IDrive® BMR

User Guide

Explore the features offered by IDrive BMR to get started with your disaster recovery plan.
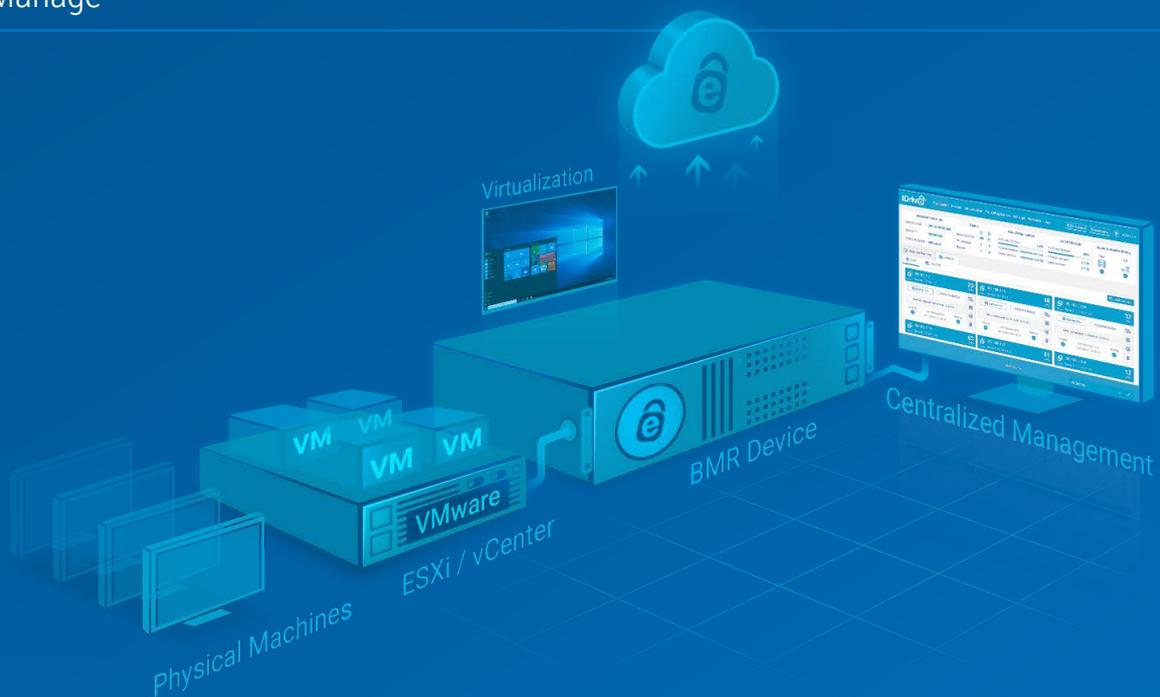
IDrive® BMR

Overview

IDrive offers the most cost-effective BMR functionality for SMBs. You can backup the entire computer including the Operating System and Application configurations to the BMR server and retrieve them in case of catastrophic failure.

We can achieve restores from backed up data in 3 ways:

1. If you quickly need some files/folders from the backup, you can use the file-level restore method.

2. For a complete system restore to the same machine or a new target machine, you can perform a bare-metal restore.

3. For faster recovery and business continuity, you can create a virtual instance of the backed-up machine on the BMR server directly.

You can also transfer backups stored on your IDrive BMR server to an offsite location through cloud replication. You have to enable the cloud replication feature by providing the IDrive account credentials. Once enabled, you are provided with the necessary interface to configure cloud replication schedule settings and monitor the backup status through the centralized web console.

You can expedite initial bulk data transfer through Cloud Seeding. Transfer large volumes of data stored on the BMR server to your cloud account using an external storage device that will be shipped to you. This ensures fast transfer and zero bandwidth consumption.

Sign in

Sign in to the IDrive BMR server web interface from a computer that is on the same LAN as the BMR server. You can connect using the BMR server IP as the application URL and manage backups and restores of the registered machines. Alternatively, use the serial key of the BMR device in small-case, followed by **'.local'** as the application URL. If you do not know the IP address or the serial key, you can navigate to bmrdevice.idrive.com on your browser and get a list of all the BMR servers that are online on your network. Click on the IP address of the required BMR server and you will be redirected to the sign-in page of the BMR server interface.

For the initial sign in, use 'support123' as the password. We highly recommend you to change the default password after the initial sign in to the BMR server web interface.

Encryption settings

When you set up the BMR server for the first time, you will be prompted to configure your encryption settings.

You can choose either of the following encryption methods:

Default Encryption: IDrive BMR will set an encryption key to encrypt all your data.

Private Encryption: This option will allow you to set a self-defined encryption key.
(This is the recommended option.)

BMR uses AES-256 CCM encryption to secure your data when stored on the BMR server and the cloud. Your data is also encrypted during the transfer to the cloud account; thereby, ensuring adequate protection for your data.

It is recommended to set a Private Encryption Key for enhanced security. This key is not stored anywhere on IDrive Cloud servers and therefore, it cannot be retrieved, if lost. Ensure that you store this key safely for continued access to your data.

To configure encryption on your BMR server,

1. Sign in to the BMR web interface with your credentials.

2. Once you sign in, you will be prompted with a message to configure your server with encryption. Choose default encryption or private encryption based on your requirements.

3. To set 'Default encryption key', click 'Continue'.

4. Alternatively, to set 'Private encryption key', enter a private encryption key of your choice in the respective field, and confirm the same. Click 'Continue'.

   Note:

   - *Once you set the encryption key (default or private), you will not be able to change this key in the future.*

   - *BMR does not store your private encryption key on its servers. It uses a special technique to encrypt your private encryption key so that it can be verified but not retrieved.*

- *It is recommended that you archive it safely. Without your private encryption key, you will not be able to retrieve your data. We will not be able to provide private encryption key information.*

Forgot password

This option lets you reset the password that you use to sign in to your BMR server web interface.

To change the password,

1. On the 'Sign in' page, click 'Forgot Password'.

2. Click 'Confirm' in the confirmation window. An email with the security code will be sent to the registered email address.

3. Enter the security code and click 'Verify'.

4. Enter the new password, confirm the same, and click 'Reset password'.

A confirmation message will be displayed on the top.

Note: If you do not receive an email with a security code, click 'Resend security code' to resend the email. After this, if you still do not receive the mail, it could be due to the following reasons:

- *You may be checking the wrong email account. The address provided when placing the request for the device is the default email address for notification.*

- *Your incoming email server might be rejecting the message.*

Admin

You can update the profile information such as the primary email address and password from this option.

Change Password

To change the password,

1. Sign in to the IDrive BMR server web interface.

2. Click 'Admin' displayed on the top-right corner of the page.

3. Click 'Change Password'.

4. Enter the new password, confirm the same, and click 'Change Password'. Once this is completed, you will receive a success notification.

Update Primary Email

To update your registered email address, sign in to the IDrive BMR server web interface.

1. Click 'Admin' displayed on the top-right corner of the page.

2. Click 'Email Settings'.

3. In the 'Email Notification' tab, click ✏️, and enter the new email address.

4. Click 'Save' to update the changes.

Power Options

You can perform the power operations of the IDrive BMR server from this tab. Following are the two available power options:

✔ **Restart -** Click this to restart the server.

✔ **Shutdown -** Click this to shut down the server.

Support

This section details the support options available for our product along with the contact and chat - support information.

Dashboard

The 'Dashboard' tab displays important information about backup status, activities, registered physical or virtual machines, and devices mounted for restore. Also, the dashboard provides an overview of the storage used, virtualization, cloud replication, and the health status of the devices. You can also enable cloud manage from here.

Device Information

The 'Device Information' section displays the unique serial number of the BMR server and networking information.

Status

The total number of registered physical client machines and VMware Virtual machines on the server and the number of restore mounts are displayed here.

Cloud Replication

This section displays the used quota of your BMR cloud space and the date and time of the cloud backup operation. You can click this section to go to the 'Cloud Replication' tab.

Local Storage

The 'Local Storage' section displays the consumed storage space and the date and time of the last local backup operation.

System Health Status

The 'System Health Status' displays the health status of the storage RAID array and the individual health status of the OS hard drive.

Health status and what they indicate:

- ✅ The drives are working fine.
- 🔺 Failure detected. Contact the support team immediately.
- ⚠️ Bad; contact the support team immediately.

    Note:

    - *The status 'Warning' doesn't always imply that there is a critical problem with the RAID storage array. Once you contact the support team, they will analyze the required reports and let you know if there is any issue and provide the necessary information to resolve them.*

    - *A unique serial number will be provided to each storage device to identify and replace them if the health status is bad.*

Download Backup Agent

Download the agent software from 'Downloads' and install it on the computer you want to backup. IDrive BMR server auto-detects the agent and starts image backup automatically for the first time, according to the schedule. For more information on image backup, refer to Backup Instructions.

System Requirements for IDrive BMR

IDrive BMR supports bare-metal backup from physical clients and VMware machines running on Windows OS.

The system requirements for IDrive BMR include the following:

Operating Systems:

- ✔ Windows Vista (with all Windows updates installed)
- ✔ Windows Server 2008 (with all Windows updates installed)
- ✔ Windows Server 2008 R2
- ✔ Windows 7
- ✔ Small Business Server 2011 (with all Windows updates installed)
- ✔ Windows 8
- ✔ Windows 8.1
- ✔ Windows 10
- ✔ Windows Server 2012
- ✔ Windows Server 2012 R2
- ✔ Windows Server 2016
- ✔ Windows Server 2019

  Note: CBT backup for faster incremental is not supported on Windows Vista and Windows Server 2008.

Filesystem:
IDrive BMR supports backup from only NTFS formatted volumes

Disk Partition Style:
- ✔ MBR
- ✔ GPT

VMware versions:

ESXi: Versions 5.5, 6.0 and 6.5 are supported

vCenter: Versions 5.5, 6.0 and 6.5 are supported

Note:

- *You can backup dynamic or logical volumes in an MBR disk. However, the bare-metal restore of these volumes is not supported. You can still recover data from these backed up volumes by using the 'File Restore' option. Refer steps to recover backed up data using file restore option.*

- *Virtualization may also be supported for certain configurations involving dynamic and logical volumes on MBR disk.*

- *Bare-metal restore is not supported for the data backed up from client machines with software RAID-based storage. However, you can still perform a file-level restore of the backed up data to the client machine.*

Physical Machines

This section displays all the registered clients and the groups created by admin.

Clients

This section displays the following information for registered clients:

- ✔ Hostname: Name of the client added for backup
- ✔ Status: Displays the online or offline status of the clients
- ✔ Last Backup Time: Displays the date and time of the recent backup for the client
- ✔ Integrity Status: Displays the integrity status of the client
- ✔ Local Backup Status: Displays the overall backup per client

Status and what they indicate:

- ✅ Backups are running fine
- ⚠️ No recent backup, if there is no backup from a long time

Add Client

The server is designed in such a way that it automatically detects and registers a client if the agent software is installed on the client. However, if the server has not detected the client you can use the 'Add Client' option to manually add the client by its IP address.

To add a client manually,

1. On the 'Dashboard' tab, click 'Add Client'.

2. In the 'Add client' page, enter the IP address of the client to be added, and click 'Add Client'.

Once the client is added manually, it will be displayed in the 'Discover new client via IP' section on the 'Dashboard' tab.

Discover new client via IP

This section displays the list of manually added clients and their connection status. If the connection status is 'No', it could be because of the following reasons:

- ✔ The client and the server are not in the same LAN.
- ✔ The agent software is not installed on the client.

There could be firewall restrictions on the client blocking the server from detecting the agent software.

Global Server Settings

This tab allows you to configure the server-wide settings related to physical machine backup.

You can change the following server settings from this tab:

Max simultaneous backups - This option will limit the maximum number of backups allowed at a time.

Max recently active clients - 'Max recently active clients' helps you manage your local storage space by setting a limit on the number of active clients, for adding a new client to the server.

This tab allows you to configure the server-wide settings related to physical machine backup.

Note:

- *The 'Max recently active clients' limit is applicable only when adding a new client. Even if one or more inactive clients turn online later and the limit is exceeded, the backup operations will continue as usual.*

- *A client that has been offline for longer than 2 months is considered inactive.*

Max local network backup speed - Specify the bandwidth throttle to set the local network usage during backup.

Global soft file system quota - Set the storage utilization limit upon reaching which the server will initiate a cleanup. For more information, refer to FAQ.

Cleanup time window - Schedule the cleanup operation from this section. The server will delete the old backups based on your backup retention settings and any incomplete backup, to help you manage your storage space. You can schedule daily /weekday / weekend cleanups or even custom-schedule by selecting the days and hours as required.

To modify global settings for physical machines,

1. Sign in to the BMR server.
2. Go to the 'Dashboard' tab and click 　　.
3. Set the Max simultaneous backups, Max local network backup speed, and Global soft filesystem quota for physical machines.
4. Schedule the cleanup of old backups in the BMR server, in the 'Cleanup time window' section
5. Click 'Save & Close'.

Backup Settings

This tab allows you to configure your global, client, and group backup schedule and settings for physical machines.

You can change the following settings related to backing up of physical machines:

Set backup interval - Set the interval between two consecutive backups of a physical machine.

Max backup speed - Select the 'Don't Limit' radio button to allow unrestricted network bandwidth for backups or select the 'Limit To' radio button and set the local network bandwidth for backup in MBit/s.

Volumes - Choose to backup 'All' volumes of your client machines or select 'Custom' and specify the drives for backup, separated by commas. C: Drive is considered for backup by default and therefore does not need to be specified.

Note: Take care to specify the correct volumes for backup, especially when modifying global settings for backup. If volumes that do not exist are specified, the backup will fail.

Backup retention settings - Set the minimum and the maximum number of image backups the server should retain for a physical machine. The old backups will be removed during the cleanup operation.

Schedule backup - Schedule backups as 'Daily', on 'Weekdays', or on 'Weekends'. You can also select 'Custom' and select the days for backup. Also, set the 'Start Time' and 'End Time' for backups.

Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

Force full image backup - You can select the 'Force a full image backup after every _' checkbox and select the interval for forcing a full image backup.

To modify client settings for physical machines, sign in to the BMR server.

1. Go to the 'Dashboard' tab and click [icon].
2. Select the backup interval, max backup speed, and backup retention settings.
3. Specify the volumes for backup.
4. Schedule the backup by specifying the days and time.
5. Click 'Save & Close'.

Groups

A group is a collection of client machines organized together by the admin. You can create up to 30 groups, and one client machine cannot be added to more than one group.

This section displays all the created groups and the number of client machines added to the group. You can perform full or incremental image backup, and schedule them from the created groups.

Create Group

This option lets you create groups and add client machines to them. A group can have up to 25 client machines and you can create a maximum of 30 groups.

To create a group,

1. Sign in to the IDrive BMR server web interface and click 'Groups' on the 'Dashboard' tab.

2. Click 'Create Group'.

3. Enter the name of the group in the 'Group Name' field.

4. Click 'Create group'.

Group Operations

You can perform the following operations for the created group:

✔ Add or remove client machines.

✔ Perform full or incremental image backup.

✔ Configure backup settings and schedule local backup.

✔ Delete the group.

To add client machines to an existing group,

1. Sign in to the IDrive BMR server web interface and click 'Groups' on the 'Dashboard' tab. The created groups appear in the 'Groups' tab.

2. Click 👥✏ in the required group section. The 'Manage User Groups' page appears.

3. Select client machines from the list displayed list in the 'Choose host machines' section under the 'Add' tab.

4. Click 'Save'.

To remove client machines from a group,

1. Sign in to the IDrive BMR server web interface and click 'Groups' on the 'Dashboard' tab. The created groups appear in the 'Groups' tab.

2. Click 👥✏ in the required group section and go to the 'Remove' tab.

3. Select the client machines to remove from the 'Choose host machines' section.

4. Click 'Remove'.

To perform full or incremental image backup,

1. Go to the 'Dashboard' page.

2. Go to 'Physical Machines' > 'Groups'. Here the groups are displayed.

3. Click 'Backup Now' or select 'Force Full Backup' checkbox in the required group to start the backup.

To apply local backup settings to a group,

1. Go to 'Dashboard' > 'Physical Machines' > 'Groups'. The created groups are displayed.
2. Click in the required group section. The 'Backup settings' page appears.
3. Set the backup interval and max backup speed. Choose the 'Backup retention settings' and schedule the backup.
4. Set the 'Volumes' you wish to backup as 'All' or select 'Custom' and specify the volumes you want to backup.

   Note: Take care to specify the correct volumes for backup, especially when modifying global settings for backup. If volumes that do not exist are specified, the backup will fail.

5. Click 'Save & Close'

To delete a group,

1. Sign in to the IDrive BMR server web interface and click 'Groups' on the 'Dashboard' tab. The created groups appear in the 'Groups' tab.
2. Click in the required group section.
3. Click 'Yes' in the confirmation window.

   Note: When you delete a group, the applied settings will be lost and all the client machines of that group will adopt global backup settings.

Activities

This section displays information about ongoing local backups or restore operations of the physical machines. During a physical machine backup operation, you will be provided with the following options:

1. Stop - Click to force stop the ongoing local backup
2. Show Logs - Click to view the detailed information of local backup

VMware
You can backup all the registered virtual machines running on ESXi and vCenter from this section.

ESXi
This section displays the VMs running on ESXi hosts, added for backup to the BMR server.

Add ESXi Host

You need to add VMware ESXi host to the BMR server to backup data from virtual machines.

To add ESXi host,

1. Sign in to the IDrive BMR server web interface.

2. Go to the 'VMware' tab and click 'Add ESXi Host'.

3. Provide details such as, ESXi name, IP address, username, and password and click 'Next'.

4. Select the required virtual machines and click 'Next'.

5. Set the required backup schedule parameters in the respective tabs and click 'Next'. (Select 'Disable Schedule' if you want to disable the schedule.)

6. A summary of the backup operation is displayed. The backup of the VMs will be performed as per the schedule.

Once this is completed, the ESXi is added to the BMR server and backup for running VMs will occur as per the schedule. You can perform immediate full / incremental backup, change backup schedule, view integrity and backup status, last backup time for each ESXi host. You can add new VMs to an ESXi host.

To add VMs to the VMware ESXi,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'->'ESXi'.

3. Click 'Add VMs' on the required ESXi.

4. Select the required VMs to add and click 'Next'.

5. Verify the details and click 'Confirm'.

To perform an immediate backup,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'-> 'ESXi'.

3. Click 'Backup Now' or select the 'Force Full Backup' checkbox to perform an immediate incremental or full image backup respectively.

To reschedule data backup for an ESXi host,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'->'ESXi'.

3. Click ⊞ on the required ESXi Host.

4. On the 'Schedule Backup' screen, change the required parameters. You can click 'Disable Schedule' to disable the schedule.

5. Click 'Confirm' to save the changes.

To delete an ESXi host,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'-> 'ESXi'.

3. Click 🗑 on the required ESXi Host.

4. Click 'Yes' in the confirmation window.

Note: The list of deleted ESXi hosts will be displayed at the bottom of the page and all the data will be permanently removed from the server during cleanup. You can click 'Do not remove' to retain the required ESXi host.

vCenter

This section displays the VMs running on the vCenter server, added for backup to the BMR server.

Add vCenter server

You can backup data from virtual machines running on VMware vCenter server. All you need to do is add the vCenter server to the BMR server and schedule the backup. In the case of multiple ESXi hosts managed by a single vCenter server, this is the recommended method of adding all the ESXi hosts at a time.

To add a vCenter server,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware Backup' -> 'vCenter'.

3. Click 'Add vCenter Server'.

4. Provide details such as, vCenter name, IP address, username, and password and click 'Next'.

5. Select the required virtual machines and click 'Next'.

6. Set full or incremental backup schedule parameters in the respective tab and click 'Next'.

7. Verify the details and click 'Confirm' to add.

You can view the existing schedule for full image and incremental backup, change the schedule for backup, integrity and backup status, last backup time for each vCenter server. You can also add new VMs to a vCenter Server.

To add VMs to the VMware vCenter,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'->'vCenter'.

3. Click 'Add VMs' on the required vCenter tile.

4. Select the required VMs to add and click 'Next'.

5. Verify the details and click 'Confirm'.

To perform an immediate backup,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'-> 'vCenter'.

3. Click 'Backup Now' or select the 'Force Full Backup' checkbox to perform an immediate incremental or full image backup respectively.

To reschedule data backup,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'->'vCenter'.

3. Click ⊞⚙ on the required vCenter.

4. On the 'Schedule Backup' screen, change the required parameters. You can click 'Disable Schedule' to disable the schedule.

5. Click 'Confirm' to save the changes.

To delete a vCenter server,

1. Sign in to the IDrive BMR server web interface.

2. Go to 'VMware'->'vCenter'.

3. Click 🗑 on the required vCenter.

4. Click 'Yes' in the confirmation window.

    Note: The list of deleted vCenter servers will be displayed at the bottom of the page and all the data will be permanently removed from the server during cleanup. You can click 'Do not remove' to retain the required vCenter server.

Restore

This tab lets you restore data backups to the clients and the virtual machines running on VMware ESXi host or vCenter server. You can also perform file-level restore by creating a network share for the recovery points.

File Restore

You can access all backed up data by using the file restore option. a network share from the recovery points to access the backed up data from this section.

To create a network share path for the recovery point,

1. On the 'File Restore' tab, select the client from 'Choose a System' drop-down menu.

2. Select the recovery point from the 'Choose Recovery Point' drop-down menu.

3. Specify the volume(s).

4. By default 'Enable user authentication' will be selected as 'No'. This will create an open share that is accessible on the network. However, if you want the share to be secured, we recommend you to create it with username and password. To create a secure share, select 'yes' and perform the following steps:

    a. Select the username from the 'Mount username' drop-down menu.

    b. Enter the mount password.

5. Click 'Create'. The network share is created using the CIFS / SMB protocol.

    Note: You can create a maximum of 5 simultaneous network shares from the recovery points, irrespective of the authentication type selected.

Mount Path Summary

Once the network share for the recovery point is successfully created, a summary of it will be displayed in the 'Mount Path Summary' table. You can use the path displayed under 'Mount Path' to access your backed up data.

WinRE Restore

Setup instructions to build WinRE recovery media

To build WinRE recovery media for future use,

1. Launch the setup.
2. Select 'Future Use'.
3. Select the ISO image from the 'Browse' button.
4. Click 'Next'.
5. The ISO progress will be displayed on the page.
6. You will receive a success message once the ISO build is completed. Enter the IP address and click 'Next'.
7. You will be directed to the sign in page. Enter your account credentials and click 'Next'.
8. The upload progress will be displayed.
9. You will be notified once the upload is completed.

To build WinRE recovery media for immediate use,

Refer the steps given below to create a bootable CD or USB with the recovery media, for immediate use.

1. Navigate to 'Downloads' > 'BMR Recovery Builder'.
2. Launch the setup.
3. Select 'Immediate Use'.
4. Choose 'Create a Bootable ISO file' and select the ISO image from the browse button and click 'Next'.
5. The ISO progress will be displayed on the page.
6. You will receive a success message once the ISO build is completed.

To create a bootable USB for immediate use,

1. Select 'Create a bootable USB'. Then select the partition style and the USB device from the respective drop-down menus to create the boot device and click 'Next'.
2. The USB creation progress will be displayed.
3. You will be notified once the USB bootable device is successfully created along with further instructions to use the bootable device.

   Note:

   - *If the setup is not able to find the wim file, you will be prompted to download ADK after selecting future use or immediate use option.*
   - *The new page that appears will ask the user to download ADK from the link given in the instruction. After the ADK setup is completed the next button will be enabled.*
   - *Click 'Next' to proceed with the aforementioned options.*

Steps to perform WinRE Restore

You can restore data to a target machine that is connected to the same network as that of your BMR server. Create a bootable USB or media device using the WinRE builder app. Then boot your target replacement machine using the USB or media device.

Pre-requisites for performing a WinRE Restore:

1. USB drive with a minimum of 4 GB storage - to create USB recovery media.

2. Ensure that the drives on your target computer are healthy (run SMART checks on the drives if necessary).

3. The target computer must be bootable from a USB storage device.

4. The BMR server and the target computer should be inside the same LAN.

5. The target computer should have a wired network connection to the LAN (DHCP is recommended).

6. If the target computer has hardware RAID, it should be configured before initiating the restore process.

For optimal performance during bare-metal restore, stop any on-going backup operation.

Note:

1. *After restoring a machine, Windows may prompt to re-activate your license.*

2. *Bare-metal recovery of simple, mirrored, spanned, and striped dynamic volumes are supported by version 8.4.0 and above, given the dynamic disk has an MBR and not GPT partition style.*

To initiate restore,

1. Connect to the BMR server.

   a. With the 'Auto-detect IP Address' option (recommended), you can connect automatically to any available BMR server within the network.

   b. With the 'Specific IP Address' option, you can connect to a particular BMR server. This is useful when you want to connect to a specific server in a network having multiple BMR servers installed.

2. Sign in to the BMR server with your user credentials.

3. Choose the system and recovery point from the respective drop-down menu.

4. Choose the appropriate volume option and then click 'Next'.

   Note: If you click the 'Back' button on this page, you will be signed out of the server. You will have to sign in again to the server.

5. Select a destination drive.

   Note: Once the restore process is initiated, any previously existing data on the chosen destination drive will be deleted.

6. You will receive a confirmation message when the restore is completed.

VMware Restore

This tab allows you to restore the VMs to the ESXi host or vCenter server.

To restore a VM running on ESXi host,

1. Sign in to the IDrive BMR server web interface and go to the 'Restore' tab.

2. Go to 'VMware Restore'>'ESXi'.

3. Select 'VM restore'.

4. Select the required ESXi host you want to restore.

5. Select a VM and the required recovery point.

6. Select 'Same VM' if you wish to restore data to the selected VM.

7. To restore data to another VM, select 'New VM'. In the 'New VM' section, select an ESXi host, enter a name for the VM, and select a data store.

   Note: The required ESXi host needs to be on the BMR server.

8. Click 'Restore'.

9. The progress is displayed in the 'Activities' section.

   Note: In some cases, the progress may take some time to appear.

To restore a VM running on vCenter server,

1. Sign in to the IDrive BMR server web interface and go to the 'Restore' tab.

2. Go to 'VMware Restore'->'vCenter'.

3. Select 'VM restore'.

4. Select the required vCenter server you want to restore.

5. Select an ESXi host.

6. Select a VM and the required recovery point.

7. Select 'Same VM' if you wish to restore data to the selected VM.

8. To restore data to another VM, select 'New VM'. In the 'New VM' section, select a vCenter server and the required ESXi host for the new VM, enter a name for the VM, and select a data store.

   Note: The required vCenter server needs to be on the BMR server.

9. Click 'Restore'.

10. The progress is displayed in the 'Activities' section.

    Note: In some cases, the progress may take some time to appear.

You can view the detailed restore progress in the 'Activities' section.

You can also restore individual files/folders, irrespective of the type of the operating system on the VM.

To restore individual files/folders from a backed-up virtual machine on the ESXi host,

1. Sign in to the IDrive BMR server web interface and go to the 'Restore' tab.

2. Go to 'VMware Restore'->'ESXi'.

3. Select 'File restore'.

4. Select the required ESXi host you want to restore.

5. Select a VM and the required recovery point.

6. Select the username and enter the password.

7. Click 'Create Mount' to initiate the restore process.

To restore individual files/folders from a backed-up virtual machine on the vCenter server,

1. Sign in to the IDrive BMR server web interface and go to the 'Restore' tab.

2. Go to 'VMware Restore'-> 'vCenter'.

3. Select 'File restore'.

4. Select the required vCenter server you want to restore.

5. Select an ESXi host.

6. Select a VM and the required recovery point.

7. Select the mount username and enter the password.

8. Click 'Create Mount' to initiate the restore process.

Virtualizaton

This tab allows you to create a virtual instance of the backed-up physical machines and VMware virtual machines on your BMR server, in case of any physical damage or disaster. You can create a maximum of four virtual machines at a time.

Local Virtualization

You can create a virtual instance of your physical machine and VMware's virtual machine from this section using the KVM hypervisor.

To create a virtual instance of a physical machine,

1. Sign in to the IDrive BMR server web interface.

2. On the 'Virtualization' tab, click the 'Create a Virtual Machine' button. A new pop-up will appear.

3. On the 'Physical Machines' tab, select the required client from the 'Choose a System' drop-down menu.

4. Choose a recovery point.

5. Select the number of processors for the virtual machine.

6. Allocate required memory for the virtual machine in the 'Memory' field.

    Note: Memory value should be greater than 512 MB. You can decide the memory value depending on the available memory displayed below the 'Memory' field.

7. Select a network source.

8. Next, select the appropriate network model.

9. Choose the required storage controller for the virtual machine.

10. Select a graphics option from the drop-down menu.

11. Click 'Build Virtual Machine'.

Once this is completed, your virtual machine is built. You can now connect to it and access data.

To connect,

1. In the 'Virtual Machines' section, click the 'Copy VNC Password' button on the right-hand side.

2. Click against the virtual machine.

3. In the new window that appears, paste the password. Click 'Send Password'.

Remote connection to the virtual machine will be established.

Note: All the created virtual instances will be unmounted and the changes made in the virtual machine will be lost when you restart your IDrive BMR server. You can also click to unmount the virtual machine manually.

To create a virtual instance of your VMware server,

1. Sign in to the IDrive BMR server web interface.

2. On the 'Virtualization' tab, click the 'Create a Virtual Machine' button. A new pop-up appears.

3. In the 'VMware' tab, choose the required server from the 'Choose Server' drop-down menu.

4. Select the ESXi Host from the 'Choose ESXI Host' drop-down menu.

5. Select a VM from the 'Choose VM' list.

6. Choose the recovery point that will be used to create the virtual instance.

7. Specify the boot firmware. Refer to the virtual machine's hardware configuration on the VMware server to set the firmware to UEFI or Legacy BIOS.

8. Assign the number of processors for the virtual machine from the 'Processors' drop-down menu.

9. Allocate required memory for the virtual machine in the 'Memory' field.

    Note: Memory value should be greater than 512 MB. You can decide the memory value depending on the available memory displayed below the 'Memory' field.

10. Select a network source.

11. Next, select the appropriate network model.

12. Choose the required storage controller for the virtual machine.

13. Select a graphics option from the drop-down menu.

14. Click 'Build Virtual Machine'.

Once this is completed, your virtual machine is built. You can now connect to it and access data.

To connect,

1. In the 'Virtual Machines' section, click the 'Copy VNC Password' button on the right-hand side.

2. Click against the virtual machine.

3. In the new window that appears, paste the password. Click 'Send Password'.

A remote connection to the virtual machine will be established.

Note: All the created virtual instances will be unmounted and the changes made in the virtual machine will be lost when you restart your IDrive BMR server. You can also click to unmount the virtual machine manually.

Virtual Machines

This section displays the created virtual machines of your physical machines and VMware virtual machines. You can perform power operations on the virtual machine. Also, you can restart the machine, send the keyboard inputs such as windows, Ctrl+Alt+Del, Alt+Tab, and F8 to the virtual machine.

To perform power operations,

1. Sign in to the IDrive BMR web interface and go to the 'Virtualization' tab.

2. Click to power on the machine

3. Click to power off the machine.

4. You will be prompted with a confirmation window. Click 'Force Shutdown'.

   Note: Use the shutdown option in the OS of the virtual instance to shut down the machine. Force shutdown from the BMR server interface only as a last resort when facing system issues.

To restart a virtual machine,

1. Click [⟳] in the menu of the required virtual machine.

2. You will be prompted with a confirmation. Click 'Restart'.

Reconfigure a virtual instance

Typically, to reconfigure the hardware of a virtual instance, you will need to backup the virtual instance and create a new virtual instance with the backed-up data. You can skip this hassle with IDrive BMR as you can simply shut down the virtual instance and click 'Configure' to reconfigure the hardware parameters.

You can reconfigure the following parameters of a virtual instance:

Specify the boot firmware - Change the boot firmware to BIOS / UEFI. (applicable on for virtual instances for VMware machines)

Processors - Use the 'Processors' drop-down list to reassign the number of processors for the virtual machine.

RAM - Reallocate the required memory for the virtual machine.

Network Source - Change the network source and reassign a network model if needed.

Storage Controller - Change the required storage controller for the virtual machine.

Graphics - Update the graphics option from the drop-down.

Install performance-enhancing drivers

Configure your virtual instances with performance-enhancing drives to achieve better performance.

To install performance-enhancing drivers for a virtual instance,

1. Shut down the virtual instance and click 'Configure'.

2. Attach the ISO file (virtio-drivers(For_Windows_VMs).iso) containing high-performance drivers for network and graphics hardware in the virtual instance and click 'Save'.

3. Power-on the virtual instance.

4. Use the 'Device Manager' to locate the drivers on the attached ISO file.

5. Install the necessary drivers using the 'Update Driver Software' wizard.

6. Upon completion, reboot to begin using the virtual instance with the enhanced drivers.

For more detailed information, refer to Install performance-enhancing drivers for a virtual instance.

Troubleshooting: Windows OS booting issues in a virtual instance

In the case of OS boot issues during virtualization, especially for Windows OS, you can upload the pre-built Windows recovery media to correct the boot issues. You can also build a WinRE recovery media for immediate use.

Note:

- *IDrive BMR does not provide the OS recovery media.*

- *The total upload limit is 20 GB.*

To upload recovery media, for future use in case of boot issues,

1. Shut down the virtual instance and click 'Configure'.

2. Click 'Upload ISO Image'.

3. Browse and choose the OS recovery ISO file and click 'Upload'.

4. To view the ISO files uploaded to BMR, click the 'Uploaded Files List'. (virtio-drivers(For_Windows_VMs). iso) is available by default and cannot be deleted.

To troubleshoot booting issues in a virtual instance,

1. Shut down the virtual instance and click 'Configure'.

2. Enable 'Attach ISO', and select the relevant OS recovery ISO file.

3. Configure the virtual machine's boot order to 'CD/DVD-ROM', set up boot menu timeout if necessary, and repair the operating system boot issues.

   Note: It is recommended to set a boot timeout of 10 seconds or above.

4. Once the boot issue is resolved, change the boot order to 'Hard Disk' and detach the ISO file.

5. Reboot your virtual instance.

Cloud Replication

The Cloud Replication tab lets you replicate the data backed up from your physical as well as VMware machines in your server to the cloud account and even schedule cloud replication. Additionally you can use the cloud seeding service, IDrive BMR Express, to transfer data to your cloud account from the BMR server via an external device from this tab.

Note: Cloud Seeding via IDrive BMR Express is currently not supported by IDrive BMR version 7.0.0 and above.

IDrive Cloud

Replicate data stored on your BMR server to the cloud account over the Internet or even schedule the cloud replication for the required physical clients and VMware machines from this tab.

View Logs

The 'View Logs' option here would take you to a page with a comprehensive log of cloud replication activities of your physical clients and VMware machines.

Activities

This section displays the ongoing cloud replication status. Information such as hostname, drive selected for backup, recovery point, the amount of data transferred to the cloud, time taken for backup, Internet speed, and the estimated time for backup are displayed.

Cloud Replication Settings

You can schedule cloud replication from this section.

The following options available to schedule cloud replication:

Select clients for manual backup - Select clients from the drop-down menu to perform an immediate backup. Click 'Backup Now'.

Select clients to backup - Select the required physical machines. Click 'Select All' to select all the computers.

Select ESXi/vCenter VMs for backup - Select the required ESXi host or vCenter server for backup.

Scheduled backup time - Set the time at which your scheduled backup should start. Select'Daily' to perform the backup every day or select the specific days for the backup to run.

Backup end-time - Disable cut-off on backup end time or configure a soft or hard cut-off for the end time.

Note: Hard cut-off will terminate backup on the specified end time. For soft-cut off the actual end time is dependent on the ongoing tasks that are in progress.

Bandwidth throttle - Enter the bandwidth throttle value to set the Internet usage for your backups. By default, this value will be set to 100 MBit/s.

Note: Bandwidth throttle value should be between 1-1000 MBit/s.

Schedule summary

This section displays a summary of the scheduled backups. Information such as computers selected for backup, day, and time of the next scheduled backup will be displayed.

Click 'Delete Schedule' to delete all upcoming scheduled backups.

IDrive Account Information

This section provides information about your IDrive cloud account to which the data will be transferred. Information such as username and account status will be displayed.

Cloud Replication Status

This section displays the status of the last backup, including information such as hostname/VM name, last backup time, and the size of the data transferred. You can even search for the required hostname and server by using the search field.

Last Backup Log

View detailed information on the last cloud replication from the 'Last Backup Log' section.

Cloud Seeding

You can quickly transfer large amounts of data stored on the BMR server including data from physical clients and VMware machines to the cloud via physical shipment of a temporary storage device, from this tab.

Note: Cloud Seeding is currently not supported by IDrive BMR version 7.0.0 and above.

Placing an order for BMR Express device

Fill out the shipment form with all the necessary information including a key, which will be used to encrypt your data for enhanced protection during transit. You will be contacted by our team for a quote, if necessary, after we receive your order. Once you confirm the order, we will ship the device to you with all the required accessories.

Transfer data from the BMR server to the Express device

After receiving the Express device, you need to follow these instructions for transferring data from the BMR server to the device:

1. Sign in to the IDrive BMR server web interface and click the 'Cloud Replication' tab.

2. Click the 'Switch to Cloud Seeding' button.

3. Connect the Express device to the BMR server.

4. Click the 'Mount' button.

5. To transfer backups of the physical machines, go to the 'Physical Machines' tab. To transfer backups of your VMware server, go to the 'VMware' tab.

6. In the 'Cloud Seeding Settings' section, select the clients to transfer from the respective dropdown.

7. Set the backup throttle. By default, this value will be set to 100.

8. Click 'Transfer Now'.

Once data is successfully transferred to the device, you can eject the device and ship it back to IDrive. The time required to transfer data to your cloud account depends on the volume of data and our representative will update you on the same once we receive the device from you.

Cloud replication will be re-enabled from the server-side once the cloud seeding process is complete and all the backups will continue from where you left off.

To cancel cloud seeding after initiating it, you should contact the BMR support team to undo any changes made during the cloud seeding process.

View Logs

The 'View Logs' option here would take you to a page with a comprehensive log of cloud seeding activities of your physical clients and VMware machines.

Activities

This section displays the status of the ongoing data transfer to the external device. Information such as client machine name, drive selected for transfer, recovery point, amount of data transferred to the device, time taken so far to transfer, the data-write speed, and the estimated time for transfer are displayed.

Cloud Seeding Settings

You can select the client machines for transfer, set the bandwidth throttle, and also add the email address for receiving notifications related to cloud seeding.

The following options are available:

Select clients to transfer - You can select the required client machines to transfer data from the BMR server to the external device. Click 'Select All' to select all the client machines.

Backup throttle - Enter the bandwidth throttle value to set the Internet usage for your backups. By default, this value will be set to 100 MBit/s.

Note: Bandwidth throttle value should be between 1-1000 MBit/s.

Last Backup Log

View detailed information on the last cloud seeding operation from the 'Last Backup Log' section.

Express Drive Information

This section provides information about the Express device sent by IDrive. Information such as status of the device (mounted or unmounted) and disk utilization will be displayed.

Cloud Seeding Status

This section displays status of the data transfer. Information such as as the host of VM name, date and time of the last transfer, and the size of the data that was transferred. You can even search for the required client machines by using the 'Search' field.

NAS

The NAS tab lets you leverage the BMR storage space for hosting network-attached shares. You can create NAS share or object-level datashare and collaborate with associates over file-based sharing protocols such as SMB, NFS, AFP, and SFTP. Alternatively, you can create iSCSI shares or block-level datastores that imitate locally-attached disk. Additionally, you can secure your datastores locally via scheduled snapshots.

You can access the NAS and iSCSI shares on the BMR server from any external network via the Cloud Manage feature. However, to access the content of the share, you need to be on the same network as the BMR server.

Choosing the type of network share:

When creating a network share on the BMR server, choose the share type based on the required data accessibility and storage architecture.

- NAS share offers object-level storage which is suitable for sharing files and folders. These shares are accessible as mapped drives on the client machines.

- iSCSI shares, however, offer block-level storage and the storage architecture is on the network, rather than the client machine. In the case of Windows OS, the iSCSI initiator displays the shares on the BMR server as local drives on the client machines that are on the BMR network.

BMR network shares and storage space

You can create and host unlimited network shares on the BMR server. The network shares are created within your BMR quota therefore, for seamless performance, monitor your local storage utilization.

For storage details of the NAS and iSCSI shares on the BMR server, navigate to 'Statistics' > 'Storage Insights'. On the same page, you can scroll down to the 'NAS' tab below to view and download the backup statistics of your network shares.

Host and access NAS share on the BMR server

Create NAS shares on the BMR server and collaborate across SMB, AFP, NFS, and SFTP protocols.

To create a NAS share with IDrive BMR,

1. Sign in to the IDrive BMR server interface.

2. On the 'NAS Share' tab, click 'Create a new share'.

3. Select 'NAS Share' as the share type and click 'Next'.

4. Assign a name to the network share under the 'Share Settings' tab.

5. Select 'Apply New settings' and configure the share settings. Alternatively, choose the 'Use the configurations of an existing share' option to replicate the configuration of an existing share.

6. Click 'Next'.

7.   Set the snapshot frequency in the 'Local Snapshot' tab, using the dropdown against 'Capture a local snapshot every _'.

8.   Select the days for local backup as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days.

9.   Set the start and end time of the backup.

   Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

10.   Use the slider under 'Snapshot Retention Settings' to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a network share.

11.   Click 'Next'.

12.   In the 'Confirm Share' tab, review the local snapshot summary, and click 'Create'.

13.   The new share will be displayed in the 'BMR NAS' tab

To configure your NAS share,

1.   Sign in to the IDrive BMR serve interface.

2.   Navigate to the 'NAS Share' tab to view all the network shares on the BMR server.

3.   Click 'Configure Share Settings' corresponding to the required NAS share.

4.   Under the 'Manage Share Access' tab, set the access permission as public or private. In the case of private access, assign users to the share in the 'Manage Share Users' section below.

5.   Under the 'Share Protocols' section, select the network protocols that will be used for accessing the shares.

   Note: SMB protocol access is configured by default.

6.   Enable write access for all users, if required.

7.   Under the 'Configure Local Snapshot' tab, set the frequency for capturing the local snapshots and schedule the backups as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days.

8.   Set the start and end time of the backup.

   Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

9.   Use the slider in the 'Snapshot Retention Settings' section to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a NAS share.

10.   Click 'Save' to save the local snapshot settings.

Host and access iSCSI share on the BMR server

To create an iSCSI share with IDrive BMR,

1. To create an iSCSI share with IDrive BMR.

2. Go to the 'NAS Share' tab and click 'Create a new share'.

3. Select 'iSCSI Share' as the share type and click 'Next'.

4. Assign a name to the iSCSI share under the 'Share Settings' tab.

5. Select 'Apply New settings' and configure the share settings. Alternatively, choose the 'Use the configurations of an existing share' option to replicate the configuration of an existing share.

6. Assign disk space for the iSCSI target and configure the block size as 512 Bytes or 4096 Bytes.

7. Click 'Next'.

8. Set the snapshot frequency in the 'Local Snapshot' tab, using the dropdown against 'Capture a local snapshot every _'.

9. Select the days for local backup as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days

10. Set the start and end time for backup.

    Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

11. Use the slider under 'Snapshot Retention Settings' to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a network share.

12. Click 'Next'.

13. In the 'Confirm Share' tab, review the local snapshot summary, and click 'Create'.

14. The new share will be displayed in the 'BMR NAS' tab.

To configure your iSCSI share,

1. Sign in to the IDrive BMR server interface.

2. Navigate to the 'NAS Share' tab to view all the network shares on the BMR server.

3. Click 'Configure Share Settings' corresponding to the required iSCSI share.

4. In the 'CHAP Authentication' section, configure CHAP Authentication and Mutual CHAP Authentication.

    Note:

    • *CHAP authentication is recommended for the identity verification of the remote client(s).*

    • *CHAP authentication can be negotiated in both directions for mutual authentication between the client and the iSCSI target, via Mutual CHAP Authentication.*

    • *CHAP authentication needs to be enabled for configuring Mutual CHAP Authentication.*

5. Under the 'Configure Local Snapshot' tab, set the frequency for capturing the local snapshots. Schedule the backups as 'Daily', 'Weekdays', 'Weekend', or select 'Custom' and choose the days.

6. Set the start and end time of the backup.

   Note: Here, the 'Start Time' and 'End Time' is a soft cut-off. The actual start time is dependent on the backup pipeline and the actual end time is dependent on the ongoing tasks that are in progress.

7. Use the slider in the 'Snapshot Retention Settings' section to set the limit for retaining local snapshots. You can retain up to 100 local snapshots of a NAS share.

8. Click 'Save' to save the local snapshot settings.

Backup the network shares on the BMR server

Maintain a backup of your network share on the BMR server via local snapshots.

To schedule local snapshots for a network share on the BMR server,

1. Sign in to the IDrive BMR server interface.

2. Go to the 'NAS Share' tab to view all the existing network shares.

3. Click 'Configure Share Settings' corresponding to the required network share.

4. In the 'Configure Local Snapshot' section, set the frequency for capturing the local snapshots and schedule the backup.

5. Click 'Save'.

   Note:
   In the case of iSCSI share backup, IDrive BMR uses data compression and deduplication mechanism for efficient storage space utilization. The local storage used to store the iSCSI share backups can be lesser or greater than the actual amount of data physically stored.

To pause the local backup of a network share on the BMR server,

1. Sign in to the IDrive BMR server interface.

2. Go to the 'NAS Share' tab to view all the existing network shares.

3. Click 'Configure Share Settings' corresponding to the required network share.

4. In the 'Configure Local Snapshot' section, move the slide toggle to read 'Disabled'.

Restore the network shares on the BMR server

To restore your NAS share data from the local snapshots,

1. Sign in to the IDrive BMR server interface.

2. Navigate to the 'Restore' > 'NAS Restore'.

3. Choose 'NAS' as the share type.

4. Select the required share and recovery points.

5. By default, user authentication is disabled. Meaning, the share will be accessible to everyone on the network. To create a secure share.

Note:

- *Select 'Yes' and enable user authentication.*

- *Select the username from the 'Mount username' drop-down menu*

- *Enter the mount password.*

6. Click 'Create'. The data is shared over the SMB protocol. Based on the OS you are using, you can use the SMB client native to the OS, or install a dedicated application specific to your OS platform to access the data.

To restore your iSCSI share data as a secondary iSCSI target,

1. Sign in to the IDrive BMR server interface.

2. Navigate to the 'Restore' > 'NAS Restore'.

3. Choose 'iSCSI' as the share type.

4. Select the required share and recovery points.

5. Select 'Create a secondary iSCSI target'.

6. Configure CHAP and Mutual CHAP authentication, if required.

    Note: CHAP authentication needs to be enabled for configuring Mutual CHAP Authentication.

7. Click 'Create'.

To restore your iSCSI share data to the existing iSCSI target,

1. Sign in to the IDrive BMR server interface.

2. Navigate to the 'Restore' > 'NAS Restore'.

3. Choose 'iSCSI' as the share type.

4. Select the required share and recovery points.

5. Select 'Restore to the existing iSCSI target'.

6. Click 'Restore'.

7. A pop-up window will appear requesting confirmation to proceed with the restore.

Note:

- *Restoring your network share will effectuate the following changes.*

- *Data created after the selected recovery point will be permanently lost.*

- *Restore mounts of the time range beyond the recovery point will be automatically deleted.*

- *All active iSCSI connections will be terminated.*

Click 'Confirm' to continue with the restore.

User Management for BMR NAS

In the case of NAS shares, you can collaborate on the datashares across SMB, AFP, NFS, and SFTP protocols. To manage network share collaboration, IDrive BMR has introduced the 'Users' section under 'Settings'.

To add users to BMR,

1. In the BMR server interface, go to 'Settings' > 'Control Panel' > 'Users'.

2. Click 'Add User'.

3. Provide the user details and configure the user access with a password.

4. Click 'Add'. The new user is created and listed in the 'Users' tab.

To delete the user(s), select the user(s) and click 🗑

To update user details at a later time, click 📝 corresponding to the required user, update the details, and click 'Save'.

Settings

From this tab, you can change the server and network settings. You can also perform power operations such as shutdown and restart the server.

Mail

You can change the mail server settings as per your requirements from this tab. Also, you can set the email addresses to which the local backup status notification will be sent.

Email Notification

Change the registered email address, add additional email addresses to receive notifications on server health and backup operations such as backup of physical machines, virtual machines, and cloud transfer from this tab.

Server Alert Notification

Change the registered email address and add additional email addresses to receive alerts on server health such as RAID and hard drive health status from this section.

To change the registered email address,

1. Sign in to the IDrive BMR server web interface.

2. Click 'Settings' on the menu bar.

3. Go to 'Mail' -> 'Email Notification' tab.

4. Click ✏️ , enter the new email address.

5. Select the checkbox 'Send alert when the BMR server is offline for more than 48 hours (Applicable only if cloud replication is enabled).' It is recommended to select this option and enable periodic monitoring of the server health.

6. Click 'Save'.

To add additional email addresses,

1. Sign in to the IDrive BMR server web interface.

2. Click 'Settings' on the menu bar.

3. Go to 'Mail' -> 'Email Notification' tab.

4. Enter email addresses separated by a comma in the 'Additional Email' field and click ➕ to add.

5. Click 'Save' to save the changes.

Backup Report Notification

This section lets you add email addresses to receive notifications on backup operations such as backup of physical machines, virtual machines, and cloud transfer.

To add email addresses,

1. Sign in to the IDrive BMR server web interface.
2. Click 'Settings' on the menu bar.
3. Go to 'Mail' -> 'Email Notification' tab.
4. Enter email addresses separated by a comma in 'Send backup report(s)' to field and click ➕ to add.
5. Click 'Save' to save the changes.

Mail Server Settings

You can change the mail server settings from this section.

To change the mail server settings,

1. Sign in to the IDrive BMR server web interface.
2. Go to the 'Settings' tab and click 'Mail'.
3. Click 'Mail Server Settings'.
4. Select the mail server option from the 'Mail Relay Server' drop-down menu.
5. Define the other required parameters and click 'Save'.

By default, the BMR device uses the Amazon SES server for mail communications. It is recommended to use this setting. However, you can change it to the local BMR network or your preferred network.

You can also check if the Firewall is enabled for the selected port.

Control Panel

This tab allows you to configure or change the network settings and perform the power operations of the server. You can even change the time settings of the server depending on your location from this tab.

Network Settings

Change the network settings of your server from this tab.

Configure the network settings of the BMR server

The BMR server may feature one or two network Ethernet ports. You can view the ethernet settings of the port(s) in 'Control Panel' > 'Network Settings'.

The following parameters are displayed for the network port(s):

IP Mode - Specifies the configured IP mode, whether static or DHCP

IP Address - Displays the IP address or the network location of the BMR server. The IP address is how you can identify the BMR server.

Netmask - Displays the netmask value.

Gateway - Displays the gateway address of the router / network device.

MAC Address - Displays the unique hardware address of the Ethernet port on the BMR server.

Jumbo Frames - IDrive BMR supports networking switch to 'Jumbo Frames' for the Maximum Transmission Unit of up to 9216 bytes. Enable 'Jumbo Frames' if you wish to improve data transmissions, and by extension the network performance.

Note: For the switch to be effective, ensure all devices and hardware in your network infrastructure support Jumbo Frames.

Set static IP address and network configuration for the BMR server

To configure a static IP address for an Ethernet port,

1. Click 🖊 against the required ethernet port entry. The 'Network Settings' window appears.

2. Select the 'IP Mode' as 'Static' and provide the required information such as IP address, Netmask, and Gateway in the respective fields.

3. Click 'Apply Settings'.

   Note: Ensure the availability of the required static IP to avoid losing access to the server. In case the specified static IP is not available, you will lose connection to the BMR server. In which case, you will need to connect to the server's physical monitor to reset the network settings.

Configure the DNS settings for your BMR appliance

To change DNS settings,

1. In the 'DNS Settings' section, select 'Use the following DNS server address'.

2. Provide primary, secondary, and tertiary DNS server address in the respective fields and click 'Apply'.

Check firewall for blocked ports

Firewall Checkpoint is a function within the BMR server that helps you check firewall restrictions, if any. Through this function, network restrictions on services such as email delivery, cloud replication, and so on are identified.

In the 'Firewall Checkpoint section of 'Settings' > 'Control Panel', click 'Check Now' to run a firewall check for general, mail relay server, and cloud replication configurations. Either of the following statuses will be displayed:

⊘ **Successful**

⚠ **Failure**

The status 'Successful' implies that there are no firewall restrictions and you can continue to use all services related to BMR. If the Firewall check returned 'Failure' alert, troubleshoot as necessary / contact your network admin and check again.

Steps for troubleshooting:

✔ In case of issues with the general Firewall settings, unblock Port '80' and Port '443' for 'www.idrive.com' and 'www1.idrive.com' servers.

✔ If you are facing issues with the mail settings, check your Mail Server Port details and unblock the port, if blocked.

✔ To resolve an issue related to cloud Replication, contact the BMR support team for the Port details. Then share the received information with your network admin to unblock the respective ports.

Reset the BMR network

This section allows you to check firewall configuration status for the following:Go to 'Settings' > 'Control Panel' > 'Network Settings' and click 'Reset Network' to configure all the network interfaces on the BMR server to operate on DHCP mode. After network reset, the server will try to obtain DHCP provided IP from your network. You will need to connect to the BMR server with a physical monitor to view the new server IP.

Note: Before resetting the network stop any on-going backup operation and delete any virtual instances on the server.

Time Zone

Change the time zone settings of your server as per your location from this tab.

To change the time zone,

1. Sign in to the IDrive BMR server web interface.

2. Go to the 'Settings' -> 'Control Panel' and click 'Time Zone'.

3. Choose your region from the 'Select Time Zone' drop-down menu.

4. Select your country and zone.

5. Click 'Save'.

Statistics

This tab displays information about system health and storage insights of the BMR device.

System Health

This tab provides information about the health status of RAID devices, hard drives, memory used, and the network port. You can also perform the cleanup operation if the storage utilization reaches 80%.

RAID Health Status

This section displays the health status of RAID devices. If one device stops working the other acts as a backup.

RAID Health statuses and what they indicate:

ONLINE - The drives are working as expected.

DEGRADED - The drive experienced an issue and is predicted to fail

FAULTED - The drive is not found or is inaccessible

Contact the support team immediately if any of the RAID devices stop working. Our team will analyze the problem and send a replacement device after processing the issue. Once you receive the device, our team will assist in replacing the device over chat or phone support. After the device is successfully replaced and identified by the server, the rebuild operation will start. You can see the rebuild operation status in the 'RAID health status' section.

OS Drive Health Status

You can check the individual health status of the hard drive (OS and storage) under the 'OS Drive Health Status' section.

OS Health statuses and what they indicate:

GOOD - Drives are working fine.

BAD - Contact support team immediately

Predicted to Fail - Contact support team immediately

Storage Volume Usage

The 'Storage Volume Usage' section displays information about the storage space of the IDrive BMR server. The utilized and remaining storage space is displayed in percentage so that you can track your utilization and allows you to perform manual cleanup after 80% usage.

To perform manual cleanup,

1. Sign in to IDrive BMR web interface and click 'Statistics' -> 'System Health'.

2. Choose the 'Cleanup Type' from the drop-down menu.

3. Click 'Cleanup'.

4. Click 'Confirm' in the confirmation window.

You can view information about server uptime and memory used in the 'Fast Statistics' section. The 'Bandwidth' section displays information about data transmitted and received. In the 'Network' section, one can find information on network configuration of the BMR server.

General Info

This section gives information about the time since the BMR server is up and running and also about RAM usage of the BMR server.

Network

The 'Network' section displays information about network settings such as IP address and the mode of network.

Storage Insights

This tab displays information about storage usage and backup statistics for your physical and VMware machines. Details include the actual utilized storage space, the total number of mounts for file restore and virtualization, and the space used by virtual instances of physical and virtual machines. The 'Storage' section displays the storage utilized by physical machines and virtual machines in the BMR device.

Backup Statistics

This section displays information about the storage used by each client or virtual machine. You can also search for the required client or virtual machine. Enter the client or hostname in the 'Search' field to view the backup statistics.

Note: The 'Data Size' section displays the actual storage space utilization, which is far less than the original drive size. The BMR server employs the de-duplication mechanism and compression in the backend to optimize the storage space.

Logs

This tab displays information about activities performed on the server. For user convenience, logs are categorized appropriately for your physical clients and VMware machines. These logs will help support the team to analyze the cause of backup failure.

Physical Machines And VMware

Backup Logs

This tab displays information about backup activities of the registered physical clients and VMware machines. Click the required log to view detailed information about the activity.

IDrive Cloud Logs

This tab provides information about all logs related to cloud backups. This includes the date, hostname/VM name, volume, recovery point, type, backup status, and integrity information.

Cloud Seeding Logs

The tab displays information about all logs related to cloud replication initiated via BMR Express - a temporary storage device.

Restore Logs

This tab displays information about restore activities of the registered clients and VMware machines.

NAS Logs

View comprehensive logs of BMR network shares, backups, and restore operations.

System Logs

This tab displays information about system activities such as sign in, sign out, and so on.

Export

This option allows you to download the logs in CSV, Excel, and PDF format. You can also print and copy the logs. Click 'Export' in the respective tab and click the required format from the drop-down menu to download the logs.

Cloud Manage

Cloud Manage enables cloud management and access to the IDrive BMR server remotely.

To connect to your BMR server,

1. Go to www.idrive.com and sign in with your BMR cloud account credentials.

2. Go to the 'Cloud Manage' tab.

3. Click 'Connect'.

4. The server web interface is displayed via a remote access window. From here, you can perform local backups, create restore points, view logs, and also monitor the health of the devices on the server. For more information, refer to the BMR FAQs

Note: If the BMR device is purchased through a reseller, the reseller will have access to your BMR device with automatic sign in through the 'Partner Management' feature. You can disable this access any time via the BMR server interface, under 'Settings' > 'Control Panel' > 'Partner Manage'.

We hope you found this User Guide useful to get started with IDrive BMR. For additional information, you may click and refer to the help slides or read the BMR FAQs.

If you did not find what you need, write to us at support@idrive.com.