BeyondTrust

Privileged Remote Access Disaster Recovery

TC:3/4/2024

Table of Contents

Privileged Remote Access Disaster Recovery

Two key concerns of any strategic deployment are availability and uptime. In the event of a disaster, recovery time can be decreased if the necessary steps have already been taken to prepare for such an event. Please follow the best practices outlined in this guide to prepare for any issues that might arise with your Privileged Remote Access and to minimize downtime.

BeyondTrust Support

BeyondTrust Support is responsible for supporting its products worldwide and is available to help resolve any incidents experienced while using BeyondTrust products. It is important to understand the role of BeyondTrust Support in a disaster recovery situation.

The BeyondTrust Support Guide introduces you to BeyondTrust Technical Support services and explains the details of our Technical Support policies and procedures to ensure that your cases and inquiries are addressed with the appropriate care and urgency they deserve.

> *For more information, please see the BeyondTrust Support Guide at https://www.beyondtrust.com/resources/datasheets/customer-support-guide.*

Backup Procedures

Backing up the site data from BeyondTrust on a regular basis is an essential part of Secure Remote Access administration and maintenance. Most of the settings and data from the /login administrative web interface can be captured as a single NSB file. In most cases, the /appliance administrative web interface contains the SSL certificates and network configuration of the B Series Appliance. These are essential to the functionality of the B Series Appliance and must be configured during the recovery process.

With the exception of certificates, /appliance configuration cannot be downloaded as a single, password-protected file in the way /login configuration can. The /appliance configuration must be backed up using screenshots and/or text data. These files should be given an identifying name, including the B Series Appliance version, B Series Appliance serial number, base software version, and system time as shown on the **Status** page of the B Series Appliance at the time of backup.

Cloud sites have a minimal version of the /appliance web interface accessible from the **Appliance** tab of the /login administrative web interface. Since BeyondTrust manages the network configuration of BeyondTrust Cloud sites and provides a working default certificate, administrators need to backup only their own custom certificates and SSL/TLS configuration, if these have been manually customized.

Failover

BeyondTrust failover enables the synchronization of data between two peer B Series Appliances, creating a simplified process for securely swapping from a failed B Series Appliance. Two B Series Appliances host the same installed software package for a single site. DNS directs support traffic of the site to one of these B Series Appliances, the primary B Series Appliance, where all settings are configured. The backup B Series Appliance synchronizes with the primary B Series Appliance, according to the settings configured in the /login interface. BeyondTrust's failover documentation details how to configure failover between B Series Appliances.

Once two B Series Appliances are in failover mode, the backup of settings and data from the primary to the backup occurs.

1. Log in to the /login admin web interface of the backup B Series Appliance.
2. Browse to **Management > Failover**.
3. Check **Enable Backup Operations**.

> ***Note: Automatic Data-Sync Interval*** *and* ***Data-Sync Bandwidth Limit*** *do not need to be changed in most environments.*

4. Click **Sync Now** to manually force synchronization under **Backup Site Instance Status**. Failover sync captures all users, files, and configuration in /login with the exception of failover configurations, including settings on the **Failover** page and the **Inter-Appliance Pre-Shared Key** under **Management > Security**.

It is important to note that failover B Series Appliances do not sync any settings or data under /appliance. This means that certificates and network configuration are not replicated. It is not necessary to back up certificates from each B Series Appliance; however, failover B Series Appliances must have identical certificate configuration. Once replicated, a single backup copy of the certificates from either B Series Appliance is sufficient. Network configuration and any other customized /appliance settings must be backed up for each B Series Appliance; however, /login data can be backed up for each B Series Appliance as well. This applies especially to failover settings, which are not included in the failover sync. Saving backups of /login settings serves as a safeguard in case failover sync fails.

> *For more information, please see Failover Dynamics and Options at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover.*

Back Up Certificates

Cloud Appliances are managed automatically, but it is possible for administrators to install custom certificates on Cloud Appliances. If a B Series Appliance fails, network configuration and SSL certificates must be restored to the new or repaired B Series Appliance in order to connect with the remote client software (access consoles and Jump Clients, for example). BeyondTrust-hosted sites are managed by BeyondTrust, but administrators of on-premises and Cloud Appliances are encouraged to back up their certificates.

The SSL certificate issued to the B Series Appliance hostname is often unique to the B Series Appliance and is always used to validate its identity to remote client software. It is important that a backup of this certificate, all its intermediate certificates, and its root certificate are saved. We recommend that the certificate backup file be saved with a password in a secure location because in the event a malicious party obtained a copy of this certificate, they could potentially access confidential data on the network.

1. To back up the B Series Appliance certificate(s), log in to the /appliance administrative web interface.
2. Browse to **Security > Certificates**.
3. Locate the certificate with the **Alternative Names** of the B Series Appliance hostname.
4. With the **IP Address(es)** of the B Series Appliance, verify that the **Private Key?** field is set to **Yes**.
5. Check the box next to the certificate.
6. From the **Export from the** dropdown, click **Apply**.
7. Wait for the export page to load.
8. Check **Include Certificate**, **Include Private Key**, and **Include Certificate Chain**.
9. Enter a **Passphrase**.
10. Click **Export**.
11. Save the resulting p12 certificate file in a secure location.

For more information on certificates, please see SSL Certificates and BeyondTrust at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/index.htm.

Back Up /appliance

Network configuration for BeyondTrust should be saved by the networking team in a network diagram. This should include firewall rules, antivirus allow list, and IDS/IPS settings, as appropriate. A backup copy of the B Series Appliance network configuration can be saved by taking screenshots of the /appliance **Networking > IP Configuration** page. If static routes and/or SNMP are used, this information is captured from the **Networking > Static Routes** and **Networking > SNMP** pages, respectively. BeyondTrust Cloud customers and BeyondTrust-hosted sites do not have these options and do not need to be backed up. They are managed automatically.

If the B Series Appliance has custom SSL/TLS configuration or special user account, network, and/or port restrictions, take a screenshot of these from **Security > SSL/TLS Configuration** and **Security > Appliance Administration**. The B Series Appliance may also be configured to send logs to a syslog server. If this is the case, make note of the syslog server's hostname and/or IP along with its preferred message format. These settings can be found under **Security > Appliance Administration** in the **Syslog** section.

Certain companies have policies requiring users to accept legal agreements before accessing certain interfaces, such as the BeyondTrust /appliance administrative web interface. If the B Series Appliance is configured with such an agreement, the agreement is located under **Security > Appliance Administration > /appliance Prerequisite Login Agreement**. If it is configured, capture a screenshot of the agreement.

The B Series Appliance may also be configured with an SMTP server for sending email. The email configuration settings in /appliance are located in **Security > Email Configuration**. These settings are separate from the email configuration settings in /login. The /appliance email settings are used by the B Series Appliance to send SSL certificate expiration reminders. If the B Series Appliance is configured for reminders, take a screenshot of the page.

Back Up /login

The users, settings, and data in /login can be saved in a single BeyondTrust backup file, which uses the NSB extension. This file can be generated from the BeyondTrust API, from the BeyondTrust Integration Client, or from the /login administrative web interface. BeyondTrust recommends manually downloading NSB backups before installing any updates. To perform manual downloads, click **Download Backup** on the **/login > Management > Software Management** tab.The resulting NSB backup file includes the data listed below even if **Include logged history** is not checked at the time of the download:

- **Local User Accounts**
- **Security Provider Configuration**
- **Group Policy Configuration**
- **Jumpoint Configuration**
- **Jump Client Configuration**
- **Team Configuration**
- **Language Configuration**
- **Security Configuration**
- **Inter-appliance Communication Pre-shared Key**
- **Failover Configuration**
- **Outbound Event Configuration**
- **Kerberos Keytab**

If **Include logged history** is checked, the NSB backup file includes the following data:

- **Logged Session Data**
- **Logged Support Team Information**

In either case, the NSB backup file does not include the following:

- **Session Recordings**
- **Command Shell Recordings**
- **Presentation Recordings**
- **File Store files larger than 200KB**
- **File Store files beyond the first 50**
- **Settings, users, or data from /appliance**

In addition to manual downloads at each upgrade, BeyondTrust also recommends downloading NSB backups on a regular basis, using the automated schedule via the Integration Client. The Integration Client can dowload the following types of data:

- **Session Data**
- **Session Recordings**
- **Command Shell Recordings**

- **Site Backups**
- **Show My Screen Recordings**

The client installation package is available from **Downloads** in the BeyondTrust Self-Service Center. It is released only as a 32-bit Windows client; however, this runs on 64-bit Windows systems. It is available in a number of different versions, so check the BeyondTrust product release version on the **/login > Status > Information** tab to make sure to download the correct Integration Client version.

In addition to the **Download Backup** button and the Integration Client, the BeyondTrust API provides a variety of commands to download backup data. This is useful for automating backups using custom tools and/or scripts. The NSB backups can be downloaded using the BeyondTrust Backup API. Session reports, session recordings, Show My Screen recordings, command shell recordings, presentation recordings, and exit surveys can be downloaded using the Reporting API.

For more information on Integration Client setup and configuration, please see the Integration Client Guide at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/ic/index.htm.

Back Up Vault Encryption Key

The Vault encryption key is used to encrypt and decrypt all Vault credentials stored on your B Series Appliance. If you ever need to restore configuration data from a backup onto a new B Series Appliance, you must also restore the Vault encryption key from a backup to be able to use the encrypted Vault credentials contained in the configuration backup.

Backup Password

To protect your software backup file, create a password. If you do choose to set a password, you will be unable to revert to the backup without providing the password.

Download Vault Encryption Key

Go to **/login > Management > Software > Backup Vault Encryption Key** and click the **Download Vault Encryption Key** button to download the Vault encryption key to use later.

***Note:** The Vault encryption key must be password protected.*

BeyondTrust Privileged Remote Access Recovery

B Series Appliances are available in virtual, hardware, and Cloud versions, which run on shared B Series Appliances in BeyondTrust's data centers. When any of these go offline unexpectedly, the process necessary to repair or replace the B Series Appliance varies, depending on the B Series Appliance in question. The various repair and replacement scenarios are described below so an effective strategy can be developed to prepare for them in advance.

Failover and Spare B Series Appliances

BeyondTrust recommends using a preconfigured failover relationship between a *primary* and a *backup* B Series Appliance. This ensures that the BeyondTrust software is available in the event either B Series Appliance should fail. BeyondTrust customer clients and access consoles are built to attempt connection with the primary B Series Appliance at a specific address. In the event of a primary B Series Appliance failure, this address is used to redirect clients from the failed B Series Appliance to the backup B Series Appliance. This can be accomplished using one of three network routing methods: shared IP, DNS swing, or NAT swing.

Though client traffic is redirected to the backup B Series Appliance, this B Series Appliance does not accept connections until it takes the primary role. Once a backup B Series Appliance takes the primary role, it begins accepting client connections and provides all the same services the failed B Series Appliance did. This role change can be triggered manually or automatically.

Given the above information, here are the basic steps to take in the event of a primary B Series Appliance failure in a failover pair:

1. Redirect network traffic from the primary to the backup B Series Appliance. If the B Series Appliances are configured with:
    - **Shared IP:** The backup B Series Appliance automatically takes over the IP address of the failed B Series Appliance.
    - **DNS swing:** Update the DNS A-record of the primary B Series Appliance to resolve the IP address of the backup B Series Appliance.
    - **NAT swing:** Update the firewall NAT rule(s) to resolve the client-facing / public IP of the failed B Series Appliance to the private IP of the backup B Series Appliance.
2. Make the backup B Series Appliance take over the primary role. If **Enable Automatic Failover** is:
    - **Enabled:** If the backup B Series Appliance can reach the **Network Connectivity Test IPs** and cannot reach the primary B Series Appliance during the **Primary Site Instance Timeout** period, the backup B Series Appliance automatically takes the primary role.
    - **Disabled:** Use the **Become Primary** button or the **API command:set_failover_role**. To use the button, log in to the backup B Series Appliance's /login administrative web interface. Browse to **Management > Failover**. Click **Become Primary**, leaving the adjacent box unchecked.
3. Confirm the clients are working and proceed to perform maintenance on the failed B Series Appliance.

In the event that there is a cold spare instead of a failover B Series Appliance, begin the recovery process by restoring settings and data from the backup(s) to the spare B Series Appliance. Once the data is restored, redirect the client traffic to the spare B Series Appliance using DNS or NAT swing. If the spare B Series Appliance is on the same local network as the failed B Series Appliance, attempt to assign the IP of the failed B Series Appliance to the spare B Series Appliance. However, if the spare B Series Appliance is on the same switch as the failed B Series Appliance, this switch must be rebooted for the change to take effect.

For more information, please see the following:

- *Configuring Failover at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/failover-setup.htm*

- *API Command: set_failover_role at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/command/set_failover_role.htm*

PRA Virtual Appliances

BeyondTrust's SRA Virtual Appliances are certified for VMware vCenter 6.5+, Hyper-V 2012 R2, Azure, AWS, and Nutanix. These SRA Virtual Appliance support virtual machine *snapshots* (VMware) and *checkpoints* (Hyper-V). A checkpoint or snapshot represents the state of a virtual machine at the time it was taken and includes the following:

- Files and memory state of the virtual machine's guest operating system
- Settings and configuration of the virtual machine and its virtual hardware

***Note:** BeyondTrust does not recommend or support creating snapshots (VMware or Nutanix) or checkpoints (Hyper-V) of actively running SRA Virtual Appliances.*

***Note:** If the BeyondTrust SRA Virtual Appliance experiences a failure and there is a recent snapshot or checkpoint, try restoring it first. This is often the fastest way to restore functionality.*

If the BeyondTrust SRA Virtual Appliance is under an active support maintenance contract, BeyondTrust Technical Support sends an up-to-date VMware, Hyper-V/Azure, or Nutanix deployment file for the SRA Virtual Appliance upon request in the event of a failure and/or loss of the SRA Virtual Appliance. To receive a copy, contact BeyondTrust Support with company information from an authorized email address. This address would normally be the same used to communicate with BeyondTrust during the initial deployment of the B Series Appliance and/or subsequent administrative-level incident management. Save a local copy of the SRA Virtual Appliance file in case the SRA Virtual Appliance needs to be restored outside of BeyondTrust Support's normal business hours.

***Note:** To reinstall the SRA Virtual Appliance, follow the procedures outlined in the Beyondtrust SRA Installation Guide at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual-sra/index.htm.Access to the VMware, Hyper-V administrative management tool, the Nutanix console, the Azure Portal or the AWS Console is needed to complete this process.*

1. Log in to the Hyper-V Manager, VMware, or Nutanix infrastructure client.
2. Deploy the **BeyondTrust OVA** (VMware), **EXE** (Hyper-V), or **QCOW2** (Nutanix) file.

***Note:** For AWS redeployment, BeyondTrust does not send a file. The Amazon Machine Image (AMI) used for deployment should be shared with your AWS account. You can see it in the AWS Console under **EC2 > AMIs** by selecting **Private Images**.*

3. Use the Hyper-V Manager, VMware, or Nutanix console client to power on the SRA Virtual Appliance. You must use the AWS Console to power on the AWS appliance.
4. Open the virtual console.
5. Enter the IP address, subnet mask, and default gateway of the SRA Virtual Appliance.

The network settings of the SRA Virtual Appliance should already be saved from previous configuration. Otherwise, contact the company network administrator for the appropriate settings. Once the SRA Virtual Appliance is accessible on the network, log in to the /appliance administrative web interface, update the SRA Virtual Appliance, and restore settings, as needed.

Data Recovery

Once a B Series Appliance has been repaired or replaced, it is usually necessary to restore its settings and data. This is always necessary in cases where BeyondTrust has shipped an entirely new B Series Appliance from the factory. The settings and data to restore includes /appliance settings and certificates as well as /login users and configuration. Before restoring any of this, first complete the B Series Appliance IP network configuration. Once that is done, remaining /appliance configuration, certificates, and /login settings can be restored remotely as described below.

Failover

When a B Series Appliance in a failover pair has failed and been replaced, the second B Series Appliance in the pair will be servicing clients while the failed B Series Appliance is restored. The restore process for the failed B Series Appliance varies depending on its type. Once the B Series Appliance has been restored, restore its certificates either from a backup or by exporting them from the primary B Series Appliance.

Once the failed B Series Appliance is online and has the primary B Series Appliance's certificates installed, restore its /login administrative interface. Since the primary B Series Appliance should already have all settings and data, it is generally not advisable to restore backup files to a backup B Series Appliance manually. However, installing a /login site package is needed. Once that is done, establish failover from the active B Series Appliance to the repaired one and sync them.

It is still possible to download and restore backup files to failover B Series Appliances; however, it is not ideal unless the primary failover B Series Appliance is missing crucial data that exists only in a backup file. If a backup is restored, failover settings are overwritten with the values contained in the backup. This includes both **/login > Management > Failover** settings and the **Inter-appliance Communication Pre-shared Key** found in **/login > Management > Security**. This means that if a backup is restored to a B Series Appliance in active failover, the failover connection is likely to have issues. Because of this, the best practice is to break failover, restore the backup, reset the pre-shared key, and re-establish the failover relationship.

If the restored B Series Appliance in a failover pair has formerly been the primary B Series Appliance in the failover relationship, it re-enters the failover relationship as the backup B Series Appliance. Sometimes, it can remain this way, but in other scenarios, it is desirable to make it primary once again. The process varies slightly, depending on how the network is routing traffic to the primary B Series Appliance. The routing methods are IP failover, DNS swing, or NAT swing.

For more information, please see the following:

- *Establish the Primary/Backup Failover Relationship Between Two B Series Appliances at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/failover-establish-relationship.htm*
- *Failover Dynamics and Options at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/index.htm*
- *Establish Failover for Planned Maintenance at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/planned-maintenance.htm*

Atlas

Like failover, Atlas clusters have special requirements. An Atlas cluster typically consists of a failover pair of primary B Series Appliances that route traffic between a number of traffic node B Series Appliances. If one of the primary B Series Appliances fails, refer to the failover recovery guidelines described immediately above. If one fails, follow these steps:

1. Restore the B Series Appliance.
2. Install a /login site package on the B Series Appliance.
3. Re-add the recovered B Series Appliance to the Atlas cluster.
4. Sync the recovered B Series Appliance in order to restore the /login settings.
    - Log in to the primary B Series Appliance's /login administrative web interface.
    - Browse to **Management > Cluster**.
    - Click **Sync Now**.

Once completed, the traffic node is fully operational. To test, follow these steps:

1. Log in to the traffic node's /login web interface.
2. While logged in to an access console from a geographic region that is expected to route through the restored traffic node, check **Status > Connected Clients**.
3. If the value for connected access consoles increases by one immediately after authenticating to the console, the traffic node is working.

If a backup is restored from an Atlas primary node, it does not overwrite the existing Atlas configuration. As a result, copying the configuration of a primary node to each of its traffic nodes is supported; however, manually performing this task is not standard practice. Synchronizing data from the primary B Series Appliance is the standard method for restoring /login settings to a traffic node.

For more information, please see Set Up the Traffic Nodes in an Atlas Cluster at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/atlas/atlas-traffic-nodes.htm.

Recover Certificates

BeyondTrust requires SSL certificates. If any client software from a previous B Series Appliance is expected to reconnect with the replacement B Series Appliance, this B Series Appliance needs a copy of the original SSL certificate(s). Most Cloud Appliances share a standard certificate which validates the BeyondTrust Cloud domain. If the certificate and domain are changed, the non-standard certificate must be restored. Hardware and PRA Virtual Appliances have no such standard configuration and therefore have unique certificates configured by the administrator that must be restored in a disaster recovery scenario. The steps to restore certificates are given below, and they assume that the necessary steps have been taken to bring the web interfaces online.

***Note:** The steps to bring the web interfaces online vary based on the B Series Appliance type.*

1. Log in to the /appliance web interface of the BeyondTrust Appliance B Series.
2. Go to **Security > Certificates**.

***Note:** If a **B Series Appliance** certificate is listed, ignore it. This is a standard certificate that ships with all B Series Appliances.*

3. In **Security > Certificate Installation**, click **Import**.
4. Browse to the certificate file.
5. Enter the password for the certificate file.
6. Click **Upload**.

The B Series Appliance certificate appears in the **Security > Certificates** section. If the certificate was issued by a third-party Certificate Authority (CA), the intermediate certificate and root certificate are also listed here. If your B Series Appliance uses a CA certificate, all intermediate certificates and their root certificate must be present for the B Series Appliance to function properly. Here is a description of each type of certificate:

- **Self-Signed Certificate:** This has identical values for **Issued To** and **Issued By** and have the B Series Appliance's fully qualified domain name (FQDN) in the **Alternative Name(s)** field.
- **CA-Signed Certificate:** This has an **Issued To** field and/or an **Alternative Name(s)** field matching the B Series Appliance's FQDN. If a CA-signed certificate exists, the B Series Appliance also has one or more intermediate and/or root certificate(s) listed on the **Certificates** page.
- **Intermediate certificates:** These have different **Issued To** and **Issued By** fields, neither of which is an FQDN. Usually, there are only one or two intermediate certificates. Sometimes, there are none, depending on the CA.
- **Root certificate:** This has identical values for the **Issued To** and **Issued By** fields, neither of which are an FQDN. Every CA-signed certificate must have exactly one root certificate.

If a self-signed certificate is being used, a warning is present beneath it. The warning expresses that this kind of certificate should be used only temporarily until a CA-signed certificate is obtained. If a CA-signed certificate has already been obtained and one or more of its intermediate or root certificates are missing, a warning appears beneath the CA-signed certificate. To resolve this, contact the CA to obtain any missing intermediate or root certificates, and upload them to the **Security > Certificates** section.

1. Once there are no certificate warnings, click the **Assign IP** link in the certificates entry for the B Series Appliance's CA-signed or self-signed certificate.
2. At the bottom of the resulting page, check the IP address of the B Series Appliance.
3. Click **Save Configuration**. This completes the restore process for the certificate(s). However, the B Series Appliance still needs /login restored before it is fully operational.

In Base 5+, you don't need to manually assign an IP to the certificate, as it is automatically handled by SNI. You can optionally select the certificate as **Default** if desired.

Recover /login

Unlike /appliance, the /login administrative web interface is not installed by default on new B Series Appliances. Therefore, in cases where a new PRA Virtual Appliance has been installed or a new hardware B Series Appliance has been shipped, the new B Series Appliance does not usually have a /login administrative web interface. If the B Series Appliance is repaired or restored from a snapshot rather than replaced or reinstalled, the repaired B Series Appliance still has a /login site package installed, but it may be necessary to upgrade the site to the same version as the failover B Series Appliance or to a version compatible with the backup file. In these cases, contact BeyondTrust Support for the necessary /login site updates. To get the updates, send BeyondTrust Support an email including these items:

- Screenshot of the /appliance **Status** page
- **B Series Appliance** FQDN registered in DNS
- Version of the most recent backup file

After receiving this information, Support registers the B Series Appliance on the BeyondTrust update servers, builds the necessary update package(s), and sends the installation instructions. There are one or more base software updates to install prior to the /login site package. Follow the instructions from BeyondTrust Support to update the B Series Appliance and log in to the /login web interface, using the default admin and password credentials. The system forces the password to be changed at login.

In failover and Atlas scenarios, /login data is recovered using data synchronization rather than backup files. Save the NSB backup files in order to restore /login settings, users, and data. However, before restoring a backup file, take into account the BeyondTrust product release version from which the backup was downloaded, as well as the version of the site receiving the backup file. BeyondTrust does not test restoring backups from every version to every other version. Only backups from the supported upgrades of a particular version are tested. Supported upgrade versions are listed in the release notes for each version.

The version of a particular backup can be found by checking the filename of the backup. By default, BeyondTrust backup file names begin with **bomgar** followed by the BeyondTrust product release version of the backup, the name of the site which generated the backup, the date on which the backup was downloaded, and the unique ID of the backup file. Check the version of the site to which the backup is being uploaded to by viewing the **Product Version** field on the **/login > Status > Information** page.

When attempting to restore backups from an old release version to a newer version of BeyondTrust not listed as the backup's supported upgrade version, unexpected issues and/or data loss can occur. When attempting to restore backups from newer versions of BeyondTrust to older, major issues occur. This is not supported. However, as long as the rules concerning release versions are followed, backups can be successfully restored between physical B Series Appliances (B200, B300, and B400) and PRA Virtual Appliances and between physical B Series Appliances of different hardware revisions.

Once the restore method is validated, restore the /login site backup by following these steps:

1. Browse to **/login > Management > Software**.
2. Locate **Software > Restore Settings**.
3. Click **Choose File**.
4. Select the backup file using the file browser.
5. Enter the backup password, if one was assigned.
6. Click **Upload Backup**.

The backup password is assigned by the administrator who downloads the backup originally. If it is lost, the backup cannot be restored. Once it is restored, all users (including the local administrator), settings, and most data are restored to the state at which the backup was originally downloaded.

After /login is online and the backup is restored, the B Series Appliance is fully operational, assuming the network's traffic has been properly routed. To test the B Series Appliance:

1. Open the access console.
2. Log in with the user credentials that worked prior to the failure event.
3. Verify that all Jump Clients, Jumpoints, options, and settings function as expected.

There is no need to deploy new client software. Instead, the original clients reconnect with the new B Series Appliance automatically.

For more information, please see the Privilege Remote Access Release Notes page at https://www.beyondtrust.com/docs/release-notes/privileged-remote-access/index.htm.