



Winlogbeat Installation on Windows Systems

Contents

Preparation	2
Step 1: Downloading Winlogbeat	2
Step 2: Starting Winlogbeat	3
Link for More Information	4

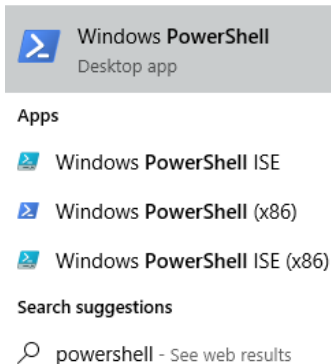
Preparation

Before installing Winlogbeat you will need:

- Notepad ++ or a program to edit .yml files

Step 1: Downloading Winlogbeat

1. Download the Winlogbeat from either the shared link or drive.
2. Move the Winlogbeat folder to C:\Program Files\
3. Click on the windows button and search for PowerShell.
 - Right click on PowerShell and click "Run as administrator"



4. Run the following commands while in PowerShell
 - cd 'C:\Program Files\Winlogbeat'
 - .\install-service-winlogbeat.ps1

PowerShell may return a Security warning – see example below – If so, type T and press enter.

*Note - If script execution is disabled on your system, you need to set the execution policy for the current session to allow the script to run. For example: PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1.

```
PS C:\Program Files\Winlogbeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Program Files\Winlogbeat\install-service-winlogbeat.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"):
```

- After pressing "enter" PowerShell will respond like the screenshot below.

```
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R
__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS    :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER         :
__NAMESPACE     :
__PATH           :
ReturnValue      : 5
PSComputerName   :

__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS    :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 1
__DERIVATION     : {}
__SERVER         :
__NAMESPACE     :
__PATH           :
ReturnValue      : 0
PSComputerName   :

Status          : Stopped
Name            : winlogbeat
DisplayName     : winlogbeat
```

Or


```
Security warning
Run only scripts that you trust. While scripts from the internet can be useful,
this script can potentially harm your computer. If you trust this script, use
the Unblock-File cmdlet to allow the script to run without this warning message.
Do you want to run C:\Program Files\Winlogbeat\install-service-winlogbeat.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): R

Status      Name           DisplayName
-----
Stopped    winlogbeat     winlogbeat
```

5. Winlogbeat is now installed, next we will start Winlogbeat.

Step 2: Starting Winlogbeat

1. Now Run `.\winlogbeat.exe test config -c .\winlogbeat.yml -e` in PowerShell to test the configuration file. You will get an end response that should say - **Config OK**
2. Input these lines into PowerShell as the administrator
 - `cd 'C:\Program Files\Winlogbeat'`
 - `Start-Service winlogbeat`

3. Winlogbeat should now be running. You can view your local logs at
C:\ProgramData\winlogbeat\Logs\winlogbeat
4. You can view winlogbeat in the Services, if you're still in PowerShell run –
 - cd 'C:\Program Files\Winlogbeat'
 - services.mscA screenshot of the Windows Services console. The 'winlogbeat' service is highlighted in blue. The status bar shows 'Running', 'Automatic', and 'Local System'.
5. You can either stop winlogbeat through services or through the PowerShell by running-
 - cd 'C:\Program Files\Winlogbeat'
 - Stop-Service winlogbeat

Link for More Information

<https://www.elastic.co/guide/en/beats/winlogbeat/7.9/winlogbeat-installation-configuration.html>

Any questions or concerns please email support@corvidcd.com or call 800-349-2549.

V20200915