

PS SERVER MONITOR - MANUAL

WHAT IS IT?

This tool will allow you to monitor:

- space on local drives of the server,
- event viewer - for the occurrence of events specified in the configuration.

This tool is configured using a simple xml configuration file.

REQUIREMENTS

- Powershell 4.0 or later,

DEPLOYMENT

INSTALLATION ON THE SERVER

Simply copy the downloaded package to the server and extract it to following path:

C:\ServerMonitor\

Remember that logs will be stored in the .\logs subfolder, so you will need dozen, up to several hundred megabytes per year for logs files.

CONFIGURATION

All parameters of Server Monitor you can set in the ServerMonitor.config file.

Example configuration:

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <configuration>
3      <!-- Checking Interval (in MINUTES) is the frequency of verification EVENTLOG and free disk space -->
4      <MonitorSettings>
5          <CheckingInterval>15</CheckingInterval>
6      </MonitorSettings>
7
8      <!-- Email addresses , which will be sent all notifications -->
9      <EmailAddressToNotify>
10         <email address="my@my-email.com"/>
11     </EmailAddressToNotify>
12
13     <!--Email Notify configuration-->
14     <!--You can use that variables for built email subject and body -->
15     <!-- $message, %checktime%, %hostname%, %domain% -->
16     <EmailSettings>
17         <SMTPPort>587</SMTPPort>
18         <SMTPAddress>smtp.my-email.com</SMTPAddress>
19         <EmailFromAddress>alerts@my-email.com</EmailFromAddress>
20         <EmailSubject>Alert | %hostname%</EmailSubject>
21         <EmailBody>On %checktime%, on server %hostname%/domain% following events occurred: %message%. Please do not
22             reply. The message is generated automatically</EmailBody>
23         <VaultCredentialName>alerts</VaultCredentialName>
24     </EmailSettings>
25
26     <!-- Disk Space monitor. Alerts in GB. You can add more disks. -->
27     <!-- You can use that variables in 'message' attribute: %drive%, %freespace%, %limit% -->
28     <DiskSpaceSettings>
29         <Disk name="c" alertlevel="10" message="On a %Drive% drive exceeded allowed minimum limit (%limit% GB) for free
30             disk space. There are %freespace% of free space left."/>
31         <Disk name="e" alertlevel="25" message="On a %Drive% drive exceeded allowed minimum limit (%limit% GB) for free
32             disk space. There are %freespace% of free space left."/>
33     </DiskSpaceSettings>
34
35     <!-- EventLog Monitor will send you an email when find defined event. You can add more events -->
36     <EventLogSettings>
37         <Event name="RDP ERROR" LogName="System" EventID="50" message="Service RDP report an error."/>
38         <Event name="System Start" LogName="System" EventID="12" message="Serwer Srv01 started."/>
39     </EventLogSettings>
40 </configuration>
```

The configuration is divided into five parts:

1) Monitor Settings

The tool works in a loop. Its length in minutes is determined by this parameter. If you set e.g. 15 minutes here, the disk space, logs will be checked at this frequency and if the condition is met an e-mail will be sent.

Email address to notify.

This parameter specifies the address to which notifications will be sent.

2) Email settings.

This configuration node contains the parameters of the e-mail box from which notifications will be sent.

3) Disk space monitor settings

This node specifies the parameters of the drives to be monitored. The configuration contains the following attributes:

- Name – drive letter
- Alert level - defines the free space threshold (in GB) below which notifications are sent.
- Message - defines the text of the notification. You can use following tags to describe alert details:
 - %Drive% - will be replace to drive letter
 - %limit% - will be replace to alert level
 - %freespace% - will be replace to the size of the available space in GB.

4) Event logs settings.

This node defines what values we look for in eventlog. If they do, a notification will be sent. The configuration contains the following attributes:

- Name - Label - will be used in the notification e-mail. It is not checked in eventlog.
- LogName - defines the log in which the event is searched for.
- Defines the ID you are looking for in the eventlog. This is the field used to search for events in eventlog.
- Message - defines the text of the notification.

CREDENTIAL MANAGER CONFIGURATION

As you can see, in the configuration file (in the email settings node), it does not store the login and password needed to authenticate the mailbox. I consider it a bad practice to keep such data in a plain text. Fortunately, in Windows, we have a special place where we can safely store credentials in a classified form. This is what Credential Manager is all about. To use it, we need to include appropriate credentials in it.

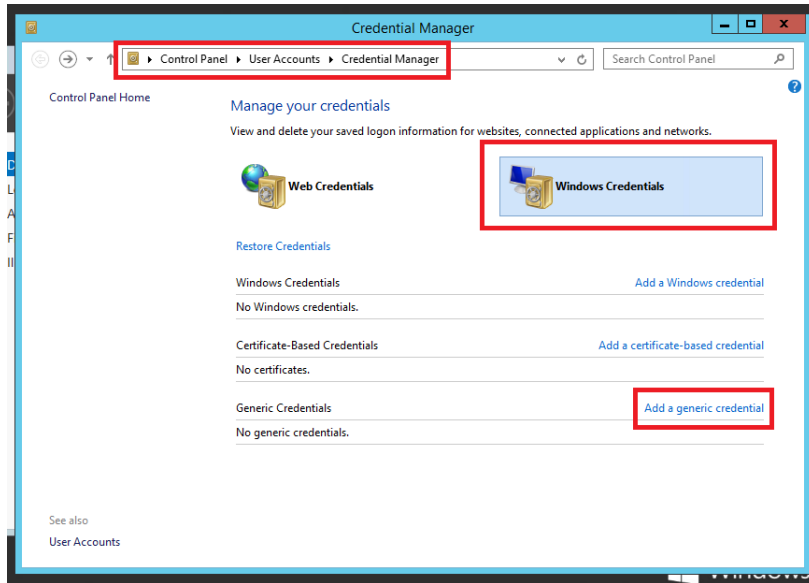
Note the EmailSettings node and VaultCredentialName attribute in the configuration file. There we will place the name of the container in which we will store credentials in Windows Credential Manager.

Configuration steps:

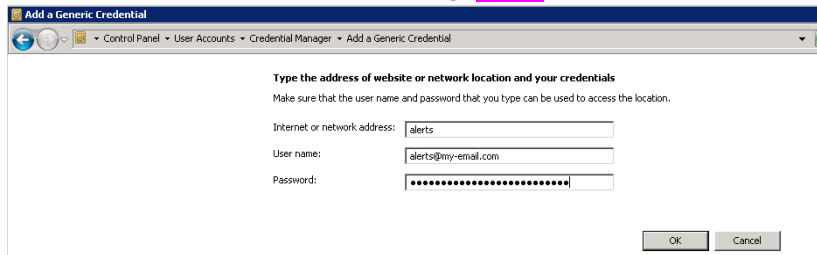
1. Open ServerMonitor.config and insert the name of the container with credentials in the credentialsVaultName attribute – e.g. **alerts**.

```
<EmailSettings>
  <SmtpPort>587</SmtpPort>
  <SmtpAddress>smtp.my-email.com</SmtpAddress>
  <EmailFromAddress>alerts@my-email.com</EmailFromAddress>
  <EmailSubject>Alert | %hostname%</EmailSubject>
  <EmailBody>On %checktime%, on server %hostname%/%domain% following events occurred: %message%. Please do not reply. The message is generated automatically</EmailBody>
  <VaultCredentialName>alerts</VaultCredentialName>
</EmailSettings>
```

2. Open **Credential Manager**. Open **Windows Credentials** and in select **New generic credentials**



3. In the **Add a Generic Credentials** fill the all fields. Field Internet or network address should contain your credentialsVaultName value (e.g. **alerts**).



INSTALLATION

To install PS Monitor as a service, please open cmd.exe with elevated privileges, navigate to the c:\ServerMonitor (where you extracted the binaries) and execute following command:

```
Administrator: Wiersz polecenia
c:\>cd ServerMonitor
c:\ServerMonitor>.\ServerMonitor.exe /install
c:\ServerMonitor>
Running a transacted installation.
Beginning the Install phase of the installation.
See the contents of the log file for the c:\ServerMonitor\ServerMonitor.exe assembly's progress.
The file is located at c:\ServerMonitor\ServerMonitor.InstallLog.
Installing assembly 'c:\ServerMonitor\ServerMonitor.exe'.
Affected parameters are:
  logtoconsole =
  assemblypath = c:\ServerMonitor\ServerMonitor.exe
  logfile = c:\ServerMonitor\ServerMonitor.InstallLog
Installing service 35-ServerMonitor...
Service 35-ServerMonitor has been successfully installed.
Creating EventLog source 35-ServerMonitor in log Application...
The Install phase completed successfully, and the Commit phase is beginning.
See the contents of the log file for the c:\ServerMonitor\ServerMonitor.exe assembly's progress.
The file is located at c:\ServerMonitor\ServerMonitor.InstallLog.
Committing assembly 'c:\ServerMonitor\ServerMonitor.exe'.
Affected parameters are:
  logtoconsole =
  assemblypath = c:\ServerMonitor\ServerMonitor.exe
  logfile = c:\ServerMonitor\ServerMonitor.InstallLog
The Commit phase completed successfully.
The transacted install has completed.
```

TEST

In the services.msc you will find new service. Please change the startup type to "Automatic" and Start the service.

If you have configured everything well, the service should create a path c:\ServerMonitor\logs and start logging in to the file in this folder.

Example logs:

```
2018-06-28|00:22:24 :[INFO] Starting Service
2018-06-28|00:22:24 :[INFO] Loading configuration file
2018-06-28|00:22:24 :[INFO] Processing Functions
2018-06-28|00:22:25 :[INFO] Starting Monitor - searching interval - 15 min.
2018-06-28|00:22:25 :[INFO] Searching point: 06/27/2018 23:52:25
2018-06-28|00:22:25 :[INFO] c: - ok.
2018-06-28|00:22:25 :[INFO] e: - ok.
2018-06-28|00:22:37 :[INFO] defined events not found.
2018-06-28|00:22:48 :[INFO] defined events not found.
2018-06-28|00:22:48 :[INFO] Searching benchmark: 22.1959287 sec.
```

In my configuration, the space on two c and e disks is checked. In both cases the vacancy threshold was not reached. I have also defined two events which, if detected, should result in sending a notification. Both were not found. The check interval is 15 minutes, so the search point is set to the current time minus 15 minutes.

The biggest problems with proper tool configuration are on the side of mailbox configuration. Read your email provider's documentation carefully and you'll be able to do it well. In my opinion, it works perfectly.