynamic-application junos:YAHOO;
          }
          then {
               routing-instance R3;
          }
     }
}
```

Your organization requests that you direct Facebook traffic out a different link to ensure that the bandwidth for critical applications is protected. Referring to the exhibit, which forwarding instance will be used on your SRX Series device?

A. R3
B. R1
C. R2
D. inet.0

Answer: C

NEW QUESTION 58
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are expected to support several UTM features.
Which two statements related to this environment are true? (Choose two.)

A. UTM features can be configured on either of the nodes within the cluster.
B. The chassis cluster must be configured for active/active mode.
C. UTM features must be configured on the primary node within the cluster.
D. The chassis cluster must be configured for active/backup mode.

Answer: AD

NEW QUESTION 62
Click the Exhibit button.

Security Director is reporting the events shown in the exhibit.
If the fallback parameter is set to pass traffic, what would cause the events?

A. The files are too large for the antivirus engine to process.
B. The files are not scanned because they were permitted by a security policy.
C. The files are not scanned because they are the wrong file format.
D. The antivirus engine is unable to re-encrypt the files.

Answer: A

NEW QUESTION 64
Your network includes SRX Series devices at the headquarters location. The SRX Series devices at this location are part of a high availability chassis cluster and are configured for IPS. There has been a node failover.
In this scenario, which statement is true?

A. Existing sessions continue to be processed by IPS because of table synchronization.
B. Existing sessions are no longer processed by IPS and become firewall sessions.
C. Existing session continue to be processed by IPS as long as GRES is configured.
D. Existing sessions are dropped and must be reestablished so IPS processing can occur.

Answer: A

NEW QUESTION 68
What are three components of Software-Defined Secure Networks? (Choose three.)

A. Contrail
B. Sky ATP
C. SRX Series device
D. Security Director
E. Network Director

Answer: BCD

NEW QUESTION 72
Which AppSecure feature identifies applications that are present in traffic?

A. AppID
B. AppTrack
C. AppFW
D. AppQoS

Answer: A

NEW QUESTION 77
Which three components are part of the AppSecure services suite? (Choose three.)

A. IDP
B. Sky ATP
C. AppQoS
D. AppFW
E. Web filtering

Answer: ACD

NEW QUESTION 81
What is a function of UTM?

A. AppFW
B. IPsec
C. content filtering
D. bridge mode

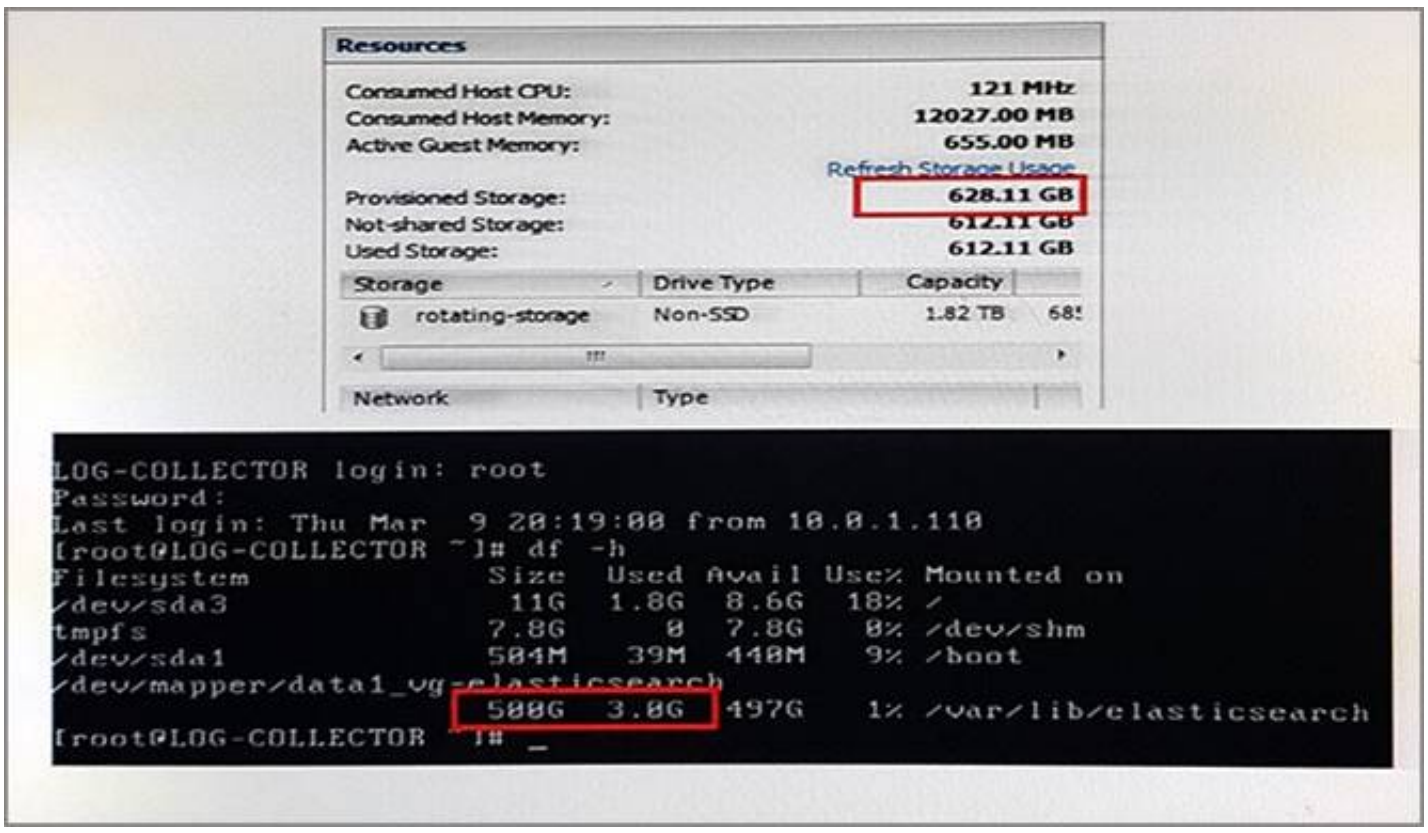
Answer: C

NEW QUESTION 85
You are implementing user authentication on your network using an SRX Series device and want to ensure that there are redundant forms of authentication for users to access the network. You have configured the device with the integrated user firewall and user role firewall features. You are testing failover methods using the default priority values.
In this scenario, which two statements are true? (Choose two.)

A. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with a user role firewall.
B. If the user fails user role firewall authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.
C. If the user fails integrated user firewall authentication, then the Junos OS will attempt toauthenticate with a user role firewall.
D. If the user fails local authentication, then the Junos OS will attempt to authenticate the user with an integrated user firewall.

Answer: CD

NEW QUESTION 87
Click the Exhibit button.



Referring to the exhibit, you have expanded the disk storage size in ESXi for your log collector from 500 GB to 600 GB. However, your log collector's disk size has not changed.
Given the scenario, which two statements are true? (Choose two.)

A. You must run a script from the console to expand the disk size.
B. The ESXi storage parameter is not associated with the Elasticsearch disk size parameter.
C. You must reboot the log collector for storage settings to be updated
D. You must re-run the log collector setup script to update the storage settings.

Answer: AC

NEW QUESTION 91
Your manager has notices a drop in productivity and believes it is due to employees checking their social media feeds too frequently. You are asked to provide analytical statistics for this traffic within your network on an hourly basis.
Which AppSecure feature should be used to collect this information?

A. AppQoS
B. AppFW

C. AppTrack
D. APBR

Answer: C

NEW QUESTION 93
What is the required when deploying a log collector in Junos Space?

A. root user access to the log collector
B. a shared log file directory on the log collector
C. the IP address of interface eth1 on the log collector
D. a distributed deployment of the log collector nodes

Answer: A

NEW QUESTION 94
Using the Policy Controller API, which configuration would post Sky ATP with PE mode to the Policy Enforcer controller configuration?

A. “configs”: {“sdsn”: false“cloudonly”: true}
B. “configs”: {“sdsn”: false“cloud”: false}
C. “configs”: {“sdsn”: true“cloudonly”: false}
D. “configs”: {“sdsn”: false“cloud”: true}

Answer: C

NEW QUESTION 99
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual jn0-634 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the jn0-634 Product From:

https://www.2passeasy.com/dumps/jn0-634/

Money Back Guarantee

jn0-634 Practice Exam Features:

* jn0-634 Questions and Answers Updated Frequently

* jn0-634 Practice Questions Verified by Expert Senior Certified Staff

* jn0-634 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* jn0-634 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year