INSTALL GUIDE · IT TEAMS AND MSPS

Windows health over WinRM

Watch Windows servers without installing anything on them. Uplivra reads CPU, memory, disks, uptime and services over WinRM, read-only, and tells you when a service you care about stops.

Uplivra Technologies LLC · Guide for Uplivra 26.10 · Updated 28 September 2026 · Latest version: https://uplivra.com/guides/windows-monitoring.html

What it measures

A **Windows health (WinRM)** check reads these from a Windows computer every few minutes:

- **CPU**, **memory** and each **disk's** use (with the same charts and thresholds as other checks)
- **Uptime**, so a surprise restart shows up
- **Services:**
- the ones you list must be running, and the check goes down when one stops;
- automatic services that aren't running are counted, as a hint.

It only runs WMI queries. Nothing is installed, and nothing is changed or started on the computer.

Before you start

1. WinRM is on. It is on by default on Windows Server 2012 and later. On other computers, run this once as an administrator:

```
winrm quickconfig
```

In a domain, you can turn it on for many computers with Group Policy: **Computer Configuration › Administrative Templates › Windows Components › Windows Remote Management**.

2. An account Uplivra can use. A normal domain account is enough if it is in the computer's **Remote Management Users** group and may read WMI. Administrators work too, but aren't needed.

3. The firewall lets the collector in:

- **TCP 5985** (HTTP), or
- **TCP 5986** if you use an HTTPS listener.

Over HTTP, the conversation is still encrypted, the same way Windows encrypts it for its own tools.

Add the check

1. **Settings › Device logins › Add a login** and choose **Windows**. Enter the user name, the domain (optional) and the password. It is stored encrypted and only sent to the collectors that need it.
2. Open the device. Under **Add a check**, choose **Windows health over WinRM**, and pick the login.
3. Optional: list **services that must be running**, for example `Spooler, MSSQLSERVER, W3SVC`. Service names or display names both work.
4. Optional: limit it to **some disks** (`C:, D:`).
5. Optional, under **Connection**: use the **HTTPS listener** (port 5986). If its certificate is self-signed, paste the certificate's SHA-256 fingerprint.

The first result arrives within a minute.

Troubleshooting

Message	What to do
Connection refused: WinRM isn't listening	Run `winrm quickconfig` on the computer, or turn WinRM on by Group Policy. Check that the firewall allows TCP 5985 from the collector.
Windows refused the sign-in	Check the user name, domain and password. Check that the account is in **Remote Management Users** (or Administrators) on that computer.
Doesn't accept NTLM sign-in over WinRM	The computer only allows Kerberos. Allow Negotiate authentication for WinRM, or use the HTTPS listener.
The HTTPS certificate isn't trusted	Paste the certificate's fingerprint into the check, or use HTTP, which is encrypted too.

Message	What to do
No such service	The service name is wrong or not installed. Run `Get-Service` on the computer to see the names.

Prefer SSH? The **Server health over SSH** check also reads Windows computers that have the built-in OpenSSH Server turned on.