

Secure Vantage

ACS Noise Filter Guide



Secure Vantage
TECHNOLOGIES

Authors: Chance Folmar

Published: April 2007

Last Modified: November 3rd 2007

Applies To: System Center Operations Manager 2007

Document Version: v 1.50

Acknowledgements: Jeremiah Beckett, Joseph Chan, Eric Fitzgerald, Rory McCaw and Randy Franklin Smith

Table of Contents

OVERVIEW	3
WINDOWS SERVER BASE FILTERS	4
FS1001: WINDOWS SERVER ESSENTIAL FILTER.....	4
<i>Event Filter Scope</i>	4
<i>Event Filter Syntax</i>	5
FS1002: WINDOWS SERVER REASONABLE FILTERS	5
<i>Event Filter Scope</i>	5
<i>Event Filter Syntax</i>	6
FS1003: WINDOWS SERVER RATIONAL FILTERS	6
<i>Event Filter Scope</i>	6
<i>Event Filter Syntax</i>	6
FS1004: WINDOWS SERVER AUTHENTICATION COMPUTER\$ FILTER	7
<i>Event Filter Scope</i>	7
<i>Event Filter Syntax</i>	7
MANAGING FILTERS	8
REVIEW EXISTING FILTERS	8
<i>Command Syntax</i>	8
APPLYING NEW FILTERS	8
<i>Command Syntax</i>	8
<i>Sample: Loading FS1001 Filter</i>	8
COMBINING DIFFERENT FILTERS	9
<i>Sample: Combining Filter FS1001 & FS1002</i>	9
COLLECTION LOAD ANALYSIS	9

OVERVIEW

In most cases it is often unnecessary or impractical to collect and store all security events. While the Audit Collection Service (ACS) natively collects all security events from a target system it includes a filtering mechanism which can be used to manage event insertion and storage to the SQL database. Filters can be implemented based on event ID or on the contents of the events themselves.

The Secure Vantage ACS Noise Filters Guide provides essential filter sets and guidance to optimize data collection which improves both online and offline storage capabilities. This guide introduces the Noise Filters for Windows Servers 2000 & 2003 Security Events.

ACS Noise Filters are based on Microsoft recommended event filters defined in the Security Attack and Detection Planning Guide and best practices from Microsoft Security MVP, Randy Franklin Smith.

Security Attack Detection and Planning Guide :

<http://www.microsoft.com/technet/security/guidance/auditingandmonitoring/securitymonitoring/default.aspx>

Ultimate Windows Security : <http://www.ultimatewindowssecurity.com>

WINDOWS SERVER BASE FILTERS

The Windows Server Base Filters recommend multiple filter sets depending on overall auditing scope and reporting needs.

FS1001: Windows Server Essential Filter

The Windows Server Essentials filter provides the basic filter set that should be used in any Audit Collection environment. This is not a standard but rather a recommendation based on Microsoft best practices and customer testing.

Event Filter Scope

Event	Description	Filter Rationale
551	User initiates logoff	Event 538 confirms logoff, use instead if you want to collect logoffs.
562	A handle to an object closed	Always records a success
573	Process generates nonsystem audit event with Authorization Application Programming Interface (AuthZ API)	MS defined Typical Behavior
577 & 578	Privilege service called, privileged object operation	Very high volume events that provide little information to act upon or understand in most cases.
594	A handle to an object was duplicated	MS defined Typical Behavior
595	Indirect access to an object was obtained	MS defined Typical Behavior
596	Backup of data protection master key	Occurs every 90 days automatically with default settings
597	Recovery of data protection master key	MS defined Typical Behavior
697	Password policy checking API called	MS defined Typical Behavior
768	Forest namespace collision	MS defined Not Security Related
769, 770, 771	Trusted forest information added, deleted or modified	Normal operations of inter-forest trusts. Do not confuse these with addition, deletion, or modification of the trust itself.
832 - 841	Various Active Directory replication issues	MS defined No Security Implications

Event Filter Syntax

```
--FS1001: Windows Server Essential Filters
SELECT *
FROM AdtsEvent WHERE NOT
(EventId=551
Or EventId=562
OR EventId=573
OR EventId=577
OR EventId=578
OR EventId=697
OR (EventId>=594 AND EventId<=597)
OR (EventId>=768 AND EventId<=771)
OR (EventId>=832 AND EventId<=841)
)
```

FS1002: Windows Server Reasonable Filters

The Windows Server Reasonable filters provide an extension to the essentials that is acceptable to most environments and reduces considerable noise.

Event Filter Scope

Event	Description	Filter Rationale
538	User logoff	This event only indicates the time a user initiates logoff or the when the system initiates logoff. This does not mean the user actually stopped using the system.
672	Kerberos AS Ticket request	If you collect logon events 528 and 540 from all computers, this event only adds data that a Kerberos TGT was granted. As there must still be a service ticket granted (event 673) for any access to occur, this event may be redundant. Please note this event can be associated with smart card logons if applicable
680	Account Logon	If you collect logon events 528 and 540 from all computers, this event only records validation of the account credentials. Separate logon events record what the user accessed, this event may be redundant.

Event Filter Syntax

--FS1002: Windows Server Reasonable Filters

```
SELECT *
FROM AdtsEvent WHERE NOT
(EventId=538
Or EventId=672
OR EventId=680
)
```

FS1003: Windows Server Rational Filters

The Windows Server Rational filters go beyond raw event id filtering to provide target filtering.

Event Filter Scope

Event	Description	Filter Rationale
571	Client Context deleted by Authorization Manager.	Normal activity where Authorization Manager is active and in use
624	User Account Created where New Account Name ends with '\$'	A domain user has created or connected a new computer account to the domain. This may be normal activity is users have this right.
627	Change Password Attempt where User equals 'System' and Target Account Name equals 'TsInternetUser' and Caller User Name ends with '\$'	This is normal behavior of a computer that runs Terminal Services.

Event Filter Syntax

--FS1003: Windows Server Rational Filters

```
SELECT *
FROM AdtsEvent WHERE NOT
(EventId=571
Or (EventId=624 And TargetUser LIKE '%$%')
OR (EventId=627 AND HeaderUser='System' AND ClientUser like '%$%' And
TargetUser = 'TsInternetUser'))
```

FS1004: Windows Server Authentication Computer\$ Filter

The Windows Server Authentication Computer\$ filter provides filtering for common logon traffic relating to computer accounts.

Event Filter Scope

Event	Description	Filter Rationale
538 & 540	Where Logon Type = 3 and User Name contains \$	Windows Computers generate many logon/logoff events on DCs as they frequently check for group policy updates and query other information in AD. Please note Filter Set 1002 already excludes event 538.
672 - 677	Where User Name contains \$	Windows Computers generate many Kerberos events as they frequently check for group policy updates and query other information in AD. Please note Filter Set 1002 already excludes event 672.

Event Filter Syntax

```
--FS1004: Windows Server Authentication Computer$ Filter
Select * from AdtsEvent where NOT (((EventId = 538 or EventId = 540)
AND (String01 = '3') AND HeaderUser like '%$%')) OR ((EventId > 671 and
EventId < 678) and ClientUser LIKE '%$%')
```

MANAGING FILTERS

Managing filters is done through the `adtAdmin` command. The following information provides general guidelines for the command syntax and use with our noise filter templates.

*Please Note: Filter complexity and length can impact WMI performance. The first place to manage event filters is at the Audit Policy level, then Objects (if auditing Directory Services or Object Access), then ACS.

Review Existing Filters

You can use the `adtAdmin` command to list the ACS Collection filters. The following information shows the general syntax and a sample of using the command. This can be used to check existing filters or validate new ones that are loaded. More information on the `adtAdmin` command can be found in the Operations Manager Help libraries on your Management Server.

Command Syntax

```
AdtAdmin.exe /getquery [/Collector:CollectorName]
```

Applying New Filters

You can use the `adtAdmin` command to update the ACS Collection filters. The following information shows the general syntax and a sample of using the command with one of the filters described in this guide.

Command Syntax

```
AdtAdmin.exe /SetQuery [/Collector:CollectorName] /Query:QuerySyntax
```

Sample: Loading FS1001 Filter

```
adtadmin /setquery /collector:"Collector Name" /query:"SELECT *  
FROM AdtsEvent WHERE NOT(EventId=551 Or EventId=562 OR EventId=573 OR  
EventId=577 OR EventId=578 OR EventId=697 OR (EventId>=594 AND  
EventId<=597)OR (EventId>=768 AND EventId<=771) OR (EventId>=532 AND  
EventId<=841))"
```

Combining Different Filters

You can consolidate different filters in the document by combining the WQL syntax to a single query

Sample: Combining Filter FS1001 & FS1002

--FS1001: Windows Server Essential Filters

```
SELECT * FROM AdtsEvent WHERE NOT (EventId=551 OR EventId=562 OR
EventId=573 OR EventId=577 OR EventId=578 OR EventId=697 OR
(EventId>=594 AND EventId<=597) OR (EventId>=768 AND EventId<=771) OR
(EventId>=832 AND EventId<=841))
```

--FS1002: Windows Server Reasonable Filters

```
SELECT * FROM AdtsEvent WHERE NOT(EventId=538 OR EventId=672 OR
EventId=680)
```

--Combined Custom Filter

```
SELECT * FROM AdtsEvent WHERE NOT (EventId=551 OR EventId=562 OR
EventId=573 OR EventId=577 OR EventId=578 OR EventId=697 OR EventId=538
OR EventId=672 OR EventId=680 OR (EventId>=594 AND EventId<=597) OR
(EventId>=768 AND EventId<=771) OR (EventId>=832 AND EventId<=841))
```

Collection Load Analysis

Before and after you implement ACS filters it is important to understand the current event stream to validate your filters are working and also help identify other opportunities for performance tuning. Customers can leverage both reports and performance counters to assist with this analysis.

Secure Vantage provides an 'Event Load Analysis' report which identifies the count of unique events and primary objects plus a range of other analytics about your event stream. Customer can also leverage the canned event analysis reports from Microsoft and ACS performance counters.