

Using BMC[®] Performance Manager to Monitor and Manage
Microsoft Windows Active Directory

BMC SOFTWARE'S ACTIVE DIRECTORY SOLUTION	3
Instantly Up and Monitoring	3
MAKING EVENT LOGS EASY	4
DNS Events to Watch	4
Core Active Directory Service Events to Watch	5
File Replication Service and Group Policy Events to Watch	5
Time Synchronization Service Event to Watch	5
Kerberos Event to Watch	6
Netlogon Event to Watch	6
Customized Event Filtering	6
ASSURING REPLICATION	7
Parameters to Watch	7
SUPPORTING FSMO ROLES	9
Parameters to Watch	9
PROPERLY PROPAGATING GROUP POLICY OBJECTS	10
Parameter to Watch	10
ENSURING RAPID ACTIVE DIRECTORY RESPONSE TIME	10
Parameters to Watch	11
KEEPING UP WITH DOMAIN NAMING SERVICE DEMANDS	12
Parameters to Watch	12
CONTROLLING DC HEALTH	14
Parameters to Watch	14
TRACKING TRUST RELATIONSHIPS	15
Parameters to Watch	15
Reference	15
Helping You Maintain Advantage	15

BMC SOFTWARE'S ACTIVE DIRECTORY SOLUTION

BMC Software solutions for monitoring and managing Microsoft Windows Active Directory includes the following Knowledge Modules (KMs), which are part of the BMC Performance Manager for Servers product:

- > PATROL Knowledge Module for Microsoft Windows Active Directory
- > PATROL Knowledge Module for Microsoft Windows
- > PATROL Knowledge Module for Microsoft Windows Domain Services

This paper explains how to use these KMs to

- > automatically browse Windows event logs, looking for key events identified by Microsoft that indicate problems with Active Directory
- > pinpoint potential replication issues before they turn into larger problems
- > ensure that each of the FSMO role holders are available
- > ensure that Group Policy Objects are propagating properly among domain controllers
- > monitor both the total and individual response times of various services and processes within Active Directory to determine the cause for poor Active Directory response times
- > ensure that DNS servers are not overloaded by monitoring DNS response time and the rate at which the server receives update requests
- > ensure that domain controllers remain healthy by monitoring operating system CPU, memory usage, and disk space, and the disk space used by the Active Directory database, Netlogon, and other services on which Active Directory depends
- > monitor trust relationships to ensure that resources used by multiple domains are always available

Instantly Up and Monitoring

There is no configuration necessary for BMC Performance Manager to monitor Active Directory. Once installed, the PATROL KM for Active Directory instantly begins monitoring the Domain Controller (DC) on which it is loaded.

MAKING EVENT LOGS EASY

Because Microsoft writes errors to the event logs when certain types of failures occur, the event log can be a good indicator of Active Directory health, particularly when errors include problems with services, failed logons, or object/policy consistency problems.

One way to find errors related to Active Directory is by browsing through the event logs of each domain controller. In a large environment, this can mean sorting through thousands of events on dozens or even hundreds of servers. To do this more efficiently, use the PATROL KM for Active Directory to automate this process by looking for key events identified by Microsoft as indicative of problems.

The PATROL KM for Active Directory has predefined AD event filters in the PATROL KM for Windows OS that automatically monitor events pertaining to

- > DNS Name Registration
- > Core Active Directory Service
- > File Replication Service and Group Policy
- > Time Synchronization Service
- > Kerberos
- > Netlogon

DNS Events to Watch

The following events have been determined by Microsoft to be critical DNS events because they indicate a domain controller had a problem registering DNS records. The predefined AD event filters in the PATROL KM for Windows OS monitor these events.

Event Log	Source	Event	Why Event is Important
System	DNSAPI	11154, 11166	DC does not have sufficient rights to perform a secure dynamic update
System	DNSAPI	11150, 11162	DNS server timed out
System	DNSAPI	11152, 11153, 11164, 11165	zone or currently connected DNS server does not support dynamic update
System	DNSAPI	11151, 11155, 11163, 11167	resource record for DC is not registered in DNS
System	NETLOGON	5773	one or more DC locator records are not registered because primary DNS server does not support dynamic update

The PATROL KM for Domain Services also monitors other facets of DNS. For more information, see [“Keeping Up with Domain Naming Service Demands”](#) on page 12.

Core Active Directory Service Events to Watch

The following events have been determined by Microsoft to be critical AD service events because they indicate problems with core Active Directory functionality. The predefined AD event filters in the PATROL KM for Windows OS monitor these events.

Event Log	Source	Event	Why Event is Important
Directory Service	All Sources	Severity = error	primary error events for Active Directory service
System	LSASS	Severity = error	core security subsystem for Active Directory

File Replication Service and Group Policy Events to Watch

The following events have been determined by Microsoft to be critical File Replication Service (FRS) and Group Policy events because they may indicate problems with Sysvol replication or the application of group policy. The predefined AD event filters in the PATROL KM for Windows OS monitor these events.

Event Log	Source	Event	Why Event is Important
FRS	All Sources	Severity = error	FRS is used to synchronize policy between all DCs in the forest
Application	USERENV	Severity = error User = System	responsible for application of group policy and profiles on DCs
Application	SCECLI	Severity = error Event ID 1058	Security Configuration Engine error messages

The PATROL KM for Active Directory also monitors other aspects of Group Policy. For more information, see [“Properly Propagating Group Policy Objects” on page 10](#).

Time Synchronization Service Event to Watch

The following event has been determined by Microsoft to be a critical Time Synchronization service event because it indicates problems with maintaining uniform time throughout the Active Directory forest. The predefined AD event filters in the PATROL KM for Windows OS monitor this event.

Event Log	Source	Event	Why Event is Important
System	W32TIME	Severity = error Severity = warning	ensures time synchronization between DCs, and is necessary for Kerberos and resolving replication conflicts

Kerberos Event to Watch

The following event has been determined by Microsoft to be a critical Kerberos event because Kerberos is the default authentication protocol. The predefined AD event filters in the PATROL KM for Windows OS monitor this event.

Event Log	Source	Event	Why Event is Important
System	KDC	Severity = error	critical Kerberos Distribution Center (KDC) service error messages

Netlogon Event to Watch

The following event has been determined by Microsoft to be a critical Netlogon event because it indicates that the Netlogon.chg file is either corrupt or unable to be accessed. This file is required for proper DC functionality. The predefined AD event filters in the PATROL KM for Windows OS monitor this event.

Event Log	Source	Event	Why Event is Important
System	Netlogon	Severity = error 5705, 5723	critical Netlogon service errors

Customized Event Filtering

If the events that you want to monitor are not included in the predefined event filters, the PATROL KM for Windows OS enables you to set up customized event filters so that you can monitor any Windows events that are critical to your environment.

You can configure BMC Performance Manager to monitor Windows events based on the following event properties:

- > type
- > ID
- > source
- > text in the event (string)
- > user
- > category

Whenever an event occurs that matches the filter criteria that you specify, BMC Performance Manager generates a warning or alarm.

To save time, you can also create event filters in the PATROL KM for Windows OS by selecting the events that you want to monitor directly from the Event Viewer in BMC Performance Manager.

ASSURING REPLICATION

Once installed, the PATROL KM for Active Directory instantly begins monitoring the DC on which it is loaded. If there is inter-site replication in your environment, the PATROL KM for Active Directory automatically discovers the configured replication interval. For example, if you have a bridgehead server in San Francisco and a bridgehead server in Singapore with a replication interval of one hour, the PATROL KM for Active Directory automatically detects the one hour replication interval between the two bridgehead servers and adjusts the collection interval for the parameter accordingly. If one bridgehead server is in San Francisco and a second bridgehead server is in Los Angeles and the replication interval is 30 minutes, the KM automatically detects that replication interval and sets the collection intervals accordingly.

The PATROL KM for Active Directory also monitors intra-site replication. The KM checks the replication status of the DC upon which it is installed every 15 minutes by default, then reports whether replication is occurring properly within the site/domain for each replication partner. The KM also determines whether updates from each replication partner within the site have been replicated in a timely manner. Because it monitors replication locally on each domain controller, the PATROL KM for Active Directory generates a minimal amount of network traffic.

Parameters to Watch

To monitor Active Directory replication, watch these parameters:

Event	Application Class	Parameters	Description
Inter-site replication	AD_AD_SERVER	AdIntersiteReplicationStatus	reports whether replication for a particular DC is occurring properly between sites in the domain
Intra-site replication	AD_AD_SERVER	AdIntrasiteReplicationStatus	reports whether replication is occurring properly within site/domain for this DC
		AdIntrasiteReplication-Latency	average replication latency between DCs within site/domain and current DC

Event	Application Class	Parameters	Description
Synchroni- zation	AD_AD_REPLICA- TION	AdRpSyncRequests	number of synchronization requests made since last collection cycle
		AdRpFailedSyncRequests	number of failed synchronization requests made since last collection cycle
		AdRpSuccessSyncRequests	number of synchronization requests successfully made since last collection cycle
		AdRpPendingSyncRepl	number of directory synchronizations that are queued for a particular server but have not yet been processed
Property change transfer	AD_AD_REPLICA- TION	AdRpOutboundProperty- Rate	rate at which property changes replicated since last collection cycle
		AdRpInboundPropertyRate	rate at which property changes are arriving since last collection cycle
Value transfer	AD_AD_REPLICA- TION	AdRpOutboundValueRate	rate at which outbound values have replicated since last collection cycle
		AdRpInboundValueRate	rate at which values have arrived since last collection cycle
Data transfer	AD_AD_REPLICA- TION	AdRpOutboundByteRate	rate at which outbound bytes of data have replicated since last collection cycle
		AdRpInboundByteRate	rate at which bytes of data have arrived since last collection cycle
Object transfer	AD_AD_REPLICA- TION	AdRpOutboundObjectRate	rate at which outbound objects have replicated since last collection cycle
		AdRpInboundObjectRate	rate at which objects have arrived since last collection cycle

SUPPORTING FSMO ROLES

With Active Directory, Microsoft introduced the concept of Flexible Single Master Operations (FSMO). Even with multiple DCs acting as peers, some operations must be handled by a single server in the environment. This means that the FSMO role holders are critical DCs because they can be single points of failure for the entire domain or forest.

For example, if the PDC emulator is down, you may experience difficulties with password authentication. If the RID Master becomes unavailable, DCs will continue to allow the creation of objects (users, policies, shares, and so on), but over time, the RID pools on DCs will completely run out, making it critical to keep your RID Master up and running.

The PATROL KM for Active Directory queries each of the FSMO role holders periodically—with a lightweight ping, or on a less frequent basis, an LDAP bind request—to ensure that these servers are available. The KM checks availability from every DC as there may be a problem with connectivity from one subnet to another that a ping from a central point would not detect. Another event the KM tracks is whether or not a FSMO role has transferred to another server.

Parameters to Watch

To monitor FSMO role-holders, watch these parameters:

Event	Application Class	Parameters	Description
Connection	AD_AD_FSMO_ROLE_CONNECTIVITY	AdFsConnectivity	<p>pings each FSMO role-holder to determine availability</p> <p>Checks LDAP connections less frequently because LDAP connections use a greater amount of server resources.</p>
Role transfer	AD_AD_FSMO_ROLE_CONNECTIVITY	AdFsRoleChanged	detects and reports when a FSMO role is moved to or from a particular DC

PROPERLY PROPAGATING GROUP POLICY OBJECTS

Group Policy information is stored in two different areas:

- > Group Policy containers — stored within Active Directory
- > Group Policy templates — stored in the Sysvol folder, a shared folder in the DC's file system

Sysvol must be shared for group policy to be replicated and applied to DCs and other objects. To ensure that GPOs are propagating properly among DCs, the PATROL KM for Active Directory monitors both Active Directory replication (see [“Assuring Replication” on page 7](#) for details) and the availability of the Sysvol share.

Parameter to Watch

To monitor GPO propagation, watch this parameter:

Event	Application Class	Parameters	Description
Sysvol sharing	AD_AD_SERVER	AdSysvolShared	reports whether Sysvol is shared

The PATROL KM for Active Directory event filters also monitor events related to Group Policy and FRS. For more information, see [“File Replication Service and Group Policy Events to Watch” on page 5](#).

ENSURING RAPID ACTIVE DIRECTORY RESPONSE TIME

End-user response time results from a combination of the response times of various services, processes, and database queries within Active Directory. All of these response times should be monitored individually so that if one fails it can be quickly identified. The most common cause of poor response times is overloaded DCs.

If you are experiencing poor Active Directory response times, the best place to start is by monitoring the response time of the Lightweight Directory Access Protocol (LDAP), as this is the most commonly used service in Active Directory. The PATROL KM for Active Directory monitors the performance of LDAP activity on the Active Directory server, in addition to the performance of other Active Directory services, processes, and queries.

Parameters to Watch

To monitor the various response times within Active Directory, watch the following parameters:

Event	Application Class	Parameters	Description
LDAP binds	AD_AD_LDAP	AdLdResponseTime	reports amount of time required to issue an LDAP bind operation
		AdLdBindRate	rate of successful LDAP binds
LDAP writes	AD_AD_LDAP	AdLdWriteRate	rate at which LDAP clients perform write operations
LDAP searches	AD_AD_LDAP	AdLdSearchRate	rate at which LDAP clients perform search operations
Object transfer	AD_AD_REPLICATION	AdRpOutboundObjectRate	rate at which objects that need to be added to other Active Directory servers have left current Active Directory server since last collection cycle
		AdRpInboundObjectRate	rate at which objects are arriving that need to be added to current Active Directory Server
Property change transfer	AD_AD_REPLICATION	AdRpOutboundPropertyRate	rate at which property changes have left Active Directory server since last collection cycle
		AdRpInboundPropertyRate	rate at which property changes are arriving at Active Directory server
Value transfer	AD_AD_REPLICATION	AdRpOutboundValueRate	rate that values are leaving Active Directory server
		AdRpInboundValueRate	rate at which values are arriving at Active Directory server

KEEPING UP WITH DOMAIN NAMING SERVICE DEMANDS

You cannot use Active Directory successfully without DNS. The DNS provides a marked improvement over the WINS used in Windows NT environments. In the event you may use a non-Microsoft DNS server, make sure that when you create a new site that you use a legal DNS name as your site name.

To prevent a forest-wide Active Directory outage due to the outage of one DNS server, make sure you have multiple DNS servers in your environment. Having at least one DNS server per site, keeps name resolution performance an optimum level.

Many access problems in Active Directory stem from a faulty DNS server or configuration. To make sure that your DNS servers are not overloaded, use the PATROL KM for Domain Services to monitor DNS response time and the rate at which the server receives update requests. If response time degrades, it might be an indication that you should add another DNS server to the site.

Parameters to Watch

To monitor DNS metrics, watch these parameters in the PATROL KM for Domain Services:

Event	Application Class	Parameters	Description
Dynamic update	NT_DNS_2000	DnDynUpdateQueuedRate	rate at which dynamic updates are being queued by DNS server
		DnDynUpdateRecvRate	rate at which dynamic updates are being received at DNS server
		DnDynUpdateRejectRate	rate at which dynamic updates are being rejected by DNS server
		DnDynUpdateTimeoutRate	rate at which dynamic updates are failing due to timeout
		DnDynUpdateWriteRate	rate at which dynamic updates are written to DNS database

Event	Application Class	Parameters	Description
DNS events	NT_DNS_2000	DnEvtLogErrorCount	number of DNS-related error events that have occurred in Windows event log since last collection cycle
		DnEvtLogInfoCount	number of DNS-related information events that have occurred in Windows event log since last collection cycle
		DnEvtLogWarningCount	number of DNS-related warning events that have occurred in Windows event log since last collection cycle
DNS query	NT_DNS_2000	DnQueryFailureRate	number of failed queries per minute
		DnQueryRate	average number of queries received per minute
		DnQueryResponseTime	number of milliseconds DNS server takes to process a sample request
		DnQuerySuccessRate	number of successful queries per minute
Secure update	NT_DNS_2000	DnSecUpdateFailRate	rate at which secure updates are failing on DNS database
		DnSecUpdateRecvRate	rate at which secure updates are being received by DNS server
DNS running	NT_DNS_2000	DnServiceStatus	monitors whether DNS service is running
WINS query	NT_DNS_2000	DnWinsLookupRate	rate at which WINS queries are being received at DNS server
		DnWinsReverseLookupRate	rate at which DNS server receives reverse lookup WINS queries
		DnWinsResponseRate	rate at which DNS server processes responses to WINS queries
		DnWinsReverseResponseRate	rate at which DNS server processes WINS reverse lookup queries

CONTROLLING DC HEALTH

The operating system is the primary factor impacting DC performance. The PATROL KM for Active Directory in conjunction with the PATROL KM for Windows OS monitors CPU, memory utilization, and disk space consumed by Active Directory. Of these statistics, the most critical is disk space.

Because each DC stores a copy of the Active Directory database, the database must be available for the DC to function. You should monitor the file system periodically because as more objects are added to Active Directory, the database size increases. If the database size becomes too large, you may need to defragment the database or extend the partition.

Active Directory also depends on many other Windows services. For example, if Netlogon is down, the DC would not be able to accept logon requests. For a description of Windows services monitored by the PATROL KM for Active Directory event filters, see [“Making Event Logs Easy” on page 4](#).

Parameters to Watch

To monitor DC health, watch these parameters:

Statistic	KM	Application Class	Parameters	Description
Disk space consumed by AD database	PATROL KM for Active Directory	AD_AD_SERVER	AdDiskSpaceUsed	amount of disk space used by Active Directory data repository
			AdDiskSpaceAvailable	disk space available on current volume that hosts Active Directory data repository
Memory	PATROL KM for Windows OS	NT_HEALTH	MemoryUsage	percentage of memory in use
System disk usage	PATROL KM for Windows OS	NT_HEALTH	DiskUsage	cumulative percent usage of system disks
CPU utilization	PATROL KM for Windows OS	NT_HEALTH	ProcessorUtilization	overall CPU utilization for server

TRACKING TRUST RELATIONSHIPS

Active Directory uses trust relationships to allow members of one domain to authenticate with another domain without requiring a duplicate domain account in the second domain. Active Directory automatically generates transitive trust relationships between domains within the same forest. Use the PATROL KM for Domain Services to monitor the trust relationships in your forest to ensure that they are always available.

Parameters to Watch

To monitor trust relationships, watch these parameters:

Event/Object	Application Class	Parameter	Description
Trust validation	NT_TRUST	TrRelationshipStatus	validates that trust relationship is available
Trust response	NT_TRUST	TrResponseTime	measures connection response time to trusting domains

Reference

Solution Operations Guide, Microsoft Corp. 2002

Helping You Maintain Advantage

BMC Software Education Services offers a strategic investment for your business, maximizing the value for your employees and Business Service Management initiatives. Education ensures successful product implementation, promoting mastery of all product capabilities and highest productivity with your BMC Software solutions.

To explore our education offerings, visit our web page at <http://www.bmc.com/bmceducation>, or contact BMC Software Education Services by telephone or e-mail:

- > **North America**
Telephone: 800 574 4262
E-mail: education@bmc.com
- > **Asia Pacific**
Telephone: +61 3 9657 4404
E-mail: ISD_AP@bmc.com
- > **Europe, Middle East, and Africa (EMEA)**
Telephone: 00800 26233822
E-mail: emea_education@bmc.com



About BMC Software

BMC Software, Inc. [NYSE:BMC], is a leading provider of enterprise management solutions that empower companies to manage their IT infrastructure from a business perspective. Delivering Business Service Management, BMC Software solutions span enterprise systems, applications, databases, and service management. Founded in 1980, BMC Software has offices worldwide and fiscal 2004 revenues of more than \$1.4 billion. For more information about BMC Software, visit www.bmc.com.



56819