DUMPSBOSS.

Security, Professional (JNCIP-SEC)

Juniper JN0-634

Version Demo

Total Demo Questions: 10

Total Premium Questions: 65

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

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

Explanation:

https://www.juniper.net/documentation/en_US/junos-space18.4/topics/task/operational/junos-space-addresse-du

QUESTION NO: 2

You have set up Sky ATP with the SRX Series devices in your network. However, your SRX Series devices are unable to communicate with the Sky ATP cloud because the communication is being blocked by a gateway network device.

Which two actions should you take to solve the problem? (Choose two.)

A. Open destination port 443 inbound from the Internet on the gateway network device.

B. Open destination port 8080 outbound from the Internet on the gateway network device.

C. Open destination port 443 outbound from the Internet on the gateway network device.

D. Open destination port 8080 inbound from the Internet on the gateway network device.

ANSWER: C D

QUESTION NO: 3

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: C D E

Explanation:

Security devices support the following types of custom signatures: ICMP-Based Mapping

Address-Based Mapping

IP Protocol-Based Mapping Layer 7-Based Signatures

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-application-identification-

QUESTION NO: 4

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

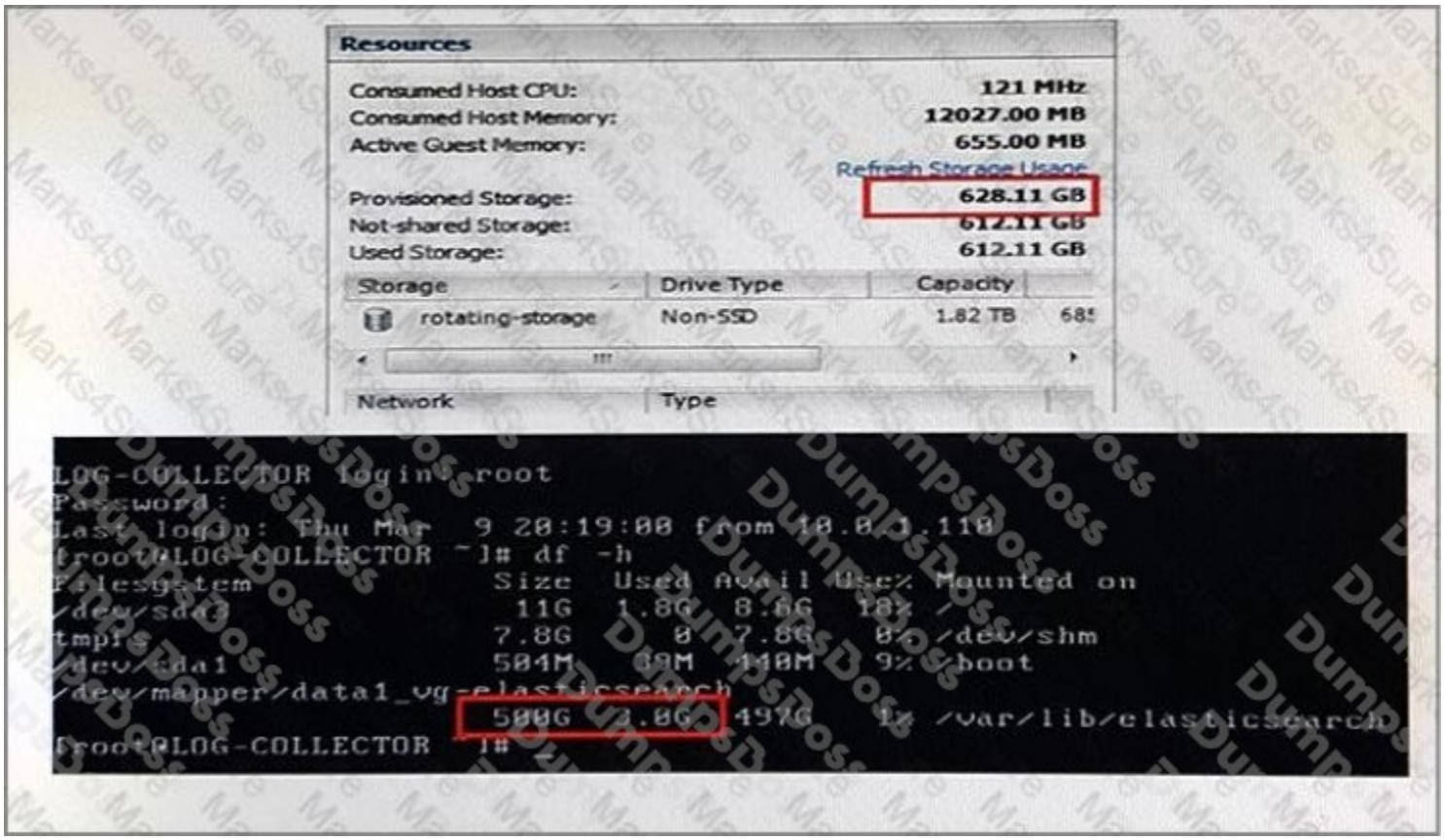
ANSWER: B C E

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-utm-content-filtering.html#id-co

QUESTION NO: 5

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: A C

Explanation:

https://www.juniper.net/documentation/en_US/junos-space16.1/topics/task/operational/junos-space-size-vm-dis

QUESTION NO: 6

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

QUESTION NO: 7

You are configuring transparent mode on an SRX Series device. You must permit IP-based traffic only, and BPDUs must be restarted to the VLANs from which they originate.

Which configuration accomplishes these objectives?

A. bridge {block-non-ip-all;bpdu-vlan-flooding;}

B. bridge {block-non-ip-all;bypass-non-ip-unicast;no-packet-flooding;}

C. bridge {bypass-non-ip-unicast;bpdu-vlan-flooding;}

D. bridge {block-non-ip-all;bypass-non-ip-unicast;bpdu-vlan-flooding;}

ANSWER: A

Explanation:

https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/family-ethernet-s

QUESTION NO: 8

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: A D

QUESTION NO: 9

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

QUESTION NO: 10

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

Explanation:

By default, the device first checks incoming e-mail against the local whitelist and blacklist. If the sender is not found on either list, the device proceeds to query the SBL server over the Internet. When both server-based antispam filtering and local list antispam filtering are enabled, checks are done in the following order:

The local whitelist is checked. If there is a match, no further checking is done. If there is no match… Local blacklist and whitelist matching continues after the antispam license key is expired.

The local blacklist is checked. If there is a match, no further checking is done. If there is no match…The SBL server list is checked.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-local-list-antispam-filtering.html