BDR for ShadowProtect Configuration Checklist

*(See the training video **How to Install and Configure an eFolder BDR for ShadowProtect** for details on each of the steps below.)*

Step 1. Setup physical configuration

- ☐ Unpack and check box for bare-metal recovery CD, power cord(s), mounting rails (if applicable)
- ☐ Physically mount BDR and connect to power source, monitor, and keyboard
- ☐ Cable and connect the BDR to the network
- ☐ Setup Lights-Out Management (iLOM) (Only available on the ST-2242, SR-2342, SR-2442, SR-3882)
  - ☐ Connect management ethernet port to switch
  - ☐ Assign IP address (default is DHCP; use BIOS to set static IP)
  - ☐ Login to https://ipaddress/ (username ADMIN password ADMIN) and change ADMIN password
- ☐ Power up the BDR

Step 2. Perform Windows configuration

- ☐ Complete the steps in the Windows Storage Server first-run setup wizard
- ☐ Log in to Windows as Administrator
- ☐ Perform any additional desired configuration tasks (such as configuring networking, renaming the server, installing additional management software, or joining the BDR to a domain)

Step 3. Verify configuration credentials

- ☐ Verify you have the following credentials: eFolder backup account, your encryption pass phrase, and the credentials for the computers that will be backed up

Step 4. Update the appliance software

- ☐ Download and install any BDR appliance monitoring software updates by double-clicking the **Update Software Appliance** icon on the desktop of the BDR

Step 5. Setup bare-metal backups

A. Perform preparatory work on machines to be backed up

- ☐ Ensure volumes are NOT dynamic volumes
- ☐ Be aware of Windows licensing and activation issues
- ☐ Defragment any heavily fragmented drives
- ☐ For domain controllers, document and synchronize the Directory Services Restore Mode password
- ☐ Identify legacy backup jobs and ensure they backup to separate partitions that will not be backed up by ShadowProtect
- ☐ Fully Document the operating system (or OS) version and Networking Settings
- ☐ For 32-bit servers, check the *IRPStackSize* registry parameter

B. Install the ShadowProtect Agent on each machine

- ☐ Decide on a push install or a manual install (For a small deployment—say, one to four agents—or for non-domain environments, the manual installation method is typically less work)
- ☐ Determine the type of license the customer will be using: MSP or Perpetual
- ☐ If needed, download the appropriate installer
- ☐ Perform a push or manual install on each machine to be backed up to install the ShadowProtect agent
- ☐ Reboot each computer (bare-metal backups will *not* be able to begin until the system has been rebooted)

C. Configure a continuous-incremental backup job to backup data from the source computers to a directory on the BDR that is unique to each computer

- ☐ Create a sub-folder in **X:\VolumeImages** or **X:\LocalVolumeImages** (if data is *not* going offsite) for each server
  - ➢ **<u>IMPORTANT</u>:** Make sure the volumes being backed up are **basic volumes**, *not* dynamic volumes

- ☐ Setup ShadowProtect continuous incremental backup jobs with compression set to high
- ☐ Start the initial backup
- ☐ Complete the other steps in this task (see the training video for details)

D. Configure the *ShadowProtect ImageManager* that is running on the BDR to monitor the directory that contains the bare-metal backup images for each computer you are backing up

- ➢ **Note:** This is crucial to monitor the integrity of the backups and to collapse incremental files to save storage space, both on the BDR and off-site.
- ☐ Log in to ImageManager and choose a time when ImageManager should collapse the deltas by clicking the **Agent Settings** button on the left side (for example, 12:05 a.m.)
  - ➢ **IMPORTANT**: On the **Global Retention** tab, you **must** keep daily image files (-cd) for at least 35 days (**must not be less than 35**)
- ☐ Complete this rest of this task (see the training video for details)

Step 6. Setup off-site monitoring and backups

- ☐ Configure the Backup Manager for monitoring and optional backups of the BDR data to the Cloud
  - ➢ **Note:** When configuring the schedule, set backups to occur about one hour after ImageManager does its work, (for example, 1:00 a.m.), even if you are only backing up locally
- ☐ Perform the initial backup
  - ➢ **Tip**: You may want to first run incremental backups for a few days to ensure deltas are reasonably sized
- ☐ Perform a USB preload for off-site backups to the cloud if the total amount of data to backup is too large to quickly backup over the Internet
  - ☐ Put account into maintenance mode using the eFolder Web Portal
  - ☐ Attach the USB drive to the BDR
  - ☐ Run the preload by starting the Backup Manager and selecting *Preload Remote Backup* in the **File** main menu option
  - ➢ Submit a ticket to ask for the shipping address, print the prepaid return label, and reply to the ticket with the tracking numbers

Step 7. (Optional) Setup cross-site replication

- ☐ Configure the replication target to receive replicated data
- ☐ Configure the replication source machine
  - ☐ Configure the Backup Manager on the source machine to monitor replication
  - ☐ Configure the Backup Manager on the source machine for replication
- ☐ Configure ImageManager on the replication target server
  - ☐ Add a folder for each server in ImageManager
  - ☐ Optionally, customize retention settings for each folder
    - ➢ **IMPORTANT**: You **must** keep daily image files (-cd) for at least 35 days (**must not be less than 35**)
- ☐ Configure data monitoring on the replication target
- ☐ (Optional) Perform a USB preload for replicated data

Step 8. (Optional) Setup notifications

- ☐ Configure partner-wide notifications by selecting the **Notifications** option in the **My Partnership** main menu option in the Web Portal (this is only available to partners)
- ☐ Optionally, configure notification email address(es) in the Online Backup Manager program

Step 9. (Optional but highly recommended) Test file restores and virtualization

- ☐ Test file and folder restores
- ☐ Test the virtualization of servers by virtualizing each server in Test Mode; then delete the virtual machine