Output.conf

[tcpout]

defaultGroup = default-autolb-group

[tcpout:default-autolb-group]

server = 192.168.1.140:9997

[tcpout-server://192.168.1.140:9997]

192.168.1.140 is the splunk server ip adress

inputs splunk TA_windows

[perfmon://CPU]

counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec

disabled = 1

instances = *

interval = 10

mode = single

object = Processor

useEnglishOnly=true

Logical Disk

[perfmon://LogicalDisk]

counters = % Free Space; Free Megabytes; Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk

Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec

disabled = 1

instances = *

interval = 10

mode = single

object = LogicalDisk

useEnglishOnly=true

Physical Disk

[perfmon://PhysicalDisk]

counters = Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec

disabled = 1

instances = *

interval = 10

mode = single

object = PhysicalDisk

useEnglishOnly=true

Memory

[perfmon://Memory]

counters = Page Faults/sec; Available Bytes; Committed Bytes; Commit Limit; Write Copies/sec; Transition Faults/sec; Cache Faults/sec; Demand Zero Faults/sec; Pages/sec; Pages Input/sec; Page Reads/sec; Pages Output/sec; Pool Paged Bytes; Pool Nonpaged Bytes; Page Writes/sec; Pool Paged Allocs; Pool Nonpaged Allocs; Free System Page Table Entries; Cache Bytes; Cache Bytes Peak; Pool Paged Resident Bytes; System Code Total Bytes; System Code Resident Bytes; System Driver Total Bytes; System Driver Resident Bytes; System Cache Resident Bytes; % Committed Bytes In Use; Available KBytes; Available MBytes; Transition Pages RePurposed/sec; Free & Zero Page List Bytes; Modified Page List Bytes; Standby Cache Reserve Bytes; Standby Cache Normal Priority Bytes; Standby Cache Core Bytes; Long-Term Average Standby Cache Lifetime (s)

disabled = 1

interval = 10

mode = single

object = Memory

useEnglishOnly=true

Network

[perfmon://Network]

counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets Sent/sec; Current Bandwidth; Bytes Received/sec; Packets Received Unicast/sec; Packets Received Non-Unicast/sec; Packets Received Discarded; Packets Received Errors; Packets Received Unknown; Bytes Sent/sec; Packets Sent Unicast/sec; Packets Sent Non-Unicast/sec; Packets Outbound Discarded; Packets Outbound Errors; Output Queue Length; Offloaded Connections; TCP Active RSC Connections; TCP RSC Coalesced Packets/sec; TCP RSC Exceptions/sec; TCP RSC Average Packet Size

disabled = 1

instances = *

interval = 10

mode = single

object = Network Interface

useEnglishOnly=true

Process

[perfmon://Process]

counters = % Processor Time; % User Time; % Privileged Time; Virtual Bytes Peak; Virtual Bytes; Page Faults/sec; Working Set Peak; Working Set; Page File Bytes Peak; Page File Bytes; Private Bytes; Thread Count; Priority Base; Elapsed Time; ID Process; Creating Process ID; Pool Paged Bytes; Pool Nonpaged Bytes; Handle Count; IO Read Operations/sec; IO Write Operations/sec; IO Data Operations/sec; IO Other Operations/sec; IO Read Bytes/sec; IO Write Bytes/sec; IO Data Bytes/sec; IO Other Bytes/sec; Working Set - Private

disabled = 1

instances = *

interval = 10

mode = single

object = Process

useEnglishOnly=true

ProcessInformation

[perfmon://ProcessorInformation]

counters = % Processor Time; Processor Frequency

disabled = 1

instances = *

interval = 10

mode = single

object = Processor Information

useEnglishOnly=true

System

[perfmon://System]

counters = File Read Operations/sec; File Write Operations/sec; File Control Operations/sec; File Read Bytes/sec; File Write Bytes/sec; File Control Bytes/sec; Context Switches/sec; System Calls/sec; File Data Operations/sec; System Up Time; Processor Queue Length; Processes; Threads; Alignment Fixups/sec; Exception Dispatches/sec; Floating Emulations/sec; % Registry Quota In Use

disabled = 1

instances = *

interval = 10

mode = single

object = System

useEnglishOnly=true

[perfmon://Processor]

object = Processor

counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec

instances = *

interval = 10

disabled = 1

mode = single

useEnglishOnly=true

index = perfmon

[perfmon://Network_Interface]

object = Network Interface

counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets Sent/sec; Current Bandwidth; Bytes Received/sec; Packets Received Unicast/sec; Packets Received Non-Unicast/sec; Packets Received Discarded; Packets Received Errors; Packets Received Unknown; Bytes Sent/sec; Packets Sent Unicast/sec; Packets Sent Non-Unicast/sec; Packets Outbound Discarded; Packets Outbound Errors; Output Queue Length; Offloaded Connections; TCP Active RSC Connections; TCP RSC Coalesced Packets/sec; TCP RSC Exceptions/sec; TCP RSC Average Packet Size

instances = *

interval = 10

disabled = 1

mode = single

useEnglishOnly=true

index = perfmon

[perfmon://DFS_Replicated_Folders]

object = DFS Replicated Folders

counters = Bandwidth Savings Using DFS Replication; RDC Bytes Received; RDC Compressed Size of Files Received; RDC Size of Files Received; RDC Number of Files Received; Compressed Size of Files Received; Size of Files Received; Total Files Received; Deleted Space In Use; Deleted Bytes Cleaned up; Deleted Files Cleaned up; Deleted Bytes Generated; Deleted Files Generated; Updates Dropped; File Installs Retried; File Installs Succeeded; Conflict Folder Cleanups Completed; Conflict Space In Use; Conflict Bytes Cleaned up; Conflict Files Cleaned up; Conflict Bytes Generated; Conflict Files Generated; Staging Space In Use; Staging Bytes Cleaned up; Staging Files Cleaned up; Staging Bytes Generated; Staging Files Generated

instances = *

interval = 30

disabled = 1

mode = single

useEnglishOnly=true

index = perfmon

[perfmon://NTDS]

object = NTDS

counters = DRA Inbound Properties Total/sec; AB Browses/sec; DRA Inbound Objects Applied/sec; DS Threads in Use; AB Client Sessions; DRA Pending Replication Synchronizations; DRA Inbound Object Updates Remaining in Packet; DS Security Descriptor sub-operations/sec; DS Security Descriptor Propagations Events; LDAP Client Sessions; LDAP Active Threads; LDAP Writes/sec; LDAP Searches/sec; DRA Outbound Objects/sec; DRA Outbound Properties/sec; DRA Inbound Values Total/sec; DRA Sync Requests Made; DRA Sync Requests Successful; DRA Sync Failures on

Schema Mismatch; DRA Inbound Objects/sec; DRA Inbound Properties Applied/sec; DRA Inbound Properties Filtered/sec; DS Monitor List Size; DS Notify Queue Size; LDAP UDP operations/sec; DS Search sub-operations/sec; DS Name Cache hit rate; DRA Highest USN Issued (Low part); DRA Highest USN Issued (High part); DRA Highest USN Committed (Low part); DRA Highest USN Committed (High part); DS % Writes from SAM; DS % Writes from DRA; DS % Writes from LDAP; DS % Writes from LSA; DS % Writes from KCC; DS % Writes from NSPI; DS % Writes Other; DS Directory Writes/sec; DS % Searches from SAM; DS % Searches from DRA; DS % Searches from LDAP; DS % Searches from LSA; DS % Searches from KCC; DS % Searches from NSPI; DS % Searches Other; DS Directory Searches/sec; DS % Reads from SAM; DS % Reads from DRA; DRA Inbound Values (DNs only)/sec; DRA Inbound Objects Filtered/sec; DS % Reads from LSA; DS % Reads from KCC; DS % Reads from NSPI; DS % Reads Other; DS Directory Reads/sec; LDAP Successful Binds/sec; LDAP Bind Time; SAM Successful Computer Creations/sec: Includes all requests; SAM Machine Creation Attempts/sec; SAM Successful User Creations/sec; SAM User Creation Attempts/sec; SAM Password Changes/sec; SAM Membership Changes/sec; SAM Display Information Queries/sec; SAM Enumerations/sec; SAM Transitive Membership Evaluations/sec; SAM Non-Transitive Membership Evaluations/sec; SAM Domain Local Group Membership Evaluations/sec; SAM Universal Group Membership Evaluations/sec; SAM Global Group Membership Evaluations/sec; SAM GC Evaluations/sec; DRA Inbound Full Sync Objects Remaining; DRA Inbound Bytes Total/sec; DRA Inbound Bytes Not Compressed (Within Site)/sec; DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec; DRA Inbound Bytes Compressed (Between Sites, After Compression)/sec; DRA Outbound Bytes Total/sec; DRA Outbound Bytes Not Compressed (Within Site)/sec; DRA Outbound Bytes Compressed (Between Sites, Before Compression)/sec; DRA Outbound Bytes Compressed (Between Sites, After Compression)/sec; DS Client Binds/sec; DS Server Binds/sec; DS Client Name Translations/sec; DS Server Name Translations/sec; DS Security Descriptor Propagator Runtime Queue; DS Security Descriptor Propagator Average Exclusion Time; DRA Outbound Objects Filtered/sec; DRA Outbound Values Total/sec; DRA Outbound Values (DNs only)/sec; AB ANR/sec; AB Property Reads/sec; AB Searches/sec; AB Matches/sec; AB Proxy Lookups/sec; ATQ Threads Total; ATQ Threads LDAP; ATQ Threads Other; DRA Inbound Bytes Total Since Boot; DRA Inbound Bytes Not Compressed (Within Site) Since Boot; DRA Inbound Bytes Compressed (Between Sites, Before Compression) Since Boot; DRA Inbound Bytes Compressed (Between Sites, After Compression) Since Boot; DRA Outbound Bytes Total Since Boot; DRA Outbound Bytes Not Compressed (Within Site) Since Boot; DRA Outbound Bytes Compressed (Between Sites, Before Compression) Since Boot; DRA Outbound Bytes Compressed (Between Sites, After Compression) Since Boot; LDAP New Connections/sec; LDAP Closed Connections/sec; LDAP New SSL Connections/sec; DRA Pending Replication Operations; DRA Threads Getting NC Changes; DRA Threads Getting NC Changes Holding Semaphore; DRA Inbound Link Value Updates Remaining in Packet; DRA Inbound Total Updates Remaining in Packet; DS % Writes from NTDSAPI; DS % Searches from NTDSAPI; DS % Reads from NTDSAPI; SAM Account Group Evaluation Latency; SAM Resource Group Evaluation Latency; ATQ Outstanding Queued Requests; ATQ Request Latency; ATQ Estimated Queue Delay; Tombstones Garbage Collected/sec; Phantoms Cleaned/sec; Link Values Cleaned/sec; Tombstones Visited/sec; Phantoms Visited/sec; NTLM Binds/sec; Negotiated Binds/sec; Digest Binds/sec; Simple Binds/sec; External Binds/sec; Fast Binds/sec; Base searches/sec; Subtree searches/sec; Onelevel searches/sec; Database adds/sec; Database modifys/sec; Database deletes/sec; Database recycles/sec; Approximate highest DNT; Transitive operations/sec; Transitive suboperations/sec; Transitive operations milliseconds run

interval = 10

disabled = 1

mode = single

useEnglishOnly=true

index = perfmon

[perfmon://DNS]

object = DNS

counters = Total Query Received; Total Query Received/sec; UDP Query Received; UDP Query Received/sec; TCP Query Received; TCP Query Received/sec; Total Response Sent; Total Response Sent/sec; UDP Response Sent; UDP Response Sent/sec; TCP Response Sent; TCP Response Sent/sec; Recursive Queries; Recursive Queries/sec; Recursive Send TimeOuts; Recursive TimeOut/sec; Recursive Query Failure; Recursive Query Failure/sec; Notify Sent; Zone Transfer Request Received; Zone Transfer Success; Zone Transfer Failure; AXFR Request Received; AXFR Success Sent; IXFR Request Received; IXFR Success Sent; Notify Received; Zone Transfer SOA Request Sent; AXFR Request Sent; AXFR Response Received; AXFR Success Received; IXFR Request Sent; IXFR Response Received; IXFR Success Received; IXFR UDP Success Received; IXFR TCP Success Received; WINS Lookup Received; WINS Lookup Received/sec; WINS Response Sent; WINS Response Sent/sec; WINS Reverse Lookup Received; WINS Reverse Lookup Received/sec; WINS Reverse Response Sent; WINS Reverse Response Sent/sec; Dynamic Update Received; Dynamic Update Received/sec; Dynamic Update NoOperation; Dynamic Update NoOperation/sec; Dynamic Update Written to Database; Dynamic Update Written to Database/sec; Dynamic Update Rejected; Dynamic Update TimeOuts; Dynamic Update Queued; Secure Update Received; Secure Update Received/sec; Secure Update Failure; Database Node Memory; Record Flow Memory; Caching Memory; UDP Message Memory; TCP Message Memory; Nbstat Memory; Unmatched Responses Received

interval = 10

disabled = 1

mode = single

useEnglishOnly=true

index = perfmon

[WinEventLog://Security]

disabled = 0

start_from oldest

current_only = 0

evt_resolve_ad_obj = 1

checkpoint Interval = 5

whitelist =

4724,4725,4726,4624,4625,4720,4732,4722,4738,4742,4729,4715, 4719

blacklist1 = EventCode="4662" Message="Object Type: (?!

\s*group Policy Container)"

blacklist2 = EventCode="566" Message="Object Type: (?!

\s*group PolicyContainer)"

renderXml=true

[WinEventLog://Microsoft-windows-Terminalservices-

LocalSessionManager/operational]

disabled = 0

index = rdp_localsessionmanager

sourcetype = rdp_localsessionmanager

inputs splunk_TA_windows_AD

###

Windows Event Logs

###

Application, System and Security logs are handled

by Splunk_TA_windows and should be compatible with

what we need

###

#

Application and Services Logs - DFS Replication

#

[WinEventLog://DFS Replication]

disabled=0

sourcetype=WinEventLog:DFS-Replication

index=wineventlog

queue=parsingQueue

```
#
# Application and Services Logs - Directory Service
#
[WinEventLog://Directory Service]
disabled=0
sourcetype=WinEventLog:Directory-Service
index=wineventlog
queue=parsingQueue

#
# Application and Services Logs - File Replication Service
#
[WinEventLog://File Replication Service]
disabled=0
sourcetype=WinEventLog:File-Replication-Service
index=wineventlog
queue=parsingQueue

#
# Application and Services Logs - Key Management Service
#
[WinEventLog://Key Management Service]
disabled=0
sourcetype=WinEventLog:Key-Management-Service
index=wineventlog
queue=parsingQueue

#
# Collect Replication Information NT6
#
[script://.\bin\runpowershell.cmd nt6-repl-stat.ps1]
```

source=Powershell

sourcetype=MSAD:NT6:Replication

interval=300

index=msad

disabled=0

#

Collect Replication Information 2012r2

#

[powershell://Replication-Stats]

script = & "$SplunkHome\etc\apps\Splunk_TA_microsoft_ad\bin\Invoke-MonitoredScript.ps1" -Command ".\powershell\2012r2-repl-stats.ps1"

schedule = 0 */5 * ? * *

index = msad

source = Powershell

sourcetype=MSAD:NT6:Replication

disabled=0

#

Collect Health and Topology Information NT6

#

[script://.\bin\runpowershell.cmd nt6-health.ps1]

source=Powershell

sourcetype=MSAD:NT6:Health

interval=300

index=msad

disabled=0

#

Collect Health and Topology Information 2012r2

#

[powershell://AD-Health]

```
script = & "$SplunkHome\etc\apps\Splunk_TA_microsoft_ad\bin\Invoke-MonitoredScript.ps1" -Command ".\powershell\2012r2-health.ps1"

schedule = 0 */5 * ? * *

index = msad

source=Powershell

sourcetype=MSAD:NT6:Health

disabled=0



#

# Collect Site, Site Link and Subnet Information NT6

#

[script://.\bin\runpowershell.cmd nt6-siteinfo.ps1]

source=Powershell

sourcetype=MSAD:NT6:SiteInfo

interval=3600

index=msad

disabled=0


#

# Collect Site, Site Link and Subnet Information 2012r2

#

[powershell://Siteinfo]

script = & "$SplunkHome\etc\apps\Splunk_TA_microsoft_ad\bin\Invoke-MonitoredScript.ps1" -Command ".\powershell\2012r2-siteinfo.ps1"

schedule = 0 15 * ? * *

index = msad

source = Powershell

sourcetype=MSAD:NT6:SiteInfo

disabled=0


#

# Perfmon Collection
```

#

[perfmon://Processor]

object = Processor

counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec

instances = *

interval = 10

disabled = 0

index=perfmon

useEnglishOnly=true

[perfmon://Memory]

object = Memory

counters = Page Faults/sec; Available Bytes; Committed Bytes; Commit Limit; Write Copies/sec; Transition Faults/sec; Cache Faults/sec; Demand Zero Faults/sec; Pages/sec; Pages Input/sec; Page Reads/sec; Pages Output/sec; Pool Paged Bytes; Pool Nonpaged Bytes; Page Writes/sec; Pool Paged Allocs; Pool Nonpaged Allocs; Free System Page Table Entries; Cache Bytes; Cache Bytes Peak; Pool Paged Resident Bytes; System Code Total Bytes; System Code Resident Bytes; System Driver Total Bytes; System Driver Resident Bytes; System Cache Resident Bytes; % Committed Bytes In Use; Available KBytes; Available MBytes; Transition Pages RePurposed/sec; Free & Zero Page List Bytes; Modified Page List Bytes; Standby Cache Reserve Bytes; Standby Cache Normal Priority Bytes; Standby Cache Core Bytes; Long-Term Average Standby Cache Lifetime (s)

interval = 10

disabled = 0

index=perfmon

useEnglishOnly=true

[perfmon://Network_Interface]

object = Network Interface

counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets Sent/sec; Current Bandwidth; Bytes Received/sec; Packets Received Unicast/sec; Packets Received Non-Unicast/sec; Packets Received Discarded; Packets Received Errors; Packets Received Unknown; Bytes Sent/sec; Packets Sent Unicast/sec; Packets Sent Non-Unicast/sec; Packets Outbound Discarded; Packets Outbound Errors; Output Queue Length; Offloaded Connections; TCP Active RSC Connections; TCP RSC Coalesced Packets/sec; TCP RSC Exceptions/sec; TCP RSC Average Packet Size

instances = *

interval = 10

disabled = 0

index=perfmon

useEnglishOnly=true

[perfmon://DFS_Replicated_Folders]

object = DFS Replicated Folders

counters = Bandwidth Savings Using DFS Replication; RDC Bytes Received; RDC Compressed Size of Files Received; RDC Size of Files Received; RDC Number of Files Received; Compressed Size of Files Received; Size of Files Received; Total Files Received; Deleted Space In Use; Deleted Bytes Cleaned up; Deleted Files Cleaned up; Deleted Bytes Generated; Deleted Files Generated; Updates Dropped; File Installs Retried; File Installs Succeeded; Conflict Folder Cleanups Completed; Conflict Space In Use; Conflict Bytes Cleaned up; Conflict Files Cleaned up; Conflict Bytes Generated; Conflict Files Generated; Staging Space In Use; Staging Bytes Cleaned up; Staging Files Cleaned up; Staging Bytes Generated; Staging Files Generated

instances = *

interval = 30

disabled = 0

index=perfmon

useEnglishOnly=true

[perfmon://NTDS]

object = NTDS

counters = DRA Inbound Properties Total/sec; AB Browses/sec; DRA Inbound Objects Applied/sec; DS Threads in Use; AB Client Sessions; DRA Pending Replication Synchronizations; DRA Inbound Object Updates Remaining in Packet; DS Security Descriptor sub-operations/sec; DS Security Descriptor Propagations Events; LDAP Client Sessions; LDAP Active Threads; LDAP Writes/sec; LDAP Searches/sec; DRA Outbound Objects/sec; DRA Outbound Properties/sec; DRA Inbound Values Total/sec; DRA Sync Requests Made; DRA Sync Requests Successful; DRA Sync Failures on Schema Mismatch; DRA Inbound Objects/sec; DRA Inbound Properties Applied/sec; DRA Inbound Properties Filtered/sec; DS Monitor List Size; DS Notify Queue Size; LDAP UDP operations/sec; DS Search sub-operations/sec; DS Name Cache hit rate; DRA Highest USN Issued (Low part); DRA Highest USN Issued (High part); DRA Highest USN Committed (Low part); DRA Highest USN Committed (High part); DS % Writes from SAM; DS % Writes from DRA; DS % Writes from LDAP; DS % Writes from LSA; DS % Writes from KCC; DS % Writes from NSPI; DS % Writes Other; DS Directory Writes/sec; DS % Searches from SAM; DS % Searches from DRA; DS % Searches from LDAP; DS % Searches from LSA; DS % Searches from KCC; DS % Searches from NSPI; DS % Searches Other; DS Directory Searches/sec; DS % Reads from SAM; DS % Reads from DRA; DRA Inbound Values (DNs only)/sec; DRA Inbound Objects Filtered/sec; DS % Reads from LSA; DS % Reads from KCC; DS % Reads from NSPI; DS % Reads Other; DS Directory Reads/sec; LDAP Successful Binds/sec; LDAP Bind Time; SAM Successful Computer Creations/sec: Includes all requests; SAM Machine Creation Attempts/sec; SAM Successful User Creations/sec; SAM User Creation Attempts/sec; SAM Password Changes/sec; SAM Membership Changes/sec; SAM Display

Information Queries/sec; SAM Enumerations/sec; SAM Transitive Membership Evaluations/sec; SAM Non-Transitive Membership Evaluations/sec; SAM Domain Local Group Membership Evaluations/sec; SAM Universal Group Membership Evaluations/sec; SAM Global Group Membership Evaluations/sec; SAM GC Evaluations/sec; DRA Inbound Full Sync Objects Remaining; DRA Inbound Bytes Total/sec; DRA Inbound Bytes Not Compressed (Within Site)/sec; DRA Inbound Bytes Compressed (Between Sites, Before Compression)/sec; DRA Inbound Bytes Compressed (Between Sites, After Compression)/sec; DRA Outbound Bytes Total/sec; DRA Outbound Bytes Not Compressed (Within Site)/sec; DRA Outbound Bytes Compressed (Between Sites, Before Compression)/sec; DRA Outbound Bytes Compressed (Between Sites, After Compression)/sec; DS Client Binds/sec; DS Server Binds/sec; DS Client Name Translations/sec; DS Server Name Translations/sec; DS Security Descriptor Propagator Runtime Queue; DS Security Descriptor Propagator Average Exclusion Time; DRA Outbound Objects Filtered/sec; DRA Outbound Values Total/sec; DRA Outbound Values (DNs only)/sec; AB ANR/sec; AB Property Reads/sec; AB Searches/sec; AB Matches/sec; AB Proxy Lookups/sec; ATQ Threads Total; ATQ Threads LDAP; ATQ Threads Other; DRA Inbound Bytes Total Since Boot; DRA Inbound Bytes Not Compressed (Within Site) Since Boot; DRA Inbound Bytes Compressed (Between Sites, Before Compression) Since Boot; DRA Inbound Bytes Compressed (Between Sites, After Compression) Since Boot; DRA Outbound Bytes Total Since Boot; DRA Outbound Bytes Not Compressed (Within Site) Since Boot; DRA Outbound Bytes Compressed (Between Sites, Before Compression) Since Boot; DRA Outbound Bytes Compressed (Between Sites, After Compression) Since Boot; LDAP New Connections/sec; LDAP Closed Connections/sec; LDAP New SSL Connections/sec; DRA Pending Replication Operations; DRA Threads Getting NC Changes; DRA Threads Getting NC Changes Holding Semaphore; DRA Inbound Link Value Updates Remaining in Packet; DRA Inbound Total Updates Remaining in Packet; DS % Writes from NTDSAPI; DS % Searches from NTDSAPI; DS % Reads from NTDSAPI; SAM Account Group Evaluation Latency; SAM Resource Group Evaluation Latency; ATQ Outstanding Queued Requests; ATQ Request Latency; ATQ Estimated Queue Delay; Tombstones Garbage Collected/sec; Phantoms Cleaned/sec; Link Values Cleaned/sec; Tombstones Visited/sec; Phantoms Visited/sec; NTLM Binds/sec; Negotiated Binds/sec; Digest Binds/sec; Simple Binds/sec; External Binds/sec; Fast Binds/sec; Base searches/sec; Subtree searches/sec; Onelevel searches/sec; Database adds/sec; Database modifys/sec; Database deletes/sec; Database recycles/sec; Approximate highest DNT; Transitive operations/sec; Transitive suboperations/sec; Transitive operations milliseconds run

interval = 10

disabled = 0

index=perfmon

useEnglishOnly=true

[admon://NearestDC]

monitorSubtree = 1

interval=3600

disabled=false

index=msad

#

Subnet Affinity Log

#

[monitor://C:\Windows\debug\netlogon.log]

sourcetype=MSAD:NT6:Netlogon

disabled=false

index=msad

Confi guration splunk supporting add on for active directory