



JN0-355^{Q&As}

Junos Pulse Secure Access, Specialist (JNCIS-SA)

Pass EC-COUNCIL JN0-355 Exam with 100% Guarantee

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

<https://www.passapply.com/jn0-355.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

Which three statements describe virtual desktops?

- A. Virtual desktops enable users to run personal computer instances on a remote central server.
- B. Virtual desktops remove workspace data when a session ends.
- C. Virtual desktops provide a real-time malware scan and remove the malware if detected.
- D. Virtual desktops lower administrative, support, and hardware costs associated with individual PCs.
- E. Virtual desktop support includes Citrix XenDesktop.

Correct Answer: ADE

QUESTION 2

You are configuring a Web resource policy and you want to ensure that a user can only access the URL <http://intranet.example.com/employees> and exactly one level below /employees. Which policy will satisfy this requirement?

- A. http://intranet.example.com/employees/*/?
- B. http://intranet.example.com/employees/*
- C. <http://intranet.example.com/employees/?>
- D. <http://intranet.example.com/employees/%>

Correct Answer: D

QUESTION 3

Which two statements describe the functionality of the client standalone installer? (Choose two.)

- A. All Windows clients are available as standalone installers, except Host Checker.
- B. Juniper Installer Service client deployment requires administrative privileges.
- C. Juniper Installer Service client can be deployed using the automated Microsoft Systems Management Server (SMS) service.
- D. Clients deployed using Juniper Installer Service require post-installation machine reboot.

Correct Answer: BC



QUESTION 4

Which statement about Public Key Infrastructure (PKI) is true?

- A. PKI negotiates a secure connection between a client and a server.
- B. PKI specifies the use of a shared key.
- C. PKI uses digital certificates to bind public keys to an entity.
- D. PKI requires the use of a certificate authority and a registration authority.

Correct Answer: C

QUESTION 5

Which Junos Pulse Secure Access Service component controls the user login URL mapping to the appropriate backend authentication service?

- A. authentication server
- B. authentication realm
- C. resource policy
- D. sign-in policy

Correct Answer: D

QUESTION 6

You want to use ESP for your VPN Tunneling transport mechanism.

Which port must you have open on your firewall to the Junos Pulse Secure Access Service in a default configuration?

- A. UDP 500
- B. TCP 500
- C. UDP 4500
- D. TCP 4500

Correct Answer: C



QUESTION 7

What is the function of the smart caching setting within a Web caching policy?

- A. to send the cache control compress header to the client
- B. to remove the cache control headers from the origin server
- C. to not modify the cache control header from the origin server
- D. to send the appropriate cache control header based on Web content.

Correct Answer: D

QUESTION 8

-- Exhibit -

Root::user1(patch management)[Web Users] - Start Policy [WEBURL/REWRITING] evaluation for resource http://www.juniper.net:80/

Root::user1(patch management)[Web Users] - Applying Policy [Initial Rewrite Policy]...

Root::user1(patch management)[Web Users] - Action [Rewrite Content (auto-detect content type)] is returned

Root::user1(patch management)[Web Users] - Policy [Initial Rewrite Policy] applies to resource

Root::user1(patch management)[Web Users] - Passthrough proxy policies are not applicable for http://www.juniper.net

Root::user1(patch management)[Web Users] - Start Policy [WEBURL/ACCESS] evaluation for resource http://www.juniper.net:80/

Root::user1(patch management)[Web Users] - Applying Policy [Web]...

Root::user1(patch management)[Web Users] - Evaluating Policy Rule 1...

Root::user1(patch management)[Web Users] - Resource filter [http://www.juniper.com:80/*] does not match

Root::user1(patch management)[Web Users] - No Policy Rule applies to resource

Root::user1(patch management)[Web Users] - Applying Policy [Initial Open Policy]...

Root::user1(patch management)[Web Users] - User roles [Web Users] do not match with



configured roles [Exclusive:Web Users]

Root::user1(patch management)[Web Users] - No Policy applies to resource

Root::user1(patch management)[Web Users] - Start Auto Allow evaluation on WEBURL for

resource <http://www.juniper.net:80/>

Root::user1(patch management)[Web Users] - No Auto Allow resources configured

-- Exhibit -A user should be able to access a Web resource but instead is receiving an error that access to the site is blocked.

Referring to the exhibit, which policy must be modified to allow access to the resource?

- A. initial rewrite policy
- B. pass-through proxy policy
- C. initial open policy
- D. selective rewrite policy

Correct Answer: C

QUESTION 9

Certain users within your organization have an LDAP attribute named userAttr.EmployeeLevel.

You want to map these users to a specific role if the value of the attribute is 65 or higher.

In the Admin UI, which role mapping rule type will perform this operation?

- A. Username
- B. Group Membership
- C. Custom Expression
- D. Certificate Attribute

Correct Answer: C

QUESTION 10

Your customer requires some users to be mapped to a specific role. The Active Directory (AD) administrator frequently changes users from one AD group to another. Which role mapping rule type should you use?

- A. the user's group membership returned by the realm's authentication server



- B. the result of a host check rule for machine certificate
- C. the authentication realm accessed
- D. the user's username and NetBIOS name

Correct Answer: A

QUESTION 11

Which action must you perform to use CRLs to validate user certificates?

- A. Configure an OCSP responder.
- B. Validate a trusted server CA.
- C. Import as a trusted client the root certificate of the CA issuing the CRL.
- D. Configure a CA chain.

Correct Answer: C

QUESTION 12

When adding a new cluster member, the cluster node state is indicated by a yellow radio button icon in the Admin UI. Which cluster node state is correct?

- A. The node is enabled, not accepting user requests.
- B. The node is transitioning.
- C. The node is enabled, unreachable.
- D. The node is disabled.

Correct Answer: B

QUESTION 13

As an administrator, what would you do to synchronize the state after configuring a license server on a virtual application?

- A. Pull the leasing state from the license server on the virtual appliance.
- B. Copy the leasing state from the license server on the virtual appliance.
- C. Push the leasing state from the license server to the virtual appliance.



D. Post the leasing state from the license server to the virtual appliance.

Correct Answer: A

QUESTION 14

How are user role-mapping rules processed by the Junos Pulse Secure Access Service gateway?

- A. All rules are processed in a top-down fashion for the best match. If no match is found, the user is not allowed to sign in to the realm.
- B. All rules are processed in a top-down fashion for the best match. If no match is found, the user is assigned to the default role.
- C. All rules are processed in a top-down fashion for all eligible matches. If no match is found, the user is not allowed to sign into the realm.
- D. All rules are processed in a top-down fashion for all eligible matches. If no match is found, the user is assigned to the default role.

Correct Answer: C

QUESTION 15

You want to restrict role access to only users who have the required client certificate and pass a Host Checker policy. Which two methods in the Admin UI would set this restriction? (Choose two.)

- A. Enable the Host Checker and certificate role restrictions.
- B. Require and enforce the Host Checker and certificate authentication policies.
- C. Use a custom expression to map users to the role based on the client certificate and Host Checker policy.
- D. Use Secure Virtual Workspace to restrict access to the role based on the client certificate and Host Checker policy.

Correct Answer: AC

[Latest JN0-355 Dumps](#)

[JN0-355 VCE Dumps](#)

[JN0-355 Brindumps](#)