Setting up Infrascale Configuration Policies

https://campus.barracuda.com/doc/91129227/

The Infrascale service module includes two default configuration policies:

- The **Server Backup Configuration Policy** is the default **Infrascale - Baremetal Backup** policy, and defines the default settings for bare metal backups.
- The **Workstation Backup Configuration Policy** is the default **Infrascale - File and Folder Backup** policy, and defines the default settings for file and folder backups.

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

To apply **Infrascale Configuration Policies**, you can create automatic inclusion rules or manual inclusion rules to define the criteria a device must meet to be included. For more information on automatic inclusion rules, see Creating Automatic Inclusion Rules for Monitoring Policies. For more information on manual inclusion, see Applying a Monitoring Policy to a Group or Device.

After you apply one of these configuration policies to a device, the required software is 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 workstation or server devices using bare metal backup to properly record the installation status.

Customizing the Default Infrascale - Baremetal Backup Policy

Important Before adding this policy to a device, the device needs to have the **Infrascale Data Protection Cloud (DPC)** for Service Module policy and the **StorageCraft ShadowProtect** for Service Module policy applied. If the device doesn't have these policies applied, the information about the device may not be correct.

The **Server Backup Configuration Policy** is the default **Infrascale - Baremetal Backup** policy, and specifies 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. Click the **Infrascale** link.
3. In the **Policies** section, click the **Server Backup Configuration Policy** link.
4. Click the **Settings** tab.
5. Click **Modify**.
6. In the **General** area, select the disk volumes to protect by selecting one of the following from the drop list:
    - **System drive**
    - **All drives**
    - Other drive letters. If you select this option, type the drive letters in the **Other drive**

letters box. When adding multiple drive letters, separate them with a semi-colon.

7. Next, set the schedule in which local images are created:
   - 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.
   - In the Max Image Split Size box, specify the maximum size, in MBs, in which to break up the local image.

     Due to the large size of local image files, by default they are split into smaller files when saved. The **Max Image Split Size** box defines the maximum size of the split files.
8. Next, specify where to save disk images once they are created. You can't save on the same computer. Specify another computer on the network.

   You don't need to have admin access to the device where the disk image will be backed up, but you must be able to access the shared folder from the Onsite Manager.
   - In the **Folder for disk images** box, specify the folder on which to save the disk images.
   - In the **PC or domain user** box, specify the computer or domain user on which to save the disk images.
   - In the **User password** box, type the computer password.

     To manage the images saved locally, you can use StorageCraft ImageManager, a free tool. For more information, see www.storagecraft.com/products/imagemanager.
9. Next, you can enable protection for the disk image. Select the **Enable disk image protection** checkbox, and do the following:
   - From the **Encryption algorithm** list, select the type of encryption to apply.
   - In the **Password for disk images** box, type the password, and then retype in the **Confirm disk image password** box.
10. Next, you will set up the schedule for backing up the disk image to the cloud.
    - In the **Frequency Timing** area, select whether disk images are backed up to the cloud on an **hourly**, **daily**, **weekly**, or **monthly** basis.
    - 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.In the **End Time** box, enter the time or click the clock icon to select a time for the backup to complete.
11. From the **Retention Category** list, select one of the following retention policies:

    The suggested retention policy for images is **Replicate**.
    - **Replicate** — Any changes in a folder, including when files are added, modified, or deleted, are reflected in the cloud backup.
    - **Forever Save** — Everything is saved forever, with no automated or scheduled deletion of data.
    - **Archive** — Used for archival situations as when documents are scanned and moved into specific folders for the sake of compliance.
    - **Time-Limited Backup** — Files are backed up to the cloud, but they are only kept for a specified number of days before being deleted from local machine storage. The timer resets if a new version of the file is backed up.

- **Cloud Time-Limited Backup** — Files are backed up to the cloud, but they are only kept for a specified number of days before being deleted from the server. This timer resets if a new version of the file is backed up.

12. Click **Save**.

The next step is Applying the Infrascale Configuration policies.

Customizing the Default Infrascale - File and Folder Backup Policy

Before adding this policy to a device, the device needs to have the **Infrascale Data Protection Cloud (DPC) for Service Module** policy applied. If the device doesn't have the **DPC** policy applied, the information about the device may not be correct.

The **Workstation Backup Configuration** policy is the default **Infrascale - File and Folder Backup** policy, and defines the settings for file and folder backups on managed workstations or servers, 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.

The following folders are not scanned for files to back up:

- **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**

The following locations, which are all in the **C:\Users** folder, are not backed up:

- **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. Click the **Infrascale** link.
3. In the **Policies** section, click the **Workstation Backup Configuration Policy**.
4. Click the **Settings** tab.
5. Click **Modify**.

6. In the **Global Settings** area, specify the files to back up, by setting the following:
   - 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.
   - 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 box.
   - 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 box.
7. To send reports by email when a backup completes, select the Send email reports at the end of the backup check box, and then provide full email addresses in the box. Separate email addresses with spaces, commas, or semi-colons.
8. In the **Scanner Settings** area, specify the types of files to scan by doing the following:
   - In the **Scan Type** list, hold down the **Ctrl** key and click each file type you want to scan.
     To cancel the selection of a scan type, hold down the **Ctrl** key and click a selected file type.
   - To specify a type of file to include in the scan, select the **Custom** check box and type the file extension in the box. Do not include an asterisk or a period before the file type. For example, to include **.zip** files, type "**zip**". You can separate file types using a space( ), a comma(,), or a semi-colon (;).
9. Next, set up the schedule for backing up the files and folders to the cloud.
   - In the **Frequency Timing** area, select whether disk images are backed up to the cloud on an hourly, daily, weekly, or monthly basis.
   - 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, 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.
   - In the **End Time** box, enter the time or click the clock icon to select a time for the backup to complete.
10. In 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 (*).
    - To specify folders that you always want to scan, select the **Included folders** checkbox, and type the folder path in the box.
    - To specify files that you always want to scan, select the **Included files** checkbox, and type the file names in the box.
    - To specify folders that you always want to exclude, select the **Excluded folders** checkbox, and type the folder path in the box.
    - To specify files that you always want to exclude, select the **Excluded Files** checkbox, and type the file names in the box.
      Any folder you specify is included or excluded on every device scanned.
11. Click **Save**.

The next step is Applying the Infrascale Configuration policies.

Creating an Infrascale Service Module Configuration Policy

You can create your own **Infrascale** 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**. It can also be helpful if you want to back up certain files or folders for one client that don't need to be backed up for another.

1. In Service Center, click **Configuration** > Service Modules.
2. Click the **Infrascale** link.
3. Scroll down to the **Policies** section, and click **Add**.
4. From the list that appears, do one of the following:
   - To create a file and folder backup configuration policy for workstations, click **Infrascale - File and Folder Backup**.
   - To create a bare metal backup configuration policy for servers, click **Infrascale - Bare metal**.
5. Click **Add Policy**.
6. Provide a name and description for the policy, and click **Create**.
7. Click the **Settings** tab, and when prompted to create settings for this configuration policy, click **Create**.
8. Fill in the configuration policy settings. For more detailed information on the configuration policy settings, see Customizing the Default Infrascale - Baremetal Backup Policy and Customizing the Default Infrascale - File and Folder Backup Policy.
9. Click **Save**.

The next step is Applying the Infrascale Configuration policies.