

# ***Passcert***

Higher Quality, better service!



# **Q&A**

***[Http://www.passcert.com](http://www.passcert.com)***

***We offer free update service for one year.***

**Exam** : **642-591**

**Title** : Implementing Cisco NAC  
Appliance

**Version** : DEMO

**1.The NAS is configured to autogenerate an IP address pool of 30 subnets with a netmask of /30, beginning at address 192.168.10.0. Which IP address is leased to the end-user host on the second subnet?**

- A.192.168.10.4
- B.192.168.10.5
- C.192.168.10.6
- D.192.168.10.7

**Correct:C**

**2.Which default administrator group has delete permissions?**

- A.admin
- B.help-desk
- C.add-edit
- D.full-control

**Correct:D**

**3.What is the result when the condition statement in a Cisco NAA check for required software evaluates to false on a client machine?**

- A.The required software is automatically downloaded to the user device.
- B.The required software is made available after the user is quarantined.
- C.The user is put in the unauthenticated role and the software is considered missing.
- D.The user is placed in the temporary role and the software is made available.

**Correct:B**

**4.Which three components comprise a Cisco NAC Appliance solution? (Choose three.)**

- A.a NAC-enabled Cisco router
- B.a Linux server for in-band or out-of-band network admission control
- C.a Linux server for centralized management of network admission servers
- D.a Cisco router to provide VPN services
- E.a read-only client operating on an endpoint device
- F.a NAC-enabled Cisco switch

**Correct:B C E**

**5.Drop**

Click and drag the default username from the left to the correct description on the right. (Choose three.)

- normal role
- blocked role
- authenticated role
- quarantine role
- remediation role
- temporary role

- assigned to this role after vulnerabilities are found in a network scan
- assigned to this role when Cisco NAA end-user policy requirements are not met
- assigned to this role after a successful login

**Correct:**

**Green choice1---->Yellow Choice3**

**Green choice6---->Yellow Choice2**

**Green choice4---->Yellow Choice1**

**6.Drop**

Click and drag each feature of a Cisco NAC Appliance solution from the left to its correct benefit on the right.

- vulnerability assessment
- authentication integration
- traffic-filtering policies
- centralized management
- remediation and repair
- adaptable levels of enforcement

- has a web-based management console that can manage several servers
- provides access to OS patches and updates, virus and spam filters, and endpoint security
- scans for specific endpoint devices and roles, and adjusts for required remediation
- supports Kerberos, LDAP, RADIUS, Active Directory, S/Ident
- supports role-based policies
- supports scanning of network-based operating systems and non-PC networked devices

**Correct:**

**Green choice1---->Yellow Choice6**

**Green choice2---->Yellow Choice4**

**Green choice3---->Yellow Choice5**

**Green choice4---->Yellow Choice1**

**Green choice5---->Yellow Choice2**

**Green choice6---->Yellow Choice3**

**7.When configuring the Cisco NAM to implement Cisco NAA requirement checking on client machines, what is the next step after configuring checks and rules?**

- A.retrieve updates
- B.require the use of the Cisco NAA
- C.configure session timeout and traffic policies
- D.map rules to requirement
- E.configure requirements

**Correct:E**

**8.Refer to the exhibit. When logging in to a Cisco NAC Appliance solution, an end user is prompted for a username, password, and provider. What should be entered in the Provider drop-down field shown in the exhibit?**



- A.the authenticating NAS
- B.the authorizing NAM
- C.the name of the ISP
- D.the external authenticating server

**Correct:D**

**9.What are the two types of traffic policies that apply to user roles? (Choose two.)**

- A.IP-based
- B.peer-based
- C.host-based
- D.manager-based
- E.server-based
- F.VLAN-based

**Correct:A C**

**10.After you implement a network scan and view the report, you notice that a plug-in did not access any of its dependent plug-ins. What did you forget to do?**

- A.enable the Dependent Plug-in check box on the General Tab form
- B.configure dependent plug-in support when you mapped the Nessus scan check to the Nessus plug-in rule
- C.install dependent plug-ins when you updated the Cisco NAC Appliance plug-in library
- D.load the dependent plug-ins for that plug-in in the Plug-in Updates form

**Correct:D**

