Monitoring Active Directory Using OpManager

Active Directory is Microsoft's implementation of LDAP directory services for Windows environments. It allows administrators to implement company wide policies on access to resources and services by the users. Active Directory is usually installed in Windows 2003 or 2000 server and together they are called the Domain Controllers. If active directory fails, it would affect the entire user base, as they won't be able to logon to their systems, access critical information from other servers, or send/receive emails.

In this section lets see how a Network Monitoring Tool such as OpManager can help administrators prevent Active Directory nightmares!

A Sample Active Directory Nightmare

Imagine a scenario where your CEO logs into his laptop and it says *access denied*. Probably he just forgot to release the CAPS LOCK key (you are saved) or the *Kerberos Key Distribution Center Service* that plays a vital role in user authentication has stopped functioning and is forcing every Windows user from logging into the domain (you are in trouble). There is no way your CEO could imagine that a simple service running at a server in an isolated room could stop him from working. All that everybody wants is uninterrupted network access.

Most of the IT helpdesk tickets originate from issues spawning from users trying to access resources outside one's computer. Active directory forms the crux of this ever-active access system. For instance common operations such as user authentication, exchange mail routing, depend on Active Directory. This makes continuous monitoring of Active Directory and related services very important – so that you may also stay away from nasty nightmare!

What should you monitor in active directory?

There are a little over half-a-dozen Active Directory components that can cause an access problem to a user. Few important factors that you need to monitor on AD are:

- System Resources Availability
- Responsiveness of LDAP
- Availability of DNS Client Service
- Availability of Kerberos Key Distribution Center Service
- Availability of Net Log On Service
- Health of File Replication Service (FRS)

System Resources Availability: Hardware failures, insufficient disk space etc., are common problems causing a server to crash. Requests to the Active Directory need to be served fast. This requires the CPU, Memory, and Disk Space of the server that hosts Active Directory to be running at optimal levels and monitored 24*7.

Responsiveness of LDAP: LDAP is the client used to retrieve directory information. Monitoring LDAP parameters like LDAP Bind Time, number of Active Connections, LDAP Searches, and LDAP Writes is a proactive step in ensuring its availability.

Availability of DNS Client Service: DNS lookup failure can cause problems. The Domain Controller might not have been able to register DNS records, which actually vouches for the Domain Controllers availability. This results in the other Domain Controllers, users, and computers in the domain in not locating this DC which again might lead to replication failure. Refer this article for troubleshooting AD related DNS problems.

Availability of Kerberos Key Distribution Center Service: Active Directory depends on this service for authentication. Failure of this service leads to log-on failures. Refer this article to know how this service works.

Availability of Net Log On Service: Request to authenticate users is served by this service. Failure of this service also makes the log-on impossible. The Domain Controller will not be able

to accept log-on requests if this service is not available.

Health of File Replication Service (FRS): FRS service replicates the objects in Active Directory among all the Domain Controllers in a network (if you have more than one domain controller). This is done to ensure round-the-clock accessibility to the information on the AD. This can be across the LAN or the WAN. When the FRS fails, the objects are not replicated on the other Domain Controllers. In the event of the primary DC failing, when the secondary (the slave) takes over the request, it will not have the user account replicated. This will cause the log-on failure. The replication failure can also occur because of incorrect DNS configuration.

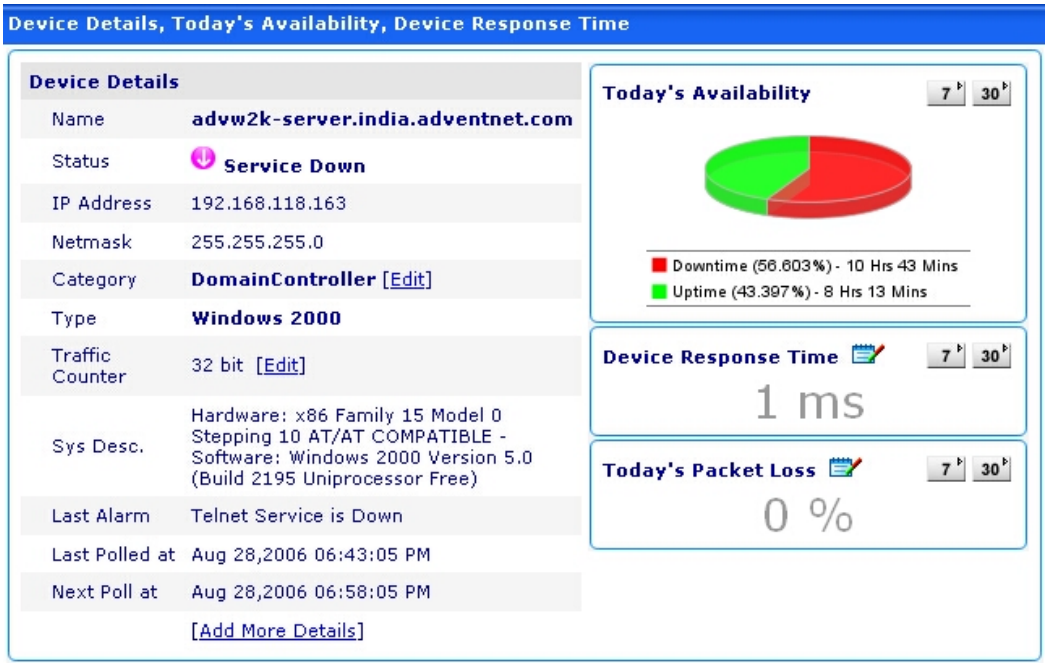
Miscellaneous: There can be other reasons like no network connectivity, too many applications accessing the DC at a time etc.

Active Directory monitoring with OpManager

OpManager monitors all the services and resources on which Active Directory relies for proper functioning. You can configure thresholds and get instantly notified if something is crossing safe limits.

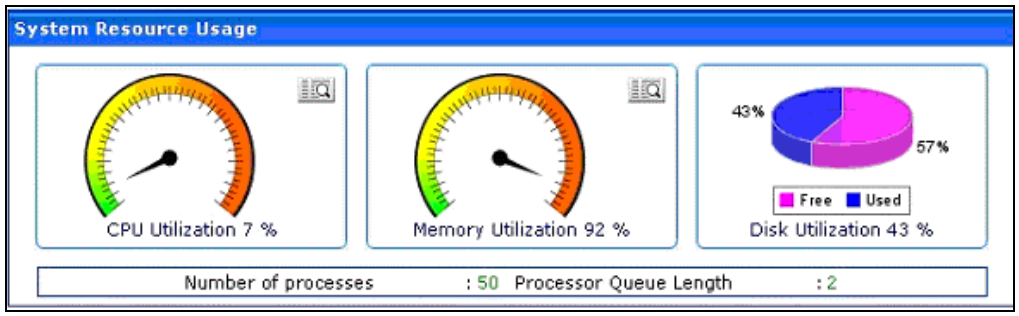
Monitor domain controller's availability

OpManager offers a dashboard view of your domain controller's availability with options to see availability statistics for the past week, month etc.



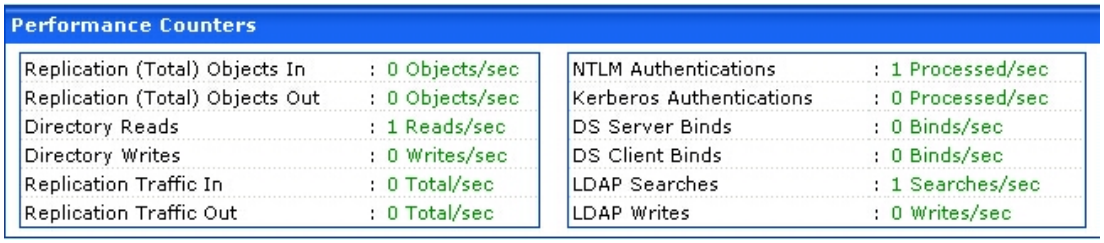
Monitor domain controller's health

System resources usage gives you real-time status of the health of your domain controller. Details such as CPU utilization, Memory utilization, and disc utilization can be viewed from here.



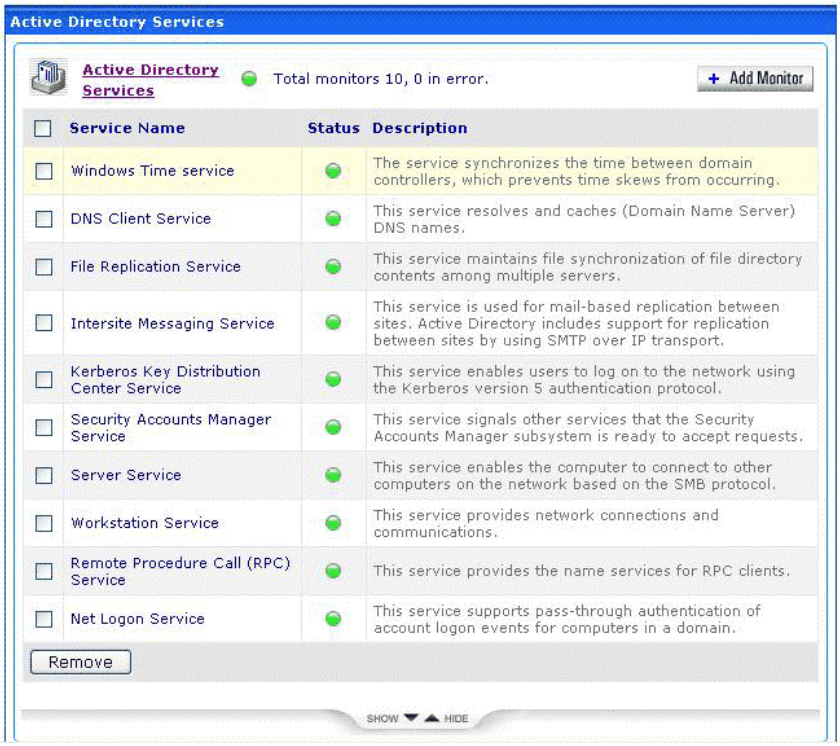
Monitor the performance counters

Active directory performance counters such as directory reads, directory writes, Kerberos authentications etc can be viewed from here.



Monitor the Active Directory services

Key active directory services such as Windows Time Service, DNS Client Service, File Replication Service, Inter-site Messaging Service, Kerberos Key Distribution Center Service, Security Accounts Manager Service, Server Service Workstation Service, RPC Service, and Net Logon Service.



Complete list of active directory parameters monitored by OpManager

Here's a tree view of the entire set of parameters monitored by OpManager to ensure that your Active Directory doesn't popup unlikely surprises.

- Availability
  - Availability
  - Response time
  - Packet loss
- Resources
  - CPU
  - Memory
  - Disc
- AD services
  - Windows Time Service
  - DNS Client Service
  - File Replication Service
  - Intersite Messaging Service
  - Kerberos Key Distribution Center Service
  - Security Accounts Manager Service
  - Server Service
  - Workstation Service
  - RPC Service
  - Net Logon Service
- AD Network parameters
  - AB Client Sessions

    - DS Notify Queue Size
    - LDAP Active Threads
    - LDAP Bind Time
    - LDAP Client Sessions
    - Number of Clients
- AD Database parameters
    - Database Free Space
    - Database Size
    - Database Total Size
    - Replication Objects Applied
    - Replication Objects Remaining
- AD Process Monitors
    - LSASS / NTFRS CPU Usage
    - LSASS / NTFRS Handle Count
    - LSASS / NTFRS Process File Reads
    - LSASS / NTFRS Process File Writes
    - LSASS / NTFRS Process Memory
- AD performance counters
    - DS Client Binds
    - DS Server Binds
    - Directory Reads
    - Directory Writes
    - Kerberos Authentications
    - LDAP Searches
    - LDAP UDP Operations
    - LDAP Writes
    - NTLM Authentications
    - Replication (Total) Objects In
    - Replication (Total) Objects Out
    - Replication Traffic In
    - Replication Traffic Out

Monitoring active directory using event logs

Active Directory writes detailed event logs during failure. You can view event logs from your Windows Event Viewer (start - settings - control panel- administrative tools - event viewer). Each active directory component failure has a pre-defined event ID with a detailed message for the failure event. OpManager allows monitoring these windows event logs using pre-defined event log rules. OpManager monitors the event logs and based on the rule it generates OpManager alarms.

Event Logs Monitoring for the Domain Controllers is configured as follows:

- Click 'Event Log Rules' on the right in the DC's snapshot page
- Scroll down to 'File Replication Service' and 'Directory Service' sections and select the rules for the failures for which you want to be notified. The selected rules will be associated to the devices.

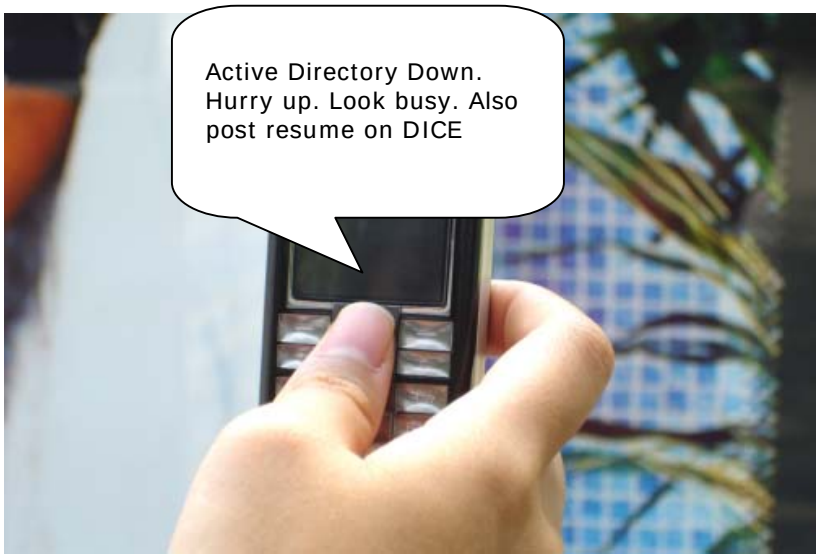
Besides receiving alarms for the default rules, you can configure new rules for the required Windows Event IDs.

Here are some IDs for which you might want OpManager to raise an alarm. *(Please note that this is only a subset of a whole lot of Windows Event Logs for various services and parameters related to Active Directory.)*

Service	Event ID
Net Logon Service	5774, 5775, 5781, 5783, 5805
FRS Service	13508, 13509, 13511, 13522, 13526
Windows Time Service	13,14, 52 to 56, 60 to 64
LDAP related	40960, 40961
LSASS related	1000, 1015
Kerberos related	675, 676, 1002, 1005, 9004 (last three are related to Exchange server)
NTLM authentication	680, 681

Instant notification from OpManager

Besides monitoring the Active Directory components, OpManager raises alarms when a service is unavailable. Configuring response time or resource utilization thresholds for the critical services and parameters alerts you much ahead of the actual problem. OpManager allows you to create and assign notification profiles to Domain Controllers. When any of the monitors fail, an email or SMS alert is sent to the pre-configured Ids.



Summary

OpManager offers excellent Active Directory monitoring capabilities and helps you stay away from Active Directory nightmares. To test drive active directory monitoring download the latest OpManager build from www.opmanager.com.