**Question 1**

When it is necessary to store secrets in variables, and what is the appropriate way to secure them?

Rely on user/group security and ACLs

Encrypt the entire playbook using GnuPG

Encrypt the secret variables using Ansible Vault

Change the playbook to use var\_prompt for all secrets

**Question 2**

When calling Ansible from another script, and a vault file is in use, what is the best way to specify the vault password?

Use the --ask-vault-pass option with echo and a pipe to supply the vault password prompt

Supply the password on the Ansible command line with --vault-pass

Decrypt the vault in the script to avoid the prompt

Store the password in a temp file and use the --vault-password-file option

**Question 3**

Which command displays the contents of a vault-encrypted variable file while still leaving the file encrypted on disk?

Encrypted file contents cannot be viewed

ansible-vault view encryptedvars.yml

ansible-vault decrypt encryptedvars.yml

ansible --decrypt-vault encryptedvars.yml

**Question 4**

How should a vault-encrypted variable file be referenced from a playbook?

Add an include\_vars directive to the play

Add an include task to the play

Add an include\_encrypted\_vars directive to the play

Add a --include-vault directive on the command line

**Question 5**

What is the best way to modify a vault-encrypted file?

vi encryptedvars.yml

ansible-vault edit encryptedvars.yml

ansible-vault decrypt encryptedvars.yml; vi encryptedvars.yml

Re-create the encrypted file