**Leads4Pass**

# JN0-334 Q&As

## Security-Specialist (JNCIS-SEC)

# Pass Juniper JN0-334 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.leads4pass.com/jn0-334.html**

## 100% Passing Guarantee
## 100% Money Back Assurance

Following Questions and Answers are all new published by Juniper Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

**QUESTION 1**

Which two solutions provide a sandboxing feature for finding zero-day malware threats? (Choose two.)

A. Sky ATP

B. UTM

C. JATP

D. IPS

Correct Answer: AC

**QUESTION 2**

Your network uses a remote e-mail server that is used to send and receive e-mails for your users. In this scenario, what should you do to protect users from receiving malicious files through e-mail?

A. Deploy Sky ATP IMAP e-mail protection

B. Deploy Sky ATP MAPI e-mail protection

C. Deploy Sky ATP SMTP e-mail protection

D. Deploy Sky ATP POP3 e-mail protection

Correct Answer: C

**QUESTION 3**

What is the correct step sequence used when Sky ATP analyzes a file?

A. static analysis -> cache lookup -> antivirus scanning -> dynamic analysis

B. cache lookup -> static analysis -> antivirus scanning -> dynamic analysis

C. cache lookup -> antivirus scanning -> static analysis -> dynamic analysis

D. dynamic analysis -> static analysis -> antivirus scanning -> cache lookup

Correct Answer: C

Reference: https://www.juniper.net/documentation/en_US/release-independent/sky-atp/informationproducts/pathway-pages/sky-atp-admin-guide.pdf page 9

**QUESTION 4**

Which two statements about JIMS high availability are true? (Choose two.)

A. JIMS supports high availability through the installation of the primary and secondary JIMS servers.

B. SRX clients are configured with the shared virtual IP (VIP) address of the JIMS server.

C. SRX clients are configured with the unique IP addresses of the primary and secondary JIMS servers.

D. SRX clients synchronize authentication tables with both the primary and secondary JIMS servers.

Correct Answer: AC

**QUESTION 5**

Click the Exhibit button.

```
user@srx> show log massages
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
no commit script changes
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
no transient commit script changes
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
finished loading commit script changes
Aug 3 15:46:56 chiron mgd[2444]: UI_COMMIT_PROGRESS: Commit operation in progress:
exporting juniper.conf
...
Aug 3 15:47:51 chiron idpd[2678]: IDP_POLICY_LOAD_SUCCEEDED: IDP
policy[/var/db/idpd/bins/idpengine.bin.gz.v] and
detector[/var/db/idpd/sec-repository/installed-detector/libidp-detector.so.tgz.v]
loaded successfully (Regular load).
Aug 3 15:47:51 chiron idpd[2678]: IDP_COMMIT_COMPLETED: IDP policy commit is
complete.
...
Aug 3 15:47:51 chiron chiron sc_set_flow_max_sessions: max sessions set 16384
```

You examine the log file shown in the exhibit after running the set security idp active-policycommand.

Which two statements are true in this scenario? (Choose two.)

A. The IDP policy compiled successfully.

B. The IDP policy loaded successfully.

C. The IDP hit cache is set to 16384.

D. The entire configuration was committed.

Correct Answer: AB

Reference: https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-policiesoverview.html

QUESTION 6

The DNS ALG performs which three functions? (Choose three.)

A. The DNS ALG performs the IPv4 and IPv6 address transformations.

B. The DNS ALG performs DNS doctoring.

C. The DNS ALG modifies the DNS payload in NAT mode.

D. The DNS ALG performs DNSSEC.

E. The DNS ALG performs DNS load balancing.

Correct Answer: ABC

QUESTION 7

What are two valid JIMS event log sources? (Choose two.)

A. Microsoft Windows Server 2012 audit logs

B. Microsoft Active Directory server event logs

C. Microsoft Exchange Server event logs

D. Microsoft Active Directory audit logs

Correct Answer: BC

QUESTION 8

Where is AppSecure executed in the flow process on an SRX Series device?

A. screens

B. security policy

C. zones

D. services

Correct Answer: D

**QUESTION 9**

You must configure JSA to accept events from an unsupported third-party log source. In this scenario, what should you do?

A. Separate event collection and flow collection on separate collectors.

B. Configure an RPM for a third-party device service module.

C. Configure JSA to silently discard unsupported log types.

D. Configure a universal device service module.

Correct Answer: D

**QUESTION 10**

You must fine tune an IPS security policy to eliminate false positives. You want to create exemptions to the normal traffic examination for specific traffic.

Which two parameters are required to accomplish this task? (Choose two.)

A. source IP address

B. destination IP address

C. destination port

D. source port

Correct Answer: AB

**QUESTION 11**

What are two management methods for cSRX? (Choose two.)

A. Network Director

B. J-Web

C. CLI

D. Contrail

Correct Answer: BC

**QUESTION 12**

After a software upgrade on an SRX5800 chassis cluster, you notice that both node0 and node1 are in the primary state, when node1 should be secondary. All control and fabric links are operating normally.

In this scenario, which step must you perform to recover the cluster?
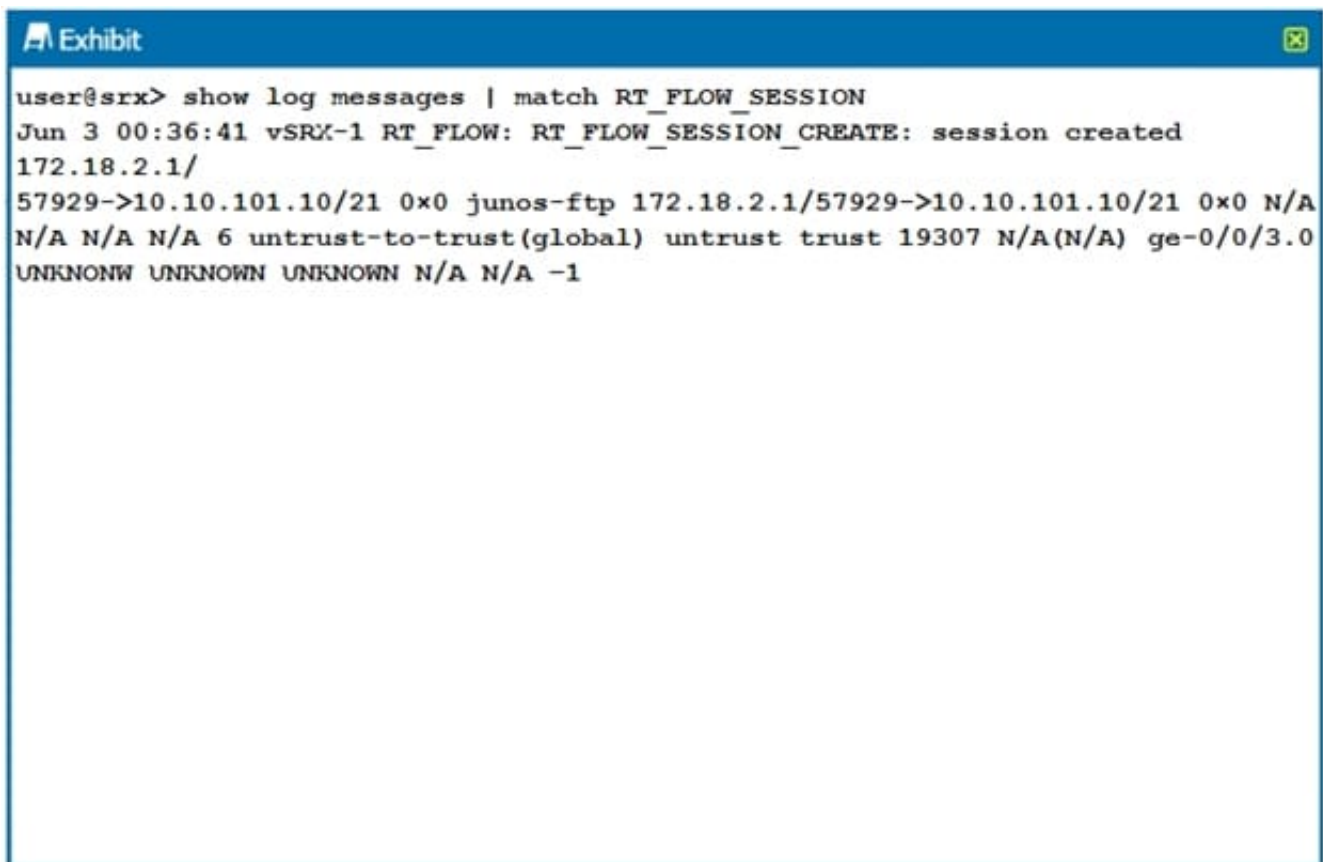
A. Execute the request system rebootcommand on node1.

B. Execute the request system software rollbackcommand on node0.

C. Execute the request system software addcommand on node1.

D. Execute the request system rebootcommand on node0.

Correct Answer: A

**QUESTION 13**

Click the Exhibit button.

```
user@srx> show log messages | match RT_FLOW_SESSION
Jun 3 00:36:41 vSRX-1 RT_FLOW: RT_FLOW_SESSION_CREATE: session created
172.18.2.1/
57929->10.10.101.10/21 0x0 junos-ftp 172.18.2.1/57929->10.10.101.10/21 0x0 N/A
N/A N/A N/A 6 untrust-to-trust(global) untrust trust 19307 N/A(N/A) ge-0/0/3.0
UNKNONW UNKNOWN UNKNOWN N/A N/A -1
```

The output shown in the exhibit is displayed in which format?

A. syslog

B. sd-syslog

C. binary

D. WELF

Correct Answer: A

**QUESTION 14**

Which feature supports sandboxing of zero-day attacks?

A. Sky ATP

B. SSL proxy

C. ALGs

D. high availability

Correct Answer: A

**QUESTION 15**

Which two functions are performed by Juniper Identity Management Service (JIMS)? (Choose two.)

A. JIMS synchronizes Active Directory authentication information between a primary and secondary JIMS server.

B. JIMS forwards Active Directory authentication information to SRX Series client devices.

C. JIMS collects and maintains a database of authentication information from Active Directory domains.

D. JIMS replicates Active Directory authentication information to non-trusted Active Directory domain controllers.

Correct Answer: AC

JN0-334 Practice Test          JN0-334 Study Guide          JN0-334 Exam Questions