

BEST PRACTICES

- 64bit Infrastructure
- Dedicated Report Server
- SQL Server Enterprise
- Use Noise Filters

COLLECTOR DEFAULTS

Retention Period = 14 Days
Database = 'OperationsManagerAC'
Data Source = 'OpsMgrAC'

KEY SQL VIEWS

dvHeader: Event & User Info
dvAll: dvHeader + all event parameters
dvAll5: dvHeader + 1st 5 parameters

NOISE FILTERING TIPS

- Syntax is WQL not SQL
- Query Length Max = 500 tokens
- Use WHERE NOT statements

COLLECTOR PERF. OBJECTS

- Connected Clients
- Database Queue % Full
- Database Queue Length
- DB Loader Events Inserts/Sec
- DB Loader Principal Inserts/Sec
- DB Loader Strings Inserts/Sec
- DB Principal Cache Hit %
- DB Requests Queue Length
- DB String Cache Hit %
- Event time in collector (milliseconds)
- Incoming Events/Sec
- Interface Audit Insertions/Sec
- Interface Queue Length
- Registered Queries

FORWARDER PERF. OBJECTS

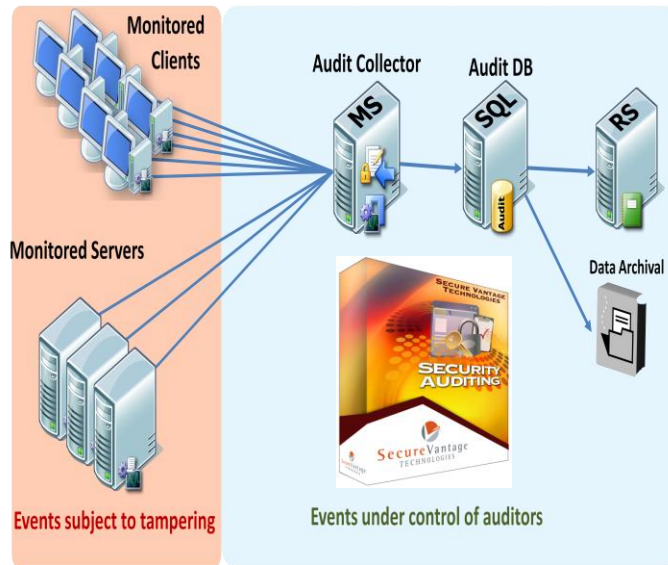
- Average time between event generation
- Incoming Audits/Sec

dtPARTITION STATUS CODES

0 = Active Partition
1 = InTransition Partition
2 = InActive Partition

dtConfig TABLE ENTRIES

1 = timestamp method
2 = database schema version
3 = perform index maintenance
4 = table switch offset in seconds
5 = table switch interval in seconds
6 = number of partitions



High Scalability

3,000 Servers or
150 Domain Controllers or
20,000 Workstations

High Performance

Average 2,500 events per sec
Peak 100,000 events per sec

Reporting Access

Read Only: AD Group with
SQL login to database and
db_datareader permission

ACS Security Quick Facts

- Requires Mutual Authentication
- Forwarder to Collector Encrypted
- Collector to Database Not Encrypted (use SSL or TLS to encrypt if required)
- TCP port 51909, Inbound to Collector

adtAdmin Command

adtAdmin.exe /<Parameter> [<subParameter>:<Value>]

Parameters

/AddGroup
/DelGroup
/Disconnect
/GetDBAuth
/GetQuery
/ListForwarders
/ListGroups
/SetDBAuth
/SetQuery
/Stats
/UpdFrowarder

SubParameters

/Collector:CollectorName
/Forwarder:Name
/ForwarderID:ForwarderID
/Group:GroupName
/GroupID:GroupID
/Value:ValueNumber

Note: adtAdmin must be run locally on Collector

Collector Directory: %systemroot%\system32\security\Adtserver

Noise Filtering – Get Example

adtadmin /getquery /collector:acs01

Default Filter: **SELECT * FROM AdtsEvent**

Noise Filtering – Set Example

Adtadmin /setquery /collector:acs01 **SELECT * FROM AdtsEvent WHERE NOT ((HEADERUSER LIKE '%SYS_%') AND(EventID = 528 OR EventID = 540))**

Important Event IDs

4618 If ACS is healthy, ignore
4619-4621 where status <> 0, partition management errors
4631 Forwarder disconnected
4635 Event gap stream detected
4636 Forwarder rejected

Collector Database Planning

Recommended Disk Space =
((IncomingEventsSec * 0.4kb * 60 sec * 60min * 24hr) / 1048576) * [RetentionPeriod] = total size of database in GB

Collector Memory Planning

Recommended Memory =
(M x .5)+(50 x N)+(S x .5)+(P x .1)
M = MaximumQueueLength
N = # of Forwarders Connected
S = StringCacheSize
P = PrincipalCacheSize

Collector Queue Settings

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AdtServer\Parameters

Setting Name	Default
MaximumQueueLength	0x40000
BackOffThreshold	75
DisconnectThreshold	90

Team Blog

<http://securevantage.spaces.live.com>

Secure Vantage ACS Value-Adds

- Audit Collection Admin™
- Audit Collection Archiver™
- Audit Collection Base Reporting™
- Audit Collection Compliance Reporting™
- Audit Collection SYSLOG Gateway™

Secure Vantage ACS Resources

- Audit Collection Noise Filter Guide
- Audit Collection Storage Planning Worksheet
- ACS Archiving & Historical Reporting Planning Guide
- Windows Security Auditing Reference List