PASSTCERT
QUESTION & ANSWER

Higher Quality
Better Service!

We offer free update service for one year
HTTP://WWW.PASSTCERT.COM

Exam: **ST0-153**

Title : Symantec PGP Universal Server 3.2 Technical Assessment

Version: DEMO

1.Under which conditions can an Additional Decryption Key (ADK) be useful?
A.If an administrator needs to bypass the Ignition Key.
B.If an administrator needs to decrypt data for a user that is unavailable.
C.If a user would like to exchange encrypted email with someone who does not have PGP Desktop installed.
D.None of the above
Answer: B

2.We assign a custom attribute to the “Engineering Department” Consumer Policy.What attributes are allowed, given the Consumer Policy’s name?
A.It depends on the directory structure but probably uid.
B.Any attribute can be used.
C.CN, memberOf, or OU.
D.memberOf only.
Answer: B

4.What are the four setup types for PGP Universal Server?
A.New Installation, Cluster Member, Gateway, Keyserver
B.Standalone, Join Cluster, Restore, Keyserver
C.New Installation, Cluster Member, Gateway, Internal
D.New Installation, Join Cluster , Restore, Gateway
E.None of the above
Answer: E

6.What attributes do you think are the most commonly used (and useful) for sorting large groups of users?
A.Uid, CN, memberOf
B.OU, memberOf, department, CN
C.mail, OU, department, memberOf
D.memberOf, employeename, CN
Answer: B

7.What can be done if a client cannot download policy for 30 days (default setting)?
A.Block or apply last downloaded policy
B.Send in the clear of block
C.Keep checking for another 30 days
D.Use the encrypt / sign buttons
Answer: A

8.What can be used to encrypt the Web Messenger data stored on PGP Universal Server?
A.The Verified Directory
B.WDE
C.PGP NetShare
D.The Ignition Key
Answer: D

9.What client functionality is available for Linux?
A.PGP NetShare
B.PGP Virtual Disk
C.WDE
D.PGP Zip
Answer: C

10.What could be used in place of an Ignition Key if it is lost or forgotten?
A.Use a new hardware ignition token.
B.Use the Organization key.
C.Use a passphrase.
D.Reinstall the Universal Server and restore the data.
Answer: B

11.What did I do to start installing PGP Universal Server?
A.Download the installer and run the .msi file.
B.Boot from an install CD or .iso.
C.Download Linux (Fedora or CentOS) after consulting the Release Notes and install, then add PGPUniversal Server packages.
D.None of the above.
Answer: B

12.What happens if a message does not match any rule in a policy chain?
A.It is sent in the clear.
B.It goes to the Exception chain.
C.It is encrypted or bounced.
D.We try to encrypt and then send in the clear if we can find a key.
E.A mail loop is created.
Answer: A

13.What is a disadvantage of TPM support for PGP Whole Disk Encryption?
A.It forces the user to use a long randomly generated passphrase if they forget their original one.
B.Without a token they will be unable to enroll.
C.It prevents Single Sign On.
D.Moving a hard drive to another machine requires special steps.
Answer: D

14.What is a feature of SCKM?
A.The decryption can be done by the key on the server or on the client.
B.The keypair is controlled only by the client.
C.The keypair passphrase matches the WDRT passphrase.
D.The signing can be done on the client or on the server.
Answer: A

15.What is a user in a PGP product environment?
A.Anything but someone that uses WDE (those are devices).
B.A user is someone that is going to utilize PGP applications in some method.
C.A user is only someone that has PGP Desktop.
D.A user could be any of the above.
Answer: B

16.What is KMS?
A.A way to manage certs and keys.
B.The name for PGP Universal Server Mail Policy.
C.The PGP Desktop policy checking protocol.
D.A way to manage user policy from clients.
Answer: A

17.What is the default encryption behavior for messages passing out of the server?
A.Attempt to encrypt / sign, send in the clear if no key is found.
B.Attempt to send in the clear, block if no key is found.
C.Attempt to encrypt / sign, bounce if no key is found.
D.Attempt to encrypt / sign, send Web Messenger if no key is found.
Answer: A

18.What is the default offline behavior for PGP Universal Server?
A.Standalone
B.Offline: Standalone
C.Offline: Block
D.Offline: Send Clear
Answer: C

19.What is the default path for an outbound SMTP email with no PGP client?
A.Default > Outbound > Outbound: Server Only
B.Default: Legacy Clients > Outbound > Outbound: Server Only
C.Default > Outbound: Server Only
D.Default > Outbound > Outbound: Send Message
Answer: A

20.What is the definition of a policy chain?
A.When a condition is matched it is what is 'executed' by the server or client.
B.A group of users who have specific PGP Desktop settings based on directory attributes and values.
C.A collection of ordered rules that determine how PGP Universal Server processes inbound/outbound emailmessages.
D.A way to bypass DNS for sending mail to a specific domain.
Answer: C

21.What is the definition of Key Not Found?
A.What action to take if an encryption key can be found.
B.When a user logs into Windows, if their key is not present and they are GKM they must download it fromthe server.
C.This has to do with Conditions in Mail Policy.
D.What action to take if an encryption key cannot be found.
Answer: D

22.What is the difference between a DMZ cluster zone server and a normal cluster server?
A.Internal servers cannot communicate with DMZ servers.
B.DMZ servers cannot initiate TCP connections.
C.Private keys cannot be stored on DMZ zone servers.
D.Web Messenger inboxes cannot be stored on DMZ servers.
Answer: B

23.What is the difference between a server and a client policy chain?
A.The client chains can process the most conditions.
B.The server cannot process dictionaries.
C.There is no difference.
D.Server chains have more conditions.
E.The client chain takes precedence over the server chains.
Answer: D

24.What is the difference between disabling a PGP Desktop component using its MSI property and disabling it through policy?
A.When you disable a component using its MSI property, it cannot be enabled without reinstalling PGPDesktop.
B.When you disable a component through policy, it cannot be enabled without reinstalling PGP Desktop.
C.There is no difference.Whether a component is disabled through policy or its MSI property, the only wayto enable that component is to reinstall PGP Desktop.
D.None of the above.
Answer: A

25.What is the difference between PGP Virtual Disk and WDE?
A.Virtual Disk is for partitions, PGP WDE secures an entire hard drive
B.Virtual Disk is for hard disks, PGP WDE is for specific partitions
C.Virtual Disk can have multiple users and WDE cannot
D.WDE can secure an entire boot disk, PGP Virtual Disk cannot
Answer: D

26.What is the keypair passphrase for a user that has used Silent Enrollment?
A.It is the user windows password.
B.It is randomly assigned.
C.It is determined assigned by the PGP Universal Server admin.

D.The user is prompted to enter and confirm one.
Answer: A

27.What is the most secure setting for storing backups?
A.Local
B.FTP
C.SCP
D.It doesn matter because backups are encrypted to the ADK.
Answer: C

28.What is the name of the Active Directory group whose members can administer PGP Whole Disk Encryption from the command line?
A.WDE-SYSTEM
B.WDE-ADMINISTRATORS
C.WDE-CONFIG
D.WDE-ADMIN
Answer: D

29.What is the newest standard for secure message processing?
A.PGP/MIME
B.PGP Partitioned
C.SMIME
D.RSA
Answer: A

30.What key can be used to encrypt Web Messenger data?
A.The ADK
B.The Organization Certificate (if the messages are SMIME).
C.The External User PGP key.
D.The Ignition Key.
Answer: D