How to Setup Site-to-Site Replication

Last Updated December 2012

Solution Overview

In many cases, an end-user or partner wants to store valuable data offsite, but needs to do so such that the data is stored in its original format at the destination site, so that it is available to be used as quickly as possible. This process of efficiently getting a copy of data from site A to site B is called replication. Replication is a key piece of the following solutions:

- A partner building their own private storage cloud for their end-users’ BDRs such that their end-users’ servers can be virtualized on the partner’s equipment almost instantly. This includes situations where a partner wants to replicate many different end-users onto the same replication target (many-to-one replication).
- An end-user that wants to replicate bare-metal backup files to a remote location (or to the public cloud) such that the bare-metal backup files are usable directly at the destination site.
- End-users that need to centralize all of their data files onto a single location, and then the data at this centralized location is encrypted and sent off-site via an online backup. For example, a company with 200 laptops may want to keep a copy of all of the data on their users’ laptops, and then centrally manage the backup of this data from one site.
- An end-user that wants to keep an extra copy of their ShadowProtect data on a USB disk (in the original ShadowProtect format), NAS device, or SAN, in addition to a BDR device.

Site-to-site replication differs from site-to-site backup because with site-to-site backup the data is stored in a proprietary format on the destination and has to be restored before the data can be used. With site-to-site replication, the data is stored in its original format, and can be used directly on the destination site. This is appropriate for situations where rapid use of the data is more important than storing the data encrypted and compressed on the destination site.

eFolder provides both site-to-site backup and site-to-site replication technologies through our proprietary network backup server software. At the destination site the network backup server software is installed and configured on a Windows computer, at which point it will listen for connections on TCP port 5470. The eFolder backup agent is then installed on the sites that need to transmit data and configured to send data to the appropriate network hostname or IP address.
**BDR Replication Scenarios**

Replication is fully compatible with eFolder’s BDR solution. BDRs can be both replication sources and replication targets, although a replication source or target does not have to be a BDR (any Windows computer will do). eFolder’s replication technology is a powerful tool to meet the needs of end-users. Here are a few of the ways it can be employed:

- **Bare-metal backup of mobile laptops to an end-user’s on-site BDR:** In this scenario, each laptop performs a bare-metal backup to a dedicated partition or external hard drive. This bare-metal backup is then replicated across the Internet to the BDR installed at the end-user’s site. If a laptop is stolen, that laptop can be virtualized on the BDR almost instantly, and can easily be restored to a new laptop if needed. Additionally, these laptop bare-metal backup images can then be further replicated or backed up as desired for further protection.

- **Cross-site replication for an end-user with two BDRs:** End-users who already have geographically diverse offices can install one BDR at each site, and then have each BDR replicated to the other site. If any site is destroyed, the data will be available for immediate use at the alternate site.

- **Many-to-one replication of several end-users’ BDRs onto a partner’s BDR:** In this scenario a partner acts as a private storage and virtualization cloud for their end-user customers. They buy one (or more) large BDRs, and then install (smaller) BDRs at their customer sites. All of their customer BDRs then replicate to the one (or at least many fewer) BDRs at the partner’s location. If a customer’s site is destroyed or disabled, the partner can quickly bring up their customer’s server on their in-house BDR. The partner will need to provide a branch office VPN tunnel to their customer so that they can transparently access the server hosted in their facility.

**Setup Overview**

First, the replication target(s) should be provisioned by installing and configuring the eFolder network backup server software (any Windows-based computer will work). The eFolder backup client should then be installed onto each computer that will be sending replicated data.

Finally, if you are replicating ShadowProtect backup images, the ImageManager *must be configured on both* the replication source and the replication target to ensure that the backups are up to date and healthy on both the source and the server. Additionally, you may want to configure the eFolder backup client to monitor the integrity of the ShadowProtect backup data on the replication target, to ensure that all consolidation processes on the target are fully monitored by eFolder.

**Configuring the Replication Target**

On the Windows computer that will act as the replication target, install the backup client software. Once installed, start the backup manager, and run the Tools menu, network backup server command.
On the Configure page, choose where the replicated data should be stored, and also enter in your credentials for an appropriate eFolder account:

![Configure page](image)

**IMPORTANT**: If the replication target is a BDR, then you should use the account credentials you received specifically for that BDR unit (and not the credentials for one of the replication source computers). If the replication target is not a BDR, create a new account in the web portal.

**IMPORTANT**: The account used for the network backup server must belong to the same end-user customer (in our web portal) as the accounts for all of the replication sources. If you are doing many-to-one replication for multiple end-user customers, please contact your account representative to ensure that many-to-one replication has been enabled for your account.

In the Options page in the network backup manager, make sure that the *Allow Replication* setting is set to Yes:

![Options page](image)

Finally, configure your network (routers/firewalls) so that any clients that will send the server data will be able to do so over a TCP/IP network on port 5470.
**Configuring each Replication Source**

On the Windows computer that will act as the replication source, install the backup client software. Once installed, start the backup manager, and go to the My Account page. Enter in the account credentials assigned to that computer (it should be different than the account credentials you used on the replication target). In the Network Server (or Local Server) field, enter in the IP address or network hostname of the Network Backup Server:

![Network Server Configuration](image1)

Next, go to the folders page, click the Add button, and choose to add a replicated folder:

![Folder Addition](image2)

The program will warn you of the differences between replication and backup. If you are sure that you want to use replication instead of backup, then click Yes to proceed.

![Replication Confirmation](image3)

Next, select the folder that should be replicated (for example, X:\VolumeImages).
Finally, choose a replication policy:

![Image]

The replication policy affects which files will be replicated to the target. Your choices are:

- **ShadowProtect Daily**: This will replicate ShadowProtect base image files (*.spf files) and ShadowProtect daily image files (*.cd.spi). It will not replicate weekly (*.cw.spi) or monthly (*.cm.spi) or rolling (*.cr.spi) image files (these files will be created by the consolidation process on the replication target).

- **ShadowProtect Realtime**: This will replicate ShadowProtect base image files (*.spf files) and any non-consolidated image files (i.e., hourly image files). This option requires more bandwidth, as all changes recorded by ShadowProtect throughout the day will be uploaded. If you choose this policy, we highly recommend setting the schedule (see below) so that replication is performed multiple times per day.

- **(custom policy)**: Choose this if you are not replicating ShadowProtect data. By default it will just replicate everything.

**IMPORTANT**: If you are configuring replication on a source computer that has already been consolidating the ShadowProtect backup chain for a while, it is possible that some of the daily image files (*.cd.spi) will have already been consolidated. If this is the case, you will need to temporarily add an ‘include *.cm.spi’ policy rule to the bottom of your replication policy. Once the initial replication has completed, you can then remove this policy rule. This extra step is normally not needed, it is only necessary if the source computer has been consolidating the backup chain for a while (long enough for some of the daily image files to be deleted).

**EXTREMELY IMPORTANT**: If you are replicating ShadowProtect data, you must configure the ImageManager on both the replication source and the replication target to consolidate the backup images. If you do not, your backups will not be verified, you will run out of disk space, and your backups may eventually have a backup chain that is too long to be usable. Setting up the ImageManager is not optional and must be configured to ensure proper data protection.
Note that the ImageManager must be configured to add individually each folder that contains ShadowProtect data. It is not sufficient to add the parent directory – you have to add each subdirectory individually. See below for more detailed instructions.

Finally, use the Schedule page in the backup manager to set the network server backup schedule. If you are using the ShadowProtect Daily policy, replication should begin 1 hour after the ImageManager processing is configured to begin. Otherwise, choose an appropriate schedule. Usually once per day is sufficient, unless you are performing real-time replication.

**Configuring ImageManager on the Replication Target**

If you are replicating ShadowProtect backup data, then on the replication target you **must** setup the ImageManager to consolidate the replicated backup images. This must be configured for each computer that you are backing up with ShadowProtect.

To configure, login to the replication target server, and use the network backup manager program to check the top-level folder where you are storing replicated data. In the example in this document, the location is X:\ReplicatedData. We will use explorer to find the location(s) of the folder(s) that need to be added to the ImageManager program.

The top-level folder will contain 3 folders (each named after your brand ID). For example:

```
Name
- generic
- generic-del
- generic-sf
- local-backup-repository.identity.txt
```

You should ignore the folders that end in ‘-del’ and ‘-sf’ – the replicated data will be contained within the folder that is named after your brand ID (in this case, ‘generic’).

In the brand ID folder, there will be one subdirectory for each replication source that is storing data on this replication target (the directory names are the account numbers of each replication source). If you drill down into one of these account directories, you’ll see:

```
Name                  Date modified
- VolumeImages         7/6/2011 2:16 AM
- @@SoftwareSettings  7/6/2011 2:16 AM
- user.meta.info       7/5/2011 7:44 PM
```

There will be one sub-directory for each top-level folder in your folders list. In this case, VolumeImages is the folder that contains the ShadowProtect data. Inside, you’ll see:
Most of the folders contain metadata needed to efficiently replicate the data. The folder that contains the actual replicated data in the **replicated-data** folder, which is what we want.

Inside of the **replicated-data** folder will be the actual replicated data from the replication source. In this case, we are replicating ShadowProtect backup images for 3 servers, so we see:

These are the folders that we need to add to the ImageManager as managed folders. In our example, we would add the following folders:

- X:\ReplicatedData\generic\12345001\VolumeImages\replicated-data\ExchangeServer
- X:\ReplicatedData\generic\12345001\VolumeImages\replicated-data\PrimaryDomainController
- X:\ReplicatedData\generic\12345001\VolumeImages\replicated-data\SQLServer

For example, here is a screenshot on the replication target adding a folder for a replicated server inside of ImageManager:
You are free to use whatever ImageManager retention policy settings that you want on both the replication source and the replication target. This is unlike site to site and online backup of ShadowProtect data, where you are required to keep at least 35 days of daily delta files. Notwithstanding, we still highly recommend keeping at least 35 days of daily delta files even when you are using replication (the default is 90 days).

Consult the eFolder BDR documentation (or the StorageCraft documentation) for more information on how to add folders to the ImageManager and set retention settings.

**Backing up or Monitoring Replicated Data Stored on the Replication Target**

In certain scenarios you may want to backup the replicated data that is stored on the replication target server to an online backup storage cloud, to another site using site-to-site backup, or using the local disk feature to make an additional backup to a USB disk (or NAS).

Even if you do not wish to backup the replicated data further, if you are replicating ShadowProtect backup data, then we highly recommend configuring eFolder to monitor the replicated ShadowProtect backups so that you will be alerted if the consolidation process on the replication target server has problems.
To configure the backup or monitoring of the data, open the backup manager on the replication target server. Configure the My Account page with the same credentials that you used in the network backup server manager program (these credentials should be unique to this replication target server).

Next, in the backup manager, go to the Folders page and add the folder that is configured as the top-level data folder in the network backup server manager. In our example, this is X:\ReplicatedData.

Next, configure remote backups, site-to-site backups, or local disk backups like you normally would for other backups. This may include setting up an encryption pass phrase and setting the relevant backup schedules. If you are only setting up monitoring and not backup, then configure the backup manager to perform remote backups (later, there is a step to indicate that the data should only be monitored, but not actually backed up).

If the replication target contains ShadowProtect data, make sure that ShadowProtect monitoring is turned on by right clicking on the folder on the Folders page and choosing properties. Make sure that all of the ShadowProtect Integration settings are enabled:

If you don’t see these folder options, then check to make sure that the ShadowProtect management console is installed on the replication target server. If it is installed in a non-default location, you may have to manually tell the backup manager where to find certain ShadowProtect files. To do this, go to the Backup tab of the Options page, and change the Full Path to sbrun.exe and Full Path to ImageManager settings:
Finally, if you only want to monitor the replicated data but do not want to back it up, on the Folders page in the backup manager (on the replication target), right click the Folder and choose Properties. Under the Advanced section, set the **Do Not Backup Data** option to Yes:

![Advanced Settings](image)

**Restoring Replicated Data**

You can ‘restore’ (or download) data stored on the replication target back to the replication source by using the File Manager tool, just like you would with a normal backup.

Please note that data that is changed on the replication target will not be automatically downloaded to the replication source (automatic replication is one way only). If data has changed on the replication target, the File Manager tool can be used to download the changed data back to the replication source.

This can be useful for example if you virtualized an end-user’s server off-site on the replication target and you need to download the updated bare-metal backup image back to the end-user’s primary site. There is an option in the file manager that allows you to skip files that already exist on the client that are the same or more recent, so you can easily and quickly download only those files that need to be downloaded to bring the replication source up to date.

**Preloading Replicated Data**

Performing a preload (initial replication to USB disk) for replicated data is quite similar to the process of performing a preload for online backups. First, you configure the account, but instead of starting the initial replication, you do the following:

1. Use the web portal to put the account into maintenance mode.
2. In the backup manager on the replication source, go to the file menu and choose Preload Remote Backup (yes, even though we will be preloading replication).
3. In the dialog, choose a path to the external USB disk and click OK.
4. It will ask which backup destination you want to do a preload for. Choose the network server location.
5. It will start the initial replication job. Wait for it to finish.
6. When finished, physically transport the USB disk and attach it to the replication target.
7. On the replication target, in explorer open the USB disk and navigate to the top-level directory that contains the preload data. Then navigate into the `brandID` subdirectory (e.g., `generic`). There should be a single subdirectory that has the same name as the account number of the account you preloaded. Use explorer to copy this directory to the replication target underneath the `NetworkServerStoragePath\brandID` directory (for example, copy `E:\mypreload\generic\12345001` to `X:\ReplicatedData\generic`).
8. Finally, use the web portal to take the account out of maintenance mode.

**IMPORTANT**: Do not take the account out of maintenance mode until you have completed all of these steps. If you clear the maintenance flag early and the replication source attempts to replicate data, you will have to do the preload all over again.

Note that you can put multiple preloads onto the same USB disk. To do this, use a different top-level directory on the USB disk for each account that you preload. When you are finished preloading multiple accounts, on the replication target there should be multiple subdirectories of the `NetworkServerStoragePath\brandID` subdirectory, one for each account that was preloaded. For example, `X:\ReplicatedData\generic` could contain the subdirectories `12345001, 12345002, 12345003`.

**Replication to NAS Devices or USB Disks**

You can also replicate data to a USB disk or NAS device (or any filesystem accessible at the replication source). Setup a replication folder like you normally would, and then instead of (or in addition to) configuring network server backups, configure local disk backups. Folders that are marked as replicated folders will be stored in their original format on the destination filesystem instead of in eFolder’s proprietary backup format.

**Many to Many Replication**

If you need a replication source to replicate to multiple replication targets over the network, you should setup multiple settings profiles on the replication source. Note that you will need to use a different account for each of the settings profiles to ensure that monitoring and alerting continues to function properly for both of the replication jobs.

Note that using multiple settings profiles is not necessary if you want to replicate to one network destination and one local filesystem (as opposed to two network destinations).

**Conclusion**

eFolder’s replication technology allows you to efficiently and safely keep multiple copies of your customer’s data in multiple places.
**Additional Assistance**

We will assist you any way that we can. Please submit questions to support@efolder.net, call us at 800-352-0248, or browse our knowledge base at https://secure.efoldering.com/support/kb/