

Setting Up Two Bomgar Boxes™ as a Disaster Recovery Best Practice

Two key concerns of any strategic hardware deployment are availability and uptime. In the event of a disaster, your transition time to recovery can be decreased if you have already taken steps to prepare. To help speed your disaster recovery, Bomgar™ has outlined these best practices for deploying two Bomgar Boxes™ in a way that offers minimal downtime.

Architecturally, the Bomgar Box™ consists of both the physical hardware and also the software that runs on it. The software component includes company-specific information such as user accounts, security settings, site aliases, and session logs. All of this company-specific information is backed up through the backup feature of the /login interface. [NOTE: Because of size, not all files in the file store may be backed up, and session recordings are not saved in the backup configuration.] The following steps will lead you through the process of setting up a second Bomgar Box™ as a failover.

If Both Bomgar Boxes™ Reside in the Same IP Subnet

Below is the setup for two Bomgar Boxes™ that reside on the same IP subnet, typically at the same geographic location. In case of physical hazards to your appliance, Bomgar™ recommends that you set up the two appliances either at opposite ends of the server room or in different server rooms altogether.

1. Update both appliances with all security patches, upgrade packages, and SSL Certificates if applicable to ensure that both appliances are running the same software version and patch level.

NOTE: If you install a new upgrade or patch on the production appliance, wait to update the backup appliance until you are sure that the new upgrade is running satisfactorily in production. Should you need to revert to a previous version, follow the recovery steps.

2. Configure the backup appliance with a different IP address than the production appliance. The IP address assigned to the backup appliance allows access to the backup appliance for applying upgrades and patches (e.g. [backup.ip]/box).
3. Frequently back up the production appliance's configuration so that this information can be restored to the backup appliance in the case of a hardware failure in the production appliance.

Recovery Steps

When both appliances are on the same IP subnet, follow the steps below to failover to the backup appliance in the case of hardware failure on the production appliance.

1. The production appliance is running, live, and online.
2. The backup appliance is standing by, configured with a different IP address than the production appliance.

NOTE: The backup appliance can be powered off until needed if physical access is available in case of disaster recovery. Otherwise, it should be powered on.

3. The systems administrator has a recent backup of the production appliance's configuration.
4. The service for the primary appliance goes down, caused by a hardware malfunction, a natural disaster, etc.
5. The systems administrator completely shuts down the production appliance.

6. The systems administrator powers up (if required) the backup appliance and changes its IP address to the IP address that had been assigned to the primary appliance, which is now down. NOTE: If you use a VLAN or port forwarding configuration to NAT a public IP address to the production appliance, you may simply substitute the backup appliance IP for the production appliance IP in the NAT or port forwarding configuration for ports 80, 443 and 8200.
7. The systems administrator restores the most recent backup configuration of the primary appliance to the backup appliance, which now becomes the production appliance.
8. Verify that everything is back online.

If the Bomgar Boxes™ Reside in Different IP Subnets

Below is the setup for two Bomgar Boxes™ that will reside on two different IP subnets, possibly in different geographic areas.

1. Update both appliances with all security patches, upgrade packages, and SSL Certificates if applicable to ensure that both appliances are running the same software version and patch level.

NOTE: If you install a new upgrade or patch on the production appliance, wait to update the backup appliance until you are sure that the new upgrade is running satisfactorily in production. Should you need to revert to a previous version, follow the recovery steps.

2. Assign the backup appliance the appropriate network configuration values for its location. The IP address assigned to the backup appliance allows access to the backup appliance for applying upgrades and patches (e.g. [backup.ip]/box).

Recovery Steps

When the two appliances reside in different IP subnets, follow the steps below to failover to the backup appliance in the case of hardware failure on the production appliance.

1. The production appliance is running, live, and online.
2. The backup appliance is up and running on a separate IP subnet.
3. The systems administrator has a recent backup of the production appliance's configuration.
4. The service for the primary appliance goes down, caused by a hardware malfunction, a natural disaster, etc.
5. The systems administrator completely shuts down the production appliance.
6. The systems administrator restores the most recent backup configuration of the primary appliance to the backup appliance.
7. The systems administrator updates the DNS entry to resolve to the backup appliance IP rather than the production appliance IP. NOTE: When an A-record is changed in the DNS server, it may take some time for any DNS servers that have a cached entry of the old IP address to expire and thus update the entry to the new IP address by polling the DNS server where the change was made. For this reason, it may be helpful to ensure that the DNS entry that points to the Bomgar Boxes™ has a very short DNS cache time to live (TTL). This is also known as the DNS cache timeout. This is not the 48-72 hours that a completely new root DNS name takes to propagate the internet's root DNS servers.
8. Once any cached DNS entries have expired, the representatives and customers should be able to use service as normal on the newly configured appliance. If they are unable to connect, an old DNS entry may be cached on their local computers. In this case, they merely need to clear the browser's cache or run a repair on the network adapter to erase the old DNS entries.
9. Verify that everything is back online.