Windows server

Prerequisites & Requirements:

Installation Requirements:

- For installation of Varonis agent(s), an account with **Local Administrator privileges** is required NOTE: A separate account can be used for agent installation.

Permanent Security Requirements:

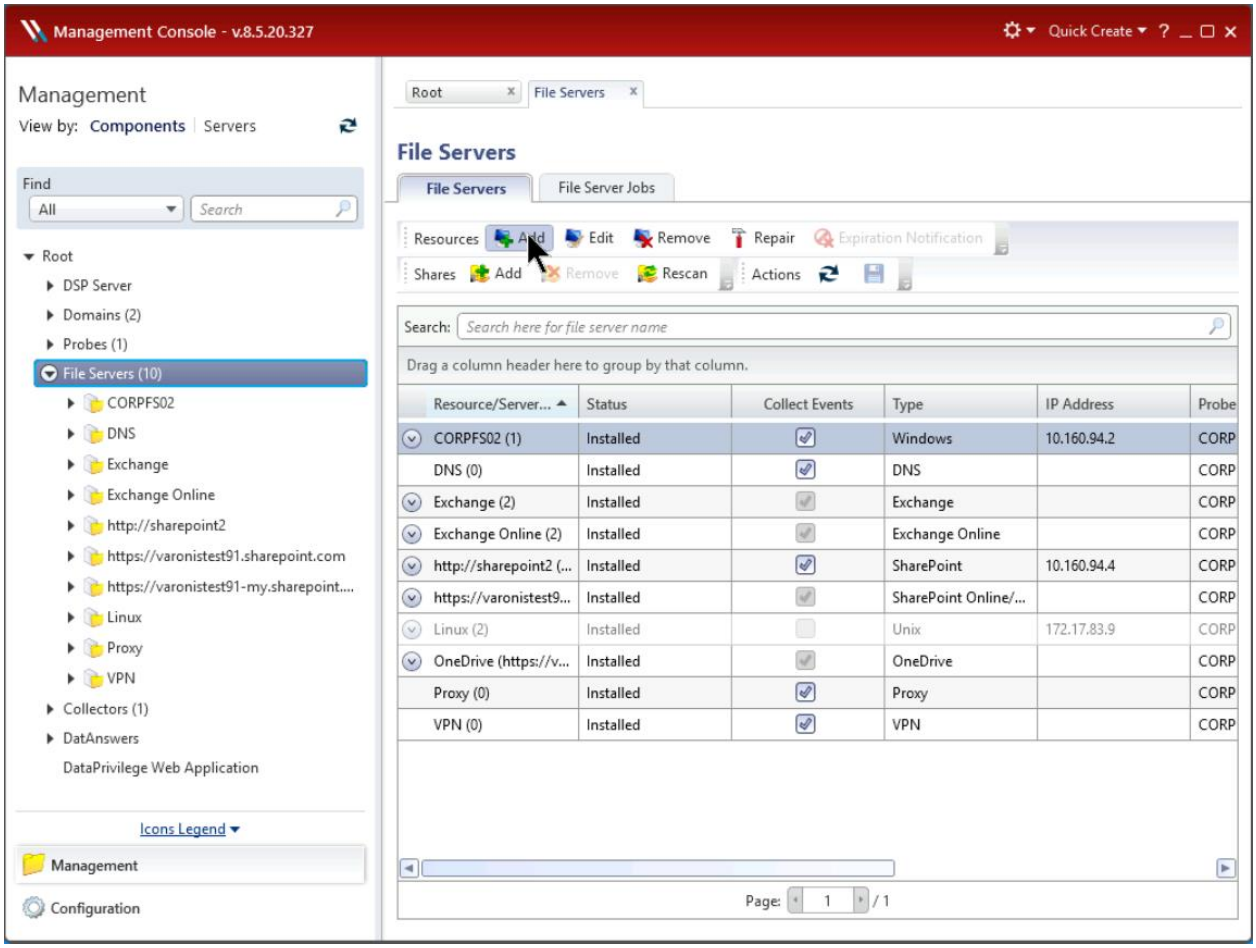
- Directory Crawling:
  - o CIFS - User with permissions to view all file system directories and their permissions (**Administrator or Backup Operators and Power Users**)
  - o Varonis Protocol - Varonis FileWalk Agent should be installed

Ports & Protocols:

Source	Destination	Port/Protocol
DSP/Probe Collector	Windows FS	135/TCP, 137-138/UDP, 139/TCP, 445/TCP, 4972/TCP, 4974/TCP, ICMP, 49171/TCP (3), 60777/TCP (2)
Windows FS	DSP/Probe Collector	4972/TCP

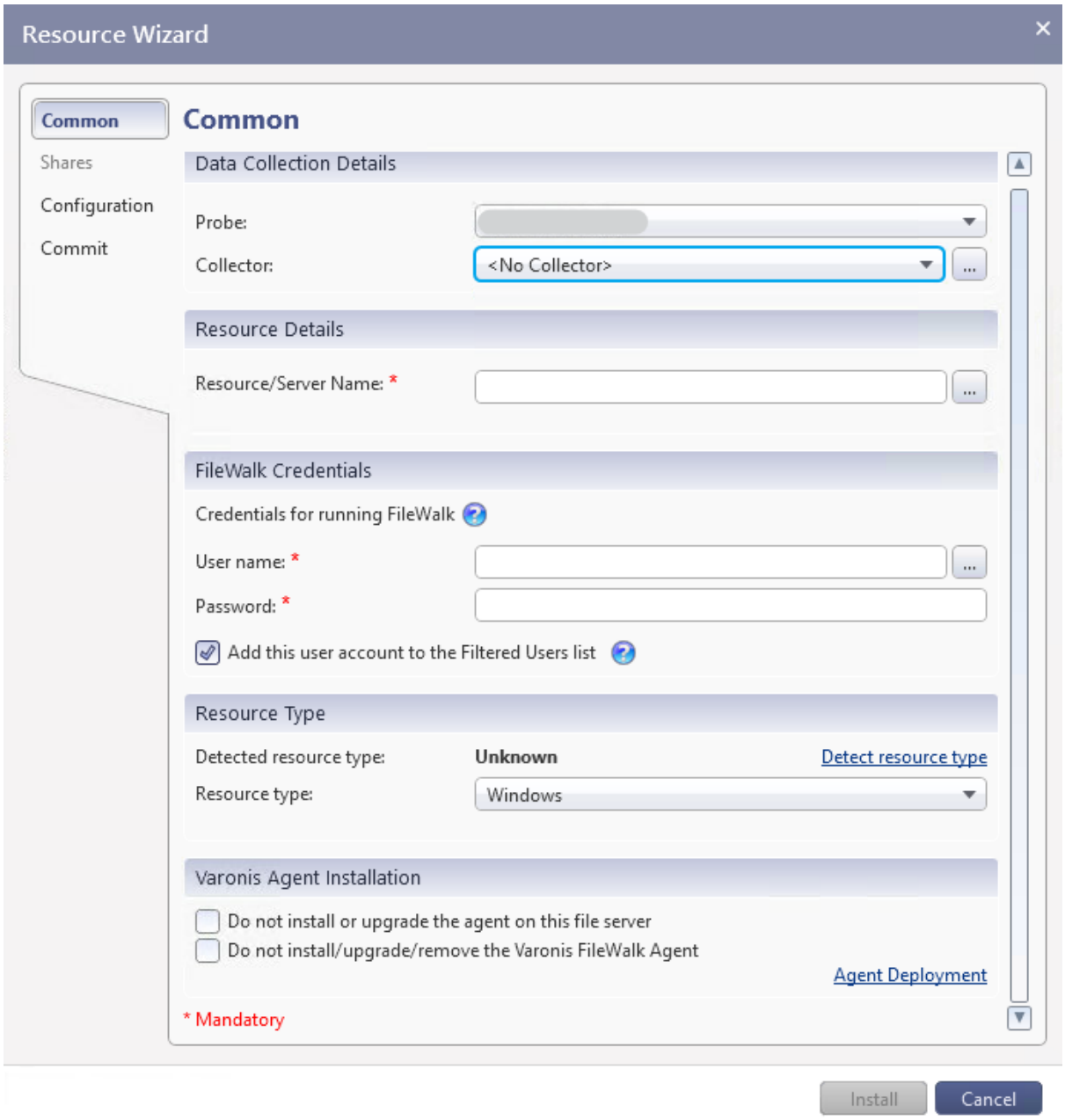
Adding to the Varonis security platform:

In the Management Console, select **Management** > **Components** > **Root** > **File Servers**, and on the **Resources** toolbar on the File Servers tab, click **Add**.



SECUBEAR

The Resource Wizard is opened.



1) On the left menu, click **Common** and set the following parameters:

- Resource Type
    - **Select resource type** - If you select a file server's type from this drop-down list, this is the type that is used no matter what type was detected earlier. **Note:** If you typed the file server's name manually, you must enter the FileWalk credentials before you can use the Detect link, due to permission requirements. If the type still cannot be detected, use the override field.
    - **Detect resource type** - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
    - **Detect resource type** - Click this link to detect the type of file server you selected. (If you used the Browse button to locate the file server's name, its type is detected automatically as long as you have already entered credentials.)
- Resource Details
    - **Resource/Server Name** - Type the resolved name or IP address of the file server to be added, or click the Browse button to locate it.
- Data Collection Details
    - **Probe** - From the drop-down list, select the Probe to be used with the file server.
    - **Collector** - From the drop-down list, select the required Collector. **Important**: Once you have configured a Collector to interface with a specific Probe, you must use that Collector with the same Probe. This means that if you have already configured a Collector to interface with the selected Probe while adding a monitored file server, you must either select the same Collector, a Collector that is not yet connected to a Probe, or <**No Collector**>. If no Collector is used with the Probe server, select <**No Collector**>.
- FileWalk Credentials - File System operations include the directory crawl (FileWalk), event collection (if set) and user crawl (ADWalk) on local accounts (if set). This account must have the backup operator and power user roles (Windows or NAS devices) on the file server during installation.
  Note: These credentials are cached, so that they are automatically entered if another file server is added during the same session.
    - **User name** - Type the name of the user account to be used for FileWalk, event collection and local ADWalk.
    - **Password** - Type the account's password.
    - **Add this user account to the Filtered Users list** - This is the default user account for Data Security Platform operations. If you clear this checkbox, a large number of events generated by the Data Security Platform will be collected.

- Varonis Agent Installation
    - **Do not install or upgrade the filter agent on this server** - Select this checkbox if you do not want the Varonis filter agent automatically installed or upgraded on the file server.
    - **Do not install/upgrade/remove the Varonis FileWalk agent** - Select this checkbox if you do not want the Varonis FileWalk agent automatically installed, upgraded, or removed from this file server.

2) To select specific shares for the file server, on the left menu, click **Shares** and do the following:

- In the Available Shares area, select the required shares and click the down arrow The selected shares are moved to the Registered Shares area.
- In the Ignore Detection column, select the shares to be ignored (and not be the subject of notifications) by the resource monitor. Note the following scenarios:
    - Shares manually moved from registered shares to available shares should be selected.
    - When users manually add shares from available shares to registered shares, the checkbox must be cleared.
- For each share, review and set the following information as required:
  Note: If the file server is installed only for use with DataPrivilege, event collection is disabled.
    - **Share Name** - The name of the share.
    - **Path** - The path on which the share resides.
    - **Protocol** - The protocol defined for the share.
    - **Events** - Select this checkbox to collect events for the share.
    - **Crawl** - To enable or disable monitoring for the share, in the Crawl column, select the relevant option.
      Note: You can also right-click the grid and select the required options for event collection and crawling.
    - **Mixed Security** - In Windows environments, NT ACL extraction is always used.
- In the Automatic Detection area, set the following:
    - **Automatically detect shares** - DatAdvantage detects shares that reside at the highest level of the hierarchy and that are not already monitored. It gives preference to administrative shares over equivalent regular shares. From the drop-down list, select the relevant option:
        - **Never** - Select to instruct DatAdvantage not to detect shares or mounts automatically.
        - **Detect and notify** - Select to send users email that lists all newly detected shares or mounts. Unreachable shares and mounts are removed from DatAdvantage.
        - **Detect and monitor** - Select to add the newly detected shares or mounts to the Registered Shares or Registered Mounts list in the dialog box, with the Events column checked and the Crawl

column set to enable crawling. Unreachable shares and mounts are removed from DatAdvantage.

- **Detect, monitor and notify** - Select to add the newly detected shares or mounts as described above, and send users email listing them. Unreachable shares and mounts are (removed from DatAdvantage.

  Note: Via the monitor selections, it is possible to add all the top-level shares per protocol (type) automatically as monitoring shares (for example, it is possible to add a 1st level share in CIFS protocol and 2nd level share in MIX mode). To remove a specific share from the monitoring shares list, move manually the required share from Register Shares to Available Shares, and select Ignore Detection to ensure the resource manager will not add this share automatically to the monitoring shares (relevant for NetApp only).

  Note: Shares using "mixed mode" are not supported.

- **Notify** - From the drop-down list, select the frequency at which to send notification of new shares or mounts. Options are:
  - **Always** - Select to send a cumulative list of all changes made (such as detection or deletion) to all shares and mounts.
  - **Once** - Select to send notification of a change (that is, detection or deletion) to a share or mount only when that change occurs.
- **Remove Deleted Shares** - Select this checkbox to remove deleted shares. Shares that were deleted from the file server will be displayed with a strikethrough red font. They will not be removed from the "Registered" list. If the file server is unavailable, the shares will not be removed.
- **Enable Event Collection** - Select this checkbox to collect events from all shares added from this volume/file server.

3) Click **Install**.
   The file server is installed.