Transcript: Optimize Appliance Failover

Introduction

With Bomgar failover, you can be assured that your support system will remain operative, regardless of external circumstances.

Initial Setup

To begin your Bomgar appliance failover configuration, go to the **/login** page of your primary Bomgar site using an account with administrative rights. Navigate to the **Management** tab and then the **Security** page. At the bottom of the **Options** section, enter a string into the **Inter-appliance Communication Pre-shared Key** box and then click **Save**.

Next, go to the **Security** page of your backup Bomgar site and enter the same string into the **Pre-shared Key** field. Saving the same key on both your primary and backup sites authorizes your two Bomgar appliances to communicate.

On your primary site, go to the **Failover** page. If you already have one site set up, it is essential that you configure failover from this site, making it the primary, to avoid losing any data. Enter the hostname or IP address of your backup Bomgar site. Enter **443** as the TLS port, and then click **Establish Relationship**.

Once the relationship has been established, both sites will refresh to show their roles, and extraneous tabs will be removed from the backup site. The backup site will automatically pull the primary site's latest data, such as site settings, user accounts, and reports. Once a sync is in progress, you can close the page without stopping the data sync.

Configuration

To share an IP address between your primary site and your backup site, check the box for the shared IP and then click **Save Changes**. This must be done on both sites. This shared IP must be enabled on the primary appliance and disabled on the backup.

Note that automatic failover will not function without a shared IP. Additionally, an IP address should be shared between only one primary site and one backup site.

Make sure that **Enable Backup Operations** is checked. This allows automatic data synchronization and automatic failover to occur.

Set how often automatic data syncs should occur. If the sync interval is set to **Every Day**, set the time at which the sync will occur. If it is set to **Once a Week**, set both the day and time.

Data-Sync Bandwidth Limit determines how much bandwidth can be used for data syncs. A lower bandwidth limit will leave more bandwidth available for other processes but will also cause data-syncs to take more time.

Check **Enable Automatic Failover** to have the backup appliance regularly poll the primary appliance to make sure the primary site is up. If a poll fails, the backup will continue to attempt to poll the primary for the time designated by **Primary Site Instance Timeout**. At the end of this time, the backup will test its own network connectivity.

In the **Network Connectivity Test IPs** field, enter external IP addresses for the backup site to test before assuming that the primary site is down. During setup, test these IPs using the **Test** button and save them using **Save Changes**.

In a failover situation, the backup site will ping this list of IP addresses. If the backup cannot reach any of the test IPs, it will assume that the problem is with its own network connection and will not fail over. However, if one or more of the test IPs can be reached, the backup will assume that the failed attempt to reach the primary is the result of the primary site's being offline and will continue with the failover process to become primary.

Becoming Primary

While automatic failover is one way for the backup site to become the primary, you can also manually switch the sites' roles.

If the primary site is still live and the data is uncorrupted, check the box to pull a final data sync from the primary site. Otherwise, leave this box unchecked. Click **Become Primary**, and the backup site will assume the role of primary. If the other site is available, it will automatically assume the role of backup.

At this point, the shared IP address will attempt to disable on the first Bomgar appliance and will enable on the second. All requests to your support site will be served by the failed-over appliance, and your support processes will continue unimpeded.