

Setting Up Monitoring

<https://campus.barracuda.com/doc/84313375/>


Although the Infrascala BDR service module is free, if you wish to perform bare metal backups on servers, or install an appliance for specialized backups, you must contact your sales representative to purchase licenses. Additionally, for file and folder backups, you must purchase a disk quota which you can then allocate to your customer sites.

To calculate how much disk quota you should request across all sites, as a rule of thumb you should allocate 25GB per device for file and folder backups, and 250GB per device for bare metal backups. If you go over quota, you can choose to automatically allow backup accounts to go over quota, and you can contact your sales representative to purchase additional disk quota.

Setting Up Infrascala Credentials

To obtain Infrascala BDR licenses and account credentials, contact your sales representative. He or she will set up an Infrascala account for you, and send you an email with a user name and a link to the Infrascala dashboard. When you log in to the Infrascala dashboard, you are prompted to provide and verify a password for your Infrascala account. Take note of this password, as you will be entering it in Service Center.

Next, you will enter your Infrascala credentials into Service Center.

1. In Service Center, click **Status > Service Modules**.
2. In the **Infrascala** section, click the gear icon .
3. In the **User Name** field, type your Infrascala user name. This is the name provided in the email sent by your sales representative.
4. In the **Password** field, type your Infrascala password. This is the password you created when you logged in to the Infrascala Dashboard to set up your account.
5. In the **Default Device Quota for File/Folder Policy (GB)** field, enter the default disk quota you want to allocate per device for file and folder backups. By default, this is set to 25GBs.
6. In the **Default Device Quota for Baremetal Policy (GB)** field, enter the default disk quota you want to allocate per device for bare metal backup. By default, this is set to 250GBs.
7. If you want to allow backup accounts to go over quota, select the **Allow backup accounts to go over quota** checkbox. When selected, if a backup requires more disk space that you've allotted, the backup will continue over quota and you will be billed for the additional disk space. If you do not select this checkbox and a backup goes over quota, the backup will fail.
Tip: You can also allow backups to go over quota on a per-device basis, if you do not want to allow this at the multi-site level. See Viewing Infrascala BDR Data for a Device.
8. In the **Agent Update Behavior** section, click the **Auto-upgrade backup agent** if you want to automatically update the OBRM agent on devices as new updates become available.

9. Click **Save**.

Setting Infrascade Configuration Policies

The BDR Infrascade service module includes two default configuration policies. The **Server Backup Configuration Policy** defines the settings for bare metal backup, and the **Workstation Backup Configuration Policy** defines the setting for file and folder backups.

You can use these default configuration policies as is, or you can customize the settings to suit your needs. You can also create your own Infrascade service module configuration policies.

Notes:

- After applying one of these configuration policies to a device, the required software will be automatically installed using our built-in automation. Manual installation is not required. You must also ensure that the StorageCraft ShadowProtect monitoring policy is applied to server devices using bare metal backup to properly record the installation status.
- The Infrascade BDR service module performs backups to the cloud and not a local backup location.

Customizing the Server Backup Configuration Policy

The Server Backup Configuration Policy specifies bare metal recovery settings, such as which disk volumes to protect, the schedule for creating local images and where to store them, and options for protecting disk images.

1. In Service Center, click **Configuration > Service Modules**.
2. From the list of service modules, select Infrascade.
3. Click the **Server Backup Configuration Policy**.
4. Click the **Settings** tab.
5. Click **Modify**.
6. In the **General** area, select which disk volumes to protect by selecting one of the following from the drop list:
 1. **System drive**
 2. **All drives**
 3. **Other drive letters**. If you select this option, type the drive letters in the Other drive letters field. When adding multiple drive letters, separate them by a semi-colon.
7. **Next**, you will set the schedule in which local images are created:
 1. In the Local Image Creation Schedule area, select the day of the week and the time. To select from a list of hourly times, click the clock icon.
 2. In the Max Image Split Size field, specify the maximum size, in MBs, in which to break up the local image.
8. Next, specify where to save disk images once they are created. You can choose to save on the

same computer, or you can specify another computer on the network.

9. a In the Folder for disk images field, specify the folder on which to save
10. the disk images.
11. In the PC or domain user field, specify the computer or domain user
12. on which to save the disk images.
13. c In the User password field, type the computer password.
14. 9Next, you can enable protection for the disk image. Select the Enable disk image protection checkbox, and do the following:
15. a From the Encryption algorithm list, select the type of encryption to
16. apply.
17. b In the Password for disk images field, enter the password, and then
18. retype it in the Confirm disk image password field.
19. 10Next, you will set up the schedule for backing up the disk image to the cloud.
20. a In the Frequency Timing area, select whether disk images will be
21. backed up to the cloud on an hourly, daily, weekly, or monthly basis.
22. b Depending on your frequency selection, specify the number of hours
23. for the hourly frequency, the time, day of week, or day of month. For
24. example, selecting an hourly frequency, and then selecting 2 from the
25. Every list results in the cloud backups occurring every 2 hours.
26. Selecting a monthly frequency, and then selecting 15 from the Day
27. number list results in cloud backups occurring on the 15th of every
28. month.
29. c In the End Time field, enter the time or click the clock icon to select a
30. time for the backup to complete.
31. 11From the Retention Category list, select one
32. of the following retention policies:
33. a Replicate - any changes in a folder, including when files are added,
34. modified, or deleted, are reflected in the cloud backup.
35. b Forever Save - everything is saved forever, with no automated or
36. scheduled deletion of data.
37. c Archive - used for archival situations as when documents are scanned
38. and moved into specific folders for the sake of compliance.
39. d Time-Limited Backup - files are backed up to the cloud, but they are
40. only kept for a specified number of days before being deleted from
41. local machine storage. The timer resets if a new version of the file is
42. backed up.
43. e Cloud Time-Limited Backup - Files are backed up to the cloud, but
44. they are only kept for a specified number of days before being deleted
45. from the server. This timer resets if a new version of the file is backed
46. up.
47. 12Click Save.

Customizing the Workstation Backup Configuration Policy

The Workstation Backup Configuration policy defines the settings for file and folder backups on managed workstations, including which files and folders to back up, the types of files to scan, whether

to email a report after backup completes, and the schedule for sending disk images to the cloud.

When you select all files to scan, the following folders are excluded from the scan:

- C:\\$Recycle.Bin
- C:\Program Files
- C:\Program Files (x86)
- C:\Program Files (x86)\Online Backup and Recovery Manager
- C:\ProgramData\Microsoft
- C:\ProgramData\Microsoft\Windows
- C:\ProgramData\Online Backup and Recovery Manager
- C:\Temp
- C:\Temp\Online Backup and Recovery Manager
- C:\Windows
- all hidden files

Additionally, in the C:\Users folder, the following locations are not backed up for all users:

- C:\Users\[user name]
- C:\Users\[user name]\AppData\Local\Microsoft\Internet Explorer\DOMStore
- C:\Users\[user name]\AppData\Local\Microsoft\Windows Mail\Stationery
- C:\Users\[user name]\AppData\LocalLow\Microsoft
- C:\Users\[user name]\AppData\Roaming\Microsoft

1 In Service Center, click Configuration > Service Modules.

2 From the list of service modules, select Infrascade.

3 Click the Workstation Backup Configuration Policy.

4 Click the Settings tab.

5 Click Modify.

6 In the Global Settings area, you will specify which files to back up, by setting the following:

a To prevent backups to files that were modified before a specific date,

select the Do not backup files modified before checkbox, and then

either type the date or click the calendar icon to select a date.

b To set a maximum size limit to file backups, select the Do not backup

files larger than MB checkbox, and then type the maximum file size, in

MBs, in the field.

c To set a minimum size limit to file backups, select the Do not backup

files smaller than KB checkbox, and then type the minimum file size,

in KBs, in the field.

7 To send reports by email when a backup completes, select the Send email reports at the end of the backup checkbox, and then provide full email addresses in the field provided. Email addresses can be delimited by spaces, commas, or semi-colons.

8 In the Scanner Settings area, specify the types of files to scan, by doing the following:

a In the Scan Type list, holding down the CTRL key and clicking each file

type you want to scan.

b To specify a type of file to exclude from the scan, select the Custom

checkbox and type the file extension in the field. Do not include an asterisk or a period before the file type. For example, to exclude .zip files, type "zip". You can separate file types using a space (), a comma(,), or a semi-colon (;).

9Next, you will set up the schedule for backing up the disk image to the cloud.

a In the Frequency Timing area, select whether disk images will be backed up to the cloud on an hourly, daily, weekly, or monthly basis.

b Depending on your frequency selection, specify the number of hours for the hourly frequency, the time, day of week, or day of month. For example, selecting an hourly frequency, and then selecting 2 from the Every list results in the cloud backups occurring every 2 hours.

Selecting a monthly frequency, and then selecting 15 from the Day number list results in cloud backups occurring on the 15th of every month.

c In the End Time field, enter the time or click the clock icon to select a time for the backup to complete.

10In the Backup Set Settings area, you can specify individual files and folders that you want to include or exclude in the scan. When typing the folder path or file names, separate items using a pipe(|) or an asterisk (*).

a To specify folders that you always want to scan, select the Included folders checkbox, and type the folder path in the field.

b To specify files that you always want to scan, select the Included files

checkbox, and type the file names in the field.

c To specify folders that you always want to exclude, select the

Excluded folders checkbox, and type the folder path in the field.

d To specify files that you always want to exclude, select the Excluded

Files checkbox, and type the file names in the field.

Note: Any folder you specify will be included or excluded on every device scanned.

11Click Save.

Creating an Infrascade Service Module Configuration Policy

You can create your own Infrascade configuration policies in addition to the two that are provided with the service module. This can be helpful if you offer varying service level agreements to your customers, and you want to create policies for each SLA.

1In Service Center, click Configuration > Service Modules.

2From the list of service modules, select Infrascade.

3Scroll down to the Policies section and click Add.

4From the list that appears, select Infrascade - File and Folder Backup to create a configuration policy for workstations, or Infrascade - Bare metal to create a configuration policy for servers.

5Click Add Policy.

6Provide a name and description for the policy, and click Create.

7Click the Settings tab, and when prompted to create settings for this configuration policy, click Create.

8Fill in the configuration policy settings. For more detailed information on the configuration policy

settings, see Customizing the Server Backup Configuration Policy and Customizing the Workstation Backup Configuration Policy.

9Click Save.

Understanding the Infrascade monitoring policies

The Infrascade service module includes three monitoring policies to monitor online backups:

Infrascade Data Protection Appliance (DPA)

This monitoring policy monitors Infrascade Data Protection Appliance (DPA), which performs specialized backups such as SQL and Exchange, and requires a an appliance set up on dedicated hardware at the customer site. If you have purchased a DPA license, you can set up manual or automatic application rules to monitor the DPA appliance. This monitoring policy monitors for the following:

- client machine is unreachable
- collects asset data for the appliance machine
- disk space low, critical, or out of space
- DPA availability
- appliance requires media
- a backup or restore job fails
- RAID health
- sensor out of range
- system settings have changed.

The Infrascade Data Protection Appliance (DPA) monitoring policy does not contain any automatic or manual application rules. If you choose to install an appliance at a customer site, it is recommended that you manually add the appliance device to this monitoring policy in the Manual Application tab.

Infrascade Data Protection Cloud (DPC)

This monitoring policy monitors devices with file and folder backups. It monitors for the following:

- collects Backup Account usage snapshots
- collects Backup Event history
- collects Infrascala DPC events
- monitors the status of offsite network backups

The Infrascala Data Protection Cloud (DPC) monitoring policy contains a single automatic application rule - Windows Service Name equals agentservice - which will automatically detect devices with bare metal recovery or file and folder backup installed. Therefore, you do not need to create automatic or manual application rules to this monitoring policy. However, you do need to add it to a policy set for monitoring to begin.

StorageCraft ShadowProtect

This monitoring policy monitors devices with StorageCraft ShadowProtect, which is deployed on servers to perform bare metal recovery. It monitors for the following events, among others:

- backup failed or stopped before completion
- cannot create or destroy snapshots
- failed to save backup
- trial period is about to expire

The StorageCraft ShadowProtect monitoring policy contains a single automatic application rule - Software Name contains ShadowProtect - to ensure that this monitoring policy only gets applied to devices that have the ShadowProtect agent installed.

Viewing and Changing the Alert Thresholds on a monitoring policy

1In Service Center, click Configuration > Service Modules.

2From the list of service modules, select Infrascala.

3Click the name of an Infrascala monitoring policy.

4 Click the Monitors tab.

5 Click the name of a monitor.

6 Click the Alerts tab.

7 Do any of the following:

- To view or modify an existing alert configuration, click the name of the alert configuration.
- To add an alert configuration, click Add Alert Configuration.

Applying the Infrascade monitoring policies

To begin monitoring with the Infrascade service module, you must either add the monitoring policies to a policy set, or manually apply it to a site, group, or device.

Best Practice: If you have a device with a policy applied, and you want to

apply a different policy to the device, do not remove the existing policy as this

will uninstall the ShadowProtect client from the device. Instead, simply apply

the new policy to the device and this policy will supersede the previous policy.

1 In Service Center, click Configuration > Service Modules.

2 From the list of service modules, select Infrascade.

3 To select a policy set to associate with the monitoring policies in the Infrascade service module, do the following:

a In the Policy Set Membership area, click Add.

b Select the checkbox beside the name of the policy set to which you want to associate with this service module.

c Click Add.

Tip: After adding the policy set, you can click the policy set name to view

and modify the sites, groups, and devices within its scope.

4To manually apply monitoring, do any of the following:

a To apply the monitoring policy to a group, click a monitoring policy

name. Click the Manual Application tab, and then under Applied

Groups, click Add. Filter on the Group Type, if desired. Select the

group and click Add.

b To apply the monitoring policy to a device, click a monitoring policy

name. Click the Manual Application tab, then under Applied Devices,

click Add. Filter the list of devices. Select the device and click Add.

Note: After the ShadowProtect StorageCraft monitoring policy is applied to a device, you must reboot that device for the policy to take effect. To reboot a device, from the Site dashboard, scroll down to the Protected Devices table, and, in the Action column, click the Reboot link.

Figures

1. gear.jpg

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.