IBM

Hot/Warm/Cold Backup Solution Definitions and Policy for Disaster Recovery Testing

Definitions

Hot Backup (Active-Active) Solution:

• Production data can be accessed concurrently from machines in a cluster. Examples of hot backup solutions are logical replication and active-active database topologies.

Warm Backup (Active-Passive) Solution:

• Production data is either switched between or replicated between storage subsystems in a cluster, and the switched or replicated data cannot be accessed by secondary nodes in the cluster until a fail-over or role-swap event occurs, at which time a secondary node becomes the production node and the production node no longer has access to the production data. Such configurations can support point-in-time copies of the production data which can be used for off-line backup operations and/or for non-production exercises such as disaster recovery compliance testing. A warm backup solution typically has an active standby operating system installed on each of the secondary nodes in the cluster for the purpose of health monitoring. Examples of warm backup solutions are shared-storage active-passive clustering topologies, such as those exhibited by IBM PowerHA installations.

Cold Backup Solution:

• A cold backup solution does not necessarily require a dedicated backup system, and the client needs to boot up (IPL) to get a backup machine into production. Production starts when applications and data are resumed or restarted on the target node. VM Restart and tape backup are examples of cold backup solutions.

Policy for Disaster Recovery Testing and Disaster Event

Concurrent use of software on both the production and backup machines requires permanent licensing for the software on both. However, certain disaster recovery testing scenarios allow for the temporary use of the production license on both machines concurrently, within the limits set forth below.

"Disaster Recovery Testing" is defined as a test intended to validate the readiness of an organization's capability to recover all aspects of IT operations at a remote location. If the Disaster Recovery Test requires the concurrent use of the program products on both the production and backup servers, the production program use on the backup servers in the disaster recovery site must be run on a point-in-time copy of the production data which is discarded after completion of the test and/or used for off-line backup operations. Therefore, this type of Disaster Recovery Testing is allowed with both warm and cold backup scenarios and is not allowed with hot backup scenarios.

When you use program licenses on your primary and backup machines concurrently for the purpose of Disaster Recovery Testing (not performing actual role swap operations), you are authorized to run four annual tests lasting up to 72 hours each to validate your disaster recovery capabilities. These tests cannot include any productive work, development, program testing, or maintenance. A "Disaster" is defined as an outage event whereby the entire data center is rendered inoperable due to some external force such as a fire, earthquake, flooding, acts of terrorism, and the like. An outage such as a hardware or software failure is not considered a Disaster event. Therefore, the periodic Disaster Recovery Testing must occur at a separate location other than the production data center.

In the event of Disaster, the system at the disaster recovery site ("Disaster Recovery System") can run the production workload up to seventy (70) days. At the end of seventy (70) days, Licensee must either:

(1) purchase the required software entitlements on the Disaster Recovery System;

(2) permanently transfer the software entitlements, if eligible per the software terms and conditions, to the Disaster Recovery System; or

(2) stop using the software on the Disaster Recovery System.

February 2018