DUMPSBOSS.

# SE Professional Accreditation-Data Center

## Palo Alto Networks PSE-DataCenter

### Version Demo

**Total Demo Questions: 4**

**Total Premium Questions: 45**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which three of these are valid profiles for configuring HA timers?

**A.** Recommended

**B.** Custom

**C.** Aggressive

**D.** Low - latency

**E.** Advanced

**ANSWER: A C E**

**Explanation:**

The valid HA timer profiles are **Recommended**, **Aggressive**, and **Advanced**. These profiles are selected in the firewall's high availability configuration to control the frequency and sensitivity of HA control-link hellos, heartbeat-backup communication, and monitoring-related failure detection. The Recommended profile uses Palo Alto Networks' standard timer values and is appropriate for most deployments because it provides a practical balance between rapid failure detection and resilience to transient network conditions. The Aggressive profile uses shorter intervals, enabling faster detection of a peer or path failure where the network is stable enough to support it. The Advanced profile exposes the individual timer settings so that an administrator can tune them for specific operational requirements, such as network latency and desired failover behavior. Palo Alto Networks advises evaluating link quality, latency, and the risk of unnecessary failovers before using lower timer values. HA timer configuration is documented as part of the HA General settings and should be applied consistently with the organization's availability objectives. See the Palo Alto Networks active/passive HA configuration documentation and the High Availability administration guide.

**QUESTION NO: 2**

An organization uses Panorama in management-only mode for centrally managing a large global firewall deployment. A regional data center produces a high volume of logs and requires its logging capacity to scale independently from the Panorama management pair.

Which two design choices meet these requirements? (Choose two.)

**A.** Deploy dedicated Log Collectors for the regional data center.

**B.** Add the dedicated collectors to a Log Collector Group.

**C.** Use the Panorama HA peers as the only regional log collectors.

**D.** Create a separate device group for each dedicated collector.

**E.** Store all regional logs only on the firewalls that generate them.

**ANSWER: A B**

**Explanation:**

Deploying **dedicated Log Collectors** separates high-volume log ingestion and retention from the Panorama management function. This allows the management tier and the logging tier to be sized independently.

Adding the dedicated collectors to a **Log Collector Group** lets the firewalls forward logs to a logical collector group while the collectors provide combined capacity and distribute the logging workload. Panorama HA provides management resiliency, but it does not make the Panorama peers a replacement for a dedicated, scalable collector architecture. A device group controls policy and object hierarchy, not log-collection capacity.

**QUESTION NO: 3**

A Panorama administrator uses a template stack to apply a common baseline to a group of data center firewalls. A lower template defines an NTP server for all firewalls, but a higher template in the same stack defines a different NTP server for one application environment.

Which NTP server setting is pushed to the firewalls assigned to the template stack?

**A.** The NTP server defined in the higher template in the stack

**B.** The NTP server defined in the lower template in the stack

**C.** Both NTP server settings, with the firewall selecting one at random

**D.** Neither setting, because conflicting template values cannot be committed

**ANSWER: A**

**Explanation:**

The setting in the higher template in the template stack is pushed to the assigned firewalls. Template stacks provide a way to layer common and environment-specific device and network configuration. When templates contain conflicting values for the same setting, the template with higher precedence in the stack overrides the lower template.

The lower template remains useful for common settings that are not overridden. Device groups are used primarily to organize policy and object configuration, not to resolve conflicting network settings in a template stack.

## QUESTION NO: 4

A parent device group contains common Security policy rules and an address object for a shared backup service. A child device group is used for a data center application environment that must reference the shared backup-service object in its own Security policy rules.

Where should the shared address object be created?

**A.** In the parent device group

**B.** In each child device group independently

**C.** As a local object on every managed firewall

**D.** In the firewall virtual router configuration

**ANSWER: A**

**Explanation:**

The address object should be created in the parent device group. Child device groups inherit objects from their parent device groups, allowing the application environment to reference the common object while retaining the ability to create environment-specific objects locally.

Creating the object only in the child device group would not make it available to sibling device groups. Creating it as a local object directly on individual firewalls would remove centralized object management and can lead to inconsistent policy references.