NETERRA
telecommunications

Additional Parameters for the Windows Environment Monitoring Service

PARAMETER	DESCRIPTION	OK	WARNING	CRITICAL
Page File Usage	Monitors the utilization of the Windows Page File (Virtual Memory).	Usage < 70%	Usage >= 85%	Usage >= 95%
Handle Count	Monitors the total number of open handles (potential resource leaks).	< 50,000	>= 100,000	>= 200,000
Thread Count	Monitors the total number of active threads in the system.	< 2,000	>= 5,000	>= 10,000
Processor Queue Length	Number of threads waiting for CPU time (indicates CPU bottleneck).	Queue < 2 per core	Queue >= 5 per core	Queue >= 10 per core
System Context Switches	Combined rate at which processors switch between threads.	< 10,000 / sec	>= 20,000 / sec	>= 50,000 / sec
Memory Pages/sec	Rate at which pages are read from or written to disk to resolve hard page faults.	< 100 / sec	>= 500 / sec	>= 2,000 / sec
Non-paged Pool Memory	Monitors memory that cannot be swapped to disk (critical for driver stability).	Within normal baseline	20% above baseline	50% above baseline
Windows Time Sync	Checks if the Windows Time service (W32Time) is synchronized with a DC or NTP.	Synchronized	Offset > 1 sec	Not Synced / Service Stopped
Registry Quota Usage	Monitors the size of the Windows Registry against the system limit.	Usage < 70%	Usage >= 85%	Usage >= 95%
Zoned Out (Zombie) Processes	Detects processes that have crashed or hung but still occupy memory.	Count = 0	Count >= 2	Count >= 5
Active Directory Replication	Checks for successful synchronization between Domain Controllers.	No replication errors	Error in last 12h	Error in last 1h / Sync failed
DNS Cache Hit Rate	Monitors the efficiency of the local DNS server cache.	Hit Rate > 80%	Hit Rate < 60%	Hit Rate < 40%
DHCP Scope Exhaustion	Monitors the percentage of available IP addresses in DHCP scopes.	Free IPs >= 20%	Free IPs < 10%	Free IPs < 5%
AD Database Size	Monitors the growth of the NTDS.dit file (Active Directory database).	Normal growth	Unexpected 10% spike	Drive capacity at risk
NTDS Client Sessions	Number of active client sessions connected to the Directory Service.	< 1,000	>= 3,000	>= 5,000
DNS Recursive Queries	Monitors the volume of recursive DNS queries handled per second.	Within baseline	2x Baseline	5x Baseline (Possible attack)
Global Catalog Availability	Checks if the Domain Controller is reachable as a Global Catalog server.	Reachable	-	Unreachable / Port 3268 closed
IIS Worker Process Health	Monitors the memory and CPU usage of W3WP.exe processes.	Normal usage	High memory/CPU spike	Process crashed/hung
IIS Current Connections	Monitors the total number of active HTTP connections to IIS.	< 5,000	>= 10,000	>= 20,000
IIS Requests Per Sec	Throughput of incoming web requests handled by the server.	Within baseline	> 500 / sec	> 2,000 / sec
SQL Buffer Cache Hit Ratio	Efficiency of the SQL Server data cache in memory.	Ratio > 95%	Ratio < 90%	Ratio < 85%
SQL Deadlocks / sec	Frequency of transaction deadlocks within SQL Server.	0 / sec	> 1 / sec	> 5 / sec
SQL Batch Requests / sec	Total number of T-SQL command batches received per second.	Within baseline	2x Baseline	5x Baseline
SQL User Connections	Number of active users/applications connected to the database.	< 500	>= 800	>= 1,000 (Limit reached)
SQL Log File Free Space	Monitors free space within the SQL Transaction Log files.	Free Space >= 20%	Free Space < 10%	Free Space < 5%
Disk Latency (C: Drive)	Monitors average disk transfer time (latency) in milliseconds.	< 10ms	>= 25ms	>= 50ms
Disk Write Bytes/sec	Throughput of data being written to the physical disk.	Within baseline	80% of disk bandwidth	95% of disk bandwidth
Shadow Copy (VSS) Status	Checks the health and space usage of Volume Shadow Copies.	VSS Healthy	Space usage > 80%	VSS Failed / Storage Full
File System Corruption	Monitors the event log for NTFS or ReFS corruption errors (Chkdsk).	No errors	-	Corruption detected / Event 55
BitLocker Status	Verifies that the drive volume is encrypted and protected.	Fully Encrypted	Encryption in progress	Decrypted / Protection Off
Disk Fragmentation	Monitors the fragmentation percentage of NTFS logical drives.	< 10%	>= 20%	>= 40%
Folder Size (Logs)	Monitors the specific size of a directory (e.g., C:\inetpub\logs).	< 5GB	>= 10GB	>= 20GB
RDP Failed Logins	Monitors failed RDP login attempts (Security Event Log 4625).	< 10 per hour	>= 50 per hour	>= 100 (Brute force alert)
Account Lockouts	Checks for users being locked out of the system (Event 4740).	0 lockouts	>= 5 lockouts	>= 10 lockouts
Windows Firewall Status	Verifies that the Windows Firewall is active for all profiles.	Firewall ON	-	Firewall DISABLED
Antivirus (Windows Defender)	Checks if the AV service is running and definitions are up to date.	Up to date / Running	Outdated definitions	Service stopped / Threat detected
User Added to Admin Group	Alerts when a user is added to the local or domain Administrators group.	No changes	-	NEW ADMIN ADDED
AppLocker / Code Integrity	Monitors for blocked executions of unauthorized software.	No blocks	-	Unauthorized execution attempt
Pending Windows Updates	Checks for the number of updates waiting to be installed.	0 updates	> 5 updates	Critical/Security updates pending
Last Boot Time	Monitors if the system has been running too long without a reboot patch.	< 30 days	> 60 days	> 90 days
Print Spooler Errors	Monitors the Print Spooler service for stuck jobs or crashes.	0 errors	> 5 stuck jobs	Service stopped
Certificate Store Expiry	Checks for expiring SSL/TLS certificates in the Windows Store.	> 30 days	< 15 days	< 7 days / Expired
Recycle Bin Size	Monitors the amount of space wasted in the system Recycle Bin.	< 2GB	>= 5GB	>= 10GB
VM Health Status	Monitors the operational state of all Virtual Machines.	All VMs Running	VM Suspended/Saved	VM Failed/Power Off
Hyper-V CPU Usage	CPU resources consumed by the Hypervisior and Guest VMs.	< 80%	>= 90%	>= 95%
Dynamic Memory Status	Monitors the pressure on RAM for VMs using Dynamic Memory.	Pressure < 80%	Pressure >= 90%	Out of Memory / Ballooning
VM Snapshot Age	Monitors how long a VM snapshot (checkpoint) has been active.	< 24 hours	> 3 days	> 7 days (Disk performance risk)