



Overview of What You Can Monitor with MonitorIT

This document provides an overview of the different types of items that you can monitor with MonitorIT. This is not a complete, exhaustive list but rather suggestive of what is possible using the various MonitorIT "Watch" types. MonitorIT uses the term "Watch" to refer to a monitoring rule you create.

The degree of how MonitorIT can address these various items listed here is categorized as COMPLETE or PARTIAL.

If there is scenario or aspect that you want to monitor on a Windows Server or Workstation, or a Linux/Unix/Solaris Server, or a Switch, Router, Firewall Infrastructure Device, contact Breakout Software support and we will work with you to define a monitoring rule ("Watch") where possible to solve your requirement. You would be surprised as to how many different scenarios that a monitoring rule can be devised to solve a monitoring problem.

1) **ADSI and Active Directory checks**

PARTIAL: MonitorIT's Windows Services and Process monitoring, as well as Event Log and CounterWatch monitoring will provide partial support for monitoring aspects of AD. MonitorIT does support ADSI in its console information it provides for several screens so MonitorIT is ADSI "aware" and we are working so this knowledge can be extended to provide monitoring of AD, NTDS and NDS aspects via ADSI and LDAP for specific User, Group, OU, etc. checks.

Also, with CustomWatch, use ADSI VB scripts or other Windows scripting to create a monitoring feature that monitors an aspect of AD that you want, and integrate this into MonitorIT alerting and reporting.

2) **Anti-Virus check**

COMPLETE: FileWatch, and the other various MonitorIT watch types cover this completely.

3) **CPU Usage check**

COMPLETE: CounterWatch monitoring of the '% Processor Time' Counter of the 'Processor' Performance Object.

4) **Directory Size check**

COMPLETE: FileWatch option.

5) **Disk Drive check**

COMPLETE: CounterWatch, various counters in the 'Physical Disk' and 'Logical Disk'

MonitorIT®

Performance Objects, and Event Log events via EventLogWatch

6) **Disk Space check**

COMPLETE: Default via AGENT Watch, also CounterWatch

7) **DNS Server check**

COMPLETE: ServerWatch-DNS

8) **Event Log check**

COMPLETE: High-performance, very flexible, real-time Event Log monitor including all Microsoft event logs as well as user custom event logs.

9) **File check**

COMPLETE: FileWatch options

10) **FTP check**

PARTIAL: ServerWatch-FTP but no credential handling.

11) **HTTP check**

COMPLETE: ServerWatch-HTTP

12) **Humidity check**

COMPLETE: Usually handled via SNMP Query and/or SNMP Trap monitoring of the environment device.

13) **ICMP Ping check**

COMPLETE: ServerWatch-PING

14) **IMAP Mailserver check**

PARTIAL: ServerWatch-USER which is the TCP Port check to check for responsiveness.

Also, with CustomWatch, use VB scripts or other Windows scripting to create a monitoring feature that monitors an aspect of IMAP that you want, and integrate this into MonitorIT alerting and reporting.



15) **LDAP check**

PARTIAL: ServerWatch-USER which is the TCP Port check to check for responsiveness.

Also, with CustomWatch, use ADSI or LDAP VB scripts or other Windows scripting to create a monitoring feature that monitors an aspect of LDAP that you want, and integrate this into MonitorIT alerting and reporting.

16) **Memory check**

COMPLETE: Default via AGENT Watch, also CounterWatch , various counters in the 'Memory' Performance Object

17) **MS Exchange 2000/2003/2007 check**

COMPLETE: CounterWatch, WinServicesWatch, ProcessWatch, EventLogWatch

18) **MS ISA 2000/2004 check**

COMPLETE: CounterWatch, WinServicesWatch, ProcessWatch, EventLogWatch

19) **MS SQL / ADO check**

COMPLETE: ServerWatch-SQL, CounterWatch, WinServicesWatch, ProcessWatch, and EventLogWatch; EXCEPT no check of retrieving data.

20) **MS TSE check**

COMPLETE: CounterWatch, WinServicesWatch, ProcessWatch, EventLogWatch

21) **NNTP New Server check**

PARTIAL: ServerWatch USER which is the TCP Port check to check for responsiveness.

22) **Novell NDS**

PARTIAL: See (1) above regarding current ADSI, LDAP awareness and work to extending and adding this specific monitoring capability for Accounts, Groups, OUs, etc.

Also, with CustomWatch, use ADSI or LDAP VB scripts or other Windows scripting to create a monitoring feature that monitors an aspect of NDS that you want, and integrate this into MonitorIT alerting and reporting.

MonitorIT®

23) NTDS

PARTIAL: See (1) above regarding current ADSI, LDAP awareness and work to extending and adding this specific monitoring capability for Accounts, Groups, OUs, etc.

Also, with CustomWatch, use ADSI or LDAP VB scripts or other Windows scripting to create a monitoring feature that monitors an aspect of NTDS that you want, and integrate this into MonitorIT alerting and reporting.

24) ODBC Database check

COMPLETE: ServerWatch-ODBC

25) Oracle Database check

COMPLETE: ServerWatch-ORACLE

26) POP3 Mailserver check

COMPLETE: ServerWatch-POP

27) Printer check

COMPLETE: CounterWatch, WinServicesWatch, EventLogWatch

28) Process check

COMPLETE: ProcessWatch options

29) Scheduled Task check

COMPLETE: FileWatch options, EventLogWatch

30) Service check

COMPLETE: WinServicesWatch options

31) SMTP Mailserver check

COMPLETE: ServerWatch-SMTP

MonitorIT®

32) **SNMP check**

COMPLETE: ServerWatch-SNMP, as well as complete SNMP Trap & Query CounterWatch monitoring.

33) **TCP Port check**

COMPLETE: ServerWatch-USER, meaning user customizable TCP port check for any port and for sending any custom text and optionally verifying any text response.

34) **Temperature check**

COMPLETE: Usually handled via SNMP Query and/or SNMP Trap monitoring of the environment device.

35) **UDP check**

COMPLETE: SNMP Query CounterWatch monitoring.

36) **UNIX Shell Script (RSH) check**

PARTIAL: MonitorIT includes a separate Linux/Unix Agent, implemented in Java so it runs on all Unix platforms including on Linux, Solaris, SUSE, AIX, SCO/Unixware, HP-UX and ESX from VMware. This Agent provides monitoring of disk space, memory, CPU utilization, processes, uptime, and availability.

37) **Users & Groups check**

PARTIAL: See (1) above regarding current ADSI, LDAP awareness and work to extending and adding this specific monitoring capability for Accounts, Groups, OAU, etc.

Also, with CustomWatch, use ADSI or LDAP VB scripts or other Windows scripting to create a monitoring feature that monitors an aspect of AD Users & Groups that you want, and integrate this into MonitorIT alerting and reporting.

38) **VBScript check**

COMPLETE: CustomWatch executes any user provided Windows executable including scripts on a specified scheduled basis with alerting and reporting based on executable exit code.

39) **Wetness check**

COMPLETE: Usually handled via SNMP Query and/or SNMP Trap monitoring of the environment device.

MonitorIT®

40) **WMI**

COMPLETE: CustomWatch executes any user provided Windows executable including scripts on a specified scheduled basis with alerting and reporting based on executable exit code.