Microsoft Windows Monitors

Windows Event Log Scanner

The Windows Event Log Scanner alerts on specific entries in a Windows log file. This monitor uses text strings or substrings to search through events, and can restrict searches to specific types of logs or errors. When the monitor runs, with WMI-based collection, events are retrieved in 15-minute batches; with agent-based collection, the number of events retrieved is user-defined.

To prevent false positives, when searching for matches, the monitor only scans as far back as the previous check; it does not alert on data further back than that. Because of this behavior, when the monitor is first set up, its initial run does not produce any results. (Its status message is, " *This is the first run. Nothing to do.* ") Its second run then looks for matches in the time slice between the current and initial run.

To avoid performance degradation, maximum number of log entries (which has a default 1,000) is 10,000 lines.

Configuring Windows Event Log Scanner Monitors

To configure Windows Event Log Scanner monitors, do the following:

1. In the Windows Event Log Scanner monitor template, complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. Complete the following fields:
   - Event Log Type
     Choose one of the following types of event log to search:
     - Application
       A log that records events generated by programs running on the server.
     - System
       A log that records the activity of various components of the operating system.
     - Security
       A log that records events such as login attempts and attempts to access files.
     - Other
       A custom or external log whose name is defined in the next step.
   - Other Windows Log to Search
     When the "Other" event log type is selected in the previous step, this field appears. Enter the name of an additional Windows event log that you want this service monitor to use. This log may accompany an application platform you are running, or could be a custom log; regardless, the name you provide should match the name that appears in the Windows Event Viewer.
   - Match event type with
     The type of event to search for, which can be one of the following:
     - Information
       Describes the successful completion of a task.
     - Warning
       Indicates that a problem may occur in the future.
     - Error
       A problem, which may involve the loss of data or system integrity, has occurred.
     - Success Audit
       Found in the Security log, this describes the successful completion of an audited security event.
     - Failure Audit
       Found in the Security log, this describes the failure of an audited security event.
   - Number of Lines
     The number of lines in the log file that *up.time* scans, using the criteria specified in the monitor template. The default is *1000* and the maximum is *10000*.
   - Match source with
     The application, system component, or application module that triggered the event.
   - Match category with
     The way in which the application, system component, or application module that triggered the event classifies the event. For example: System Event (in the Security Log); or Installation, CI Service,
     or wrapper (in the Application and System logs).
   - Match event ID with
     A number that identifies the type of event.
   - Match user name with
     The name of the user associated with a logged event.
   - Match computer name with
     The name of the computer on which the event occurred.
   - Search description for
     Enter the exact string or substring that is searched for in the event log, for example:
     The WMI Performance Adapter service entered a stopped state
     or
     stopped state
     Note that the monitor does not process regular expressions.
   - Response Time
     Enter the Warning and Critical Response Time thresholds for the length of time a service check takes to complete. For more information, see Configuring Warning and Critical Thresholds.
     To save the data from the thresholds for graphing or reporting, click the *Save for Graphing* checkbox beside the Response Time metrics.
3. Complete the following settings:
   - Timing Settings (see Adding Monitor Timing Settings Information for more information)
   - Alert Settings (see Monitor Alert Settings for more information)
   - Monitoring Period settings (see Monitor Timing Settings for more information)
   - Alert Profile settings (see Alert Profiles for more information)
   - Action Profile settings (see Action Profiles for more information)
4. Click *Finish*.

Windows Service Check

The Windows Service Check monitor alerts you to changes in the status of Windows services. Windows services are processes that extend the features of Windows by providing support to other programs; they are controlled in the Microsoft Management Console. The default installation of Windows provides a core set of services and configurations that suits most needs.

There are approximately 100 services in the Windows Server family of operating systems. You can add services that you develop, or by installing third-party applications on a system.

Every Windows service has one of the following states, which control how the services are launched or prevented from launching:

- Disabled
  Services that are installed but not currently running.
- Set to manual
  Services that are installed but start only when another service or application needs its functions.
- Set to automatic
  Services that are started by the operating system after device drivers are loaded at boot time.

Configuring Windows Service Check Monitors

To configure Windows Service Check monitors, do the following:

1. In the Windows Service Check monitor template, complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. Complete the following fields:
   - Service Name (Mandatory)
     Use the service **Display name** shown in Services (which can be accessed from the Windows Control Panel). If you are logged into Windows as an administrator, Services shows all locally available Windows services, their states, and their status. Double-clicking a service displays its properties, including its actual system service name, as well as the descriptive Display name that is used to configure the Windows Service Check monitor.

     > If you enter the name of a service that does not exist, or mistype the name, the monitor changes the status of the service to Critical.

   - Service Status (Mandatory)
     Select a comparison method from the dropdown list, and then select one of the following:
     - Stopped: the service is stopped
     - Start Pending: the service is stopped or paused while waiting for another process or condition to be satisfied before starting
     - Stop Pending: the service is running while waiting for another process or condition to be satisfied before stopping
     - Running: the service is running
     - Continue Pending: the service is waiting for another process or condition to be satisfied before continuing to run the service
     - Pause Pending: the service is running while waiting for another process or condition to be satisfied before pausing the service
     - Paused: the service is paused
   - Response Time
     Enter the Warning and Critical Response Time thresholds. For more information, see Configuring Warning and Critical Thresholds.
3. To save the data from the thresholds for graphing or reporting, click the **Save for Graphing** check box beside each of the metrics that you selected in the previous step.
4. Complete the following settings:
   - Timing Settings (see Adding Monitor Timing Settings Information for more information).
   - Alert Settings (see Monitor Alert Settings for more information)
   - Monitoring Period settings (see Monitor Timing Settings for more information).
   - Alert Profile settings (see Alert Profiles for more information)
   - Action Profile settings (see Action Profiles for more information)
5. Click **Finish**.

Windows File Shares (SMB)

The Windows File Shares (SMB) monitor can check the availability of file shares on a Windows server. If a file share is not available, the status of this monitor becomes critical and *up.time* sends an alert.

Configuring Windows File Shares (SMB) Monitors

To configure Windows File Shares (SMB) monitors, do the following:

1. In the Windows Files Shares (SMB) monitor template, complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. Complete the following fields:
   - Username
     The user name that is required to login to the file share. The value entered can include the file share domain if input with the following formats: *<domain>\<username>* or *<domain>;<username>*
   - Password
     The password that is required to log in to the file share.
   - Shares
     The names of file shares that you want to monitor on a host system. Specify the name of the file share - for example *Main* .
     To specify multiple file shares, add a comma between the names - for example, *Main, home*.
     To check all of the file shares on a system, leave this field blank.
   - Response Time
     Enter the Warning and Critical Response Time thresholds. For more information, see Configuring Warning and Critical Thresholds.

3. Click the *Save for Graphing* checkbox to save the data for a metric to the DataStore, which can be used to generate a report or graph.
4. Complete the following settings:
    - Timing Settings (see Adding Monitor Timing Settings Information for more information).
    - Alert Settings (see Monitor Alert Settings for more information)
    - Monitoring Period settings (see Monitor Timing Settings for more information).
    - Alert Profile settings (see Alert Profiles for more information)
    - Action Profile settings (see Action Profiles for more information)
5. Click *Finish* .

Active Directory

Active Directory is a distributed network management service that is included in the Microsoft Windows Server 2003 operating system. Active Directory provides a centralized location for all of the information about the services and resources within your network. Using this information, you can easily manage information about users, network devices, and any other resources that you might find useful to maintain.

The Active Directory monitor can check for any settings or information in your Active Directory. The monitor can start the check from any location within your Active Directory structure.

The Active Directory monitor attempts to match information that you have specified with information available in your Active Directory. If the monitor finds the information, the service monitor returns a status of OK. Otherwise, the monitor returns a Critical error and *up.time* generates an alert.

Configuring Active Directory Monitors

To configure Active Directory monitors, do the following:

1. In the Active Directory monitor template, complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. Complete the following fields:
    - Port
      The number of the port number on which the Active Directory server is listening.
    - Password
      The password that is required to log in to the Active Directory server.
    - Base
      The location in the Active Directory from which you want the monitor to begin searching for information.
    - Bind
      The Bind string, which associates user account properties and Active Directory account attributes. This string gives you access to the Base location of your Active Directory structure.
      The format of the Bind string must match the Base location of your Active Directory structure. Depending on your network security model, you must have domain controller administration privileges to bind to the locations on which you want to match information.
    - Attribute
      The attribute or information for which you want to search in your Active Directory.
      An Active Directory entry consists of a set of attributes. Each attribute has a type - which describes the kind of information contained in the attribute - and one or more values, which contain the actual data. For example, the entry *jsmith@inter.net* has the Attribute value *jsmith@inter.net*. The Attribute type is *e-mail*.
    - Response Time
      Enter the Warning and Critical Response Time thresholds. For more information, see Configuring Warning and Critical Thresholds.
3. Optionally, click the *Save for Graphing* checkbox beside the *Response Time* option to save the data for a metric to the DataStore, which can be used to generate a report or graph.
4. Complete the following settings:
    - Timing Settings (see Adding Monitor Timing Settings Information for more information).
    - Alert Settings (see Monitor Alert Settings for more information)
    - Monitoring Period settings (see Monitor Timing Settings for more information).
    - Alert Profile settings (see Alert Profiles for more information)
    - Action Profile settings (see Action Profiles for more information)
5. Click *Finish*.