AMIYA

Server Access log Management

ALog ConVerter®

Database Access log Management

ALog ConVerter® DB

※ALog ConVerter is the registered trademark of AMIYA Corporation.
※Each company names and trade-marks are registered company names and names of products.
※ Mentioned products' specifications and functions may be modified for improvement without any notifications.

ver. 7.4.0_4_En

ALog Series

ALog ConVerter

- Acquires server access from layers of Operation System (OS)
- Integrated log management system of multiple servers

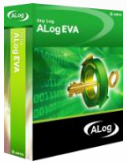
Enterprise type

Resource Athlete

- Multifunctional server management tool
- EX) Identifying access permission information of particular folders, eliminating unnecessary files, etc.

ALog ConVerter DB

- Acquires log from the database application layers
- Stores scattered database logs as a unified data



ALog EVA

- Expands the domain of ALog protection
- Unifying log product

What is ALog ConVerter ?

ALog ConVerter is a tool to obtain access history of the vital data without re-siding any agent.
You can have low cost and efficient log management as ALog ConVerter collects log data from the server side where the vital data is stored.

Analyze law log,

To the actual operation

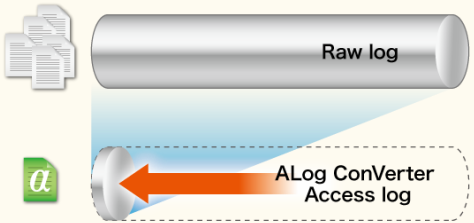
ALog's conversion engine creates a clear story of actual user actions that tells you the Who, the When, and the What about file accessed ,based on the complex raw logs.

Time	User	Server	Object	Action
2016/1/18 15:04:50	amiya.co.jp¥Steve	amiyafs-vol1	E:¥DATA¥client info¥customerlist.xls	READ
2016/1/18 15:05:22	amiya.co.jp¥Steve	amiyafs-vol1	E:¥DATA¥client info¥customerlist.xls	WRITE
2016/1/18 15:05:34	amiya.co.jp¥Steve	amiyafs-vol1	E:¥DATA¥client info¥customerlist.xls	DELETE

Automatic

Super compact

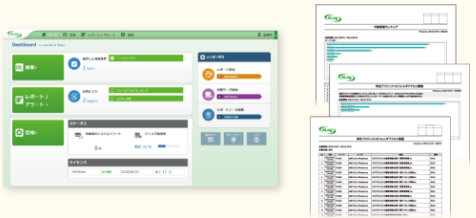
ALog's conversion engine log compress even more the minimized access and store.
Super compact means you can keep a large amount of data for a long period of time.



Intuitive

Search/Analyze

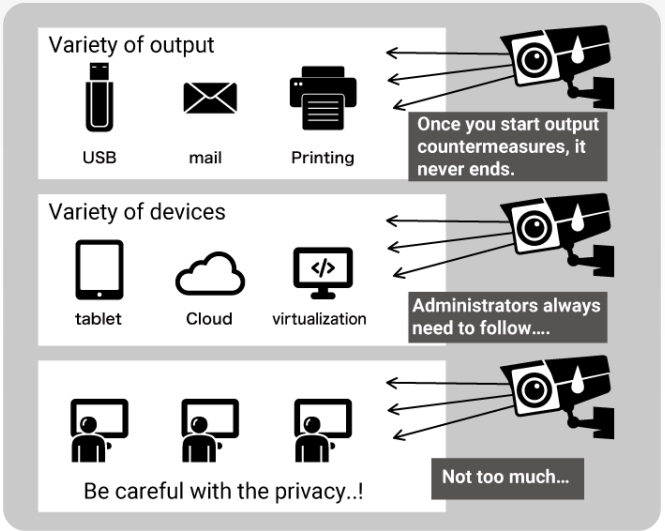
Intuitive search by using Web browser.
Not only for IT manager, Anybody can easily operate.



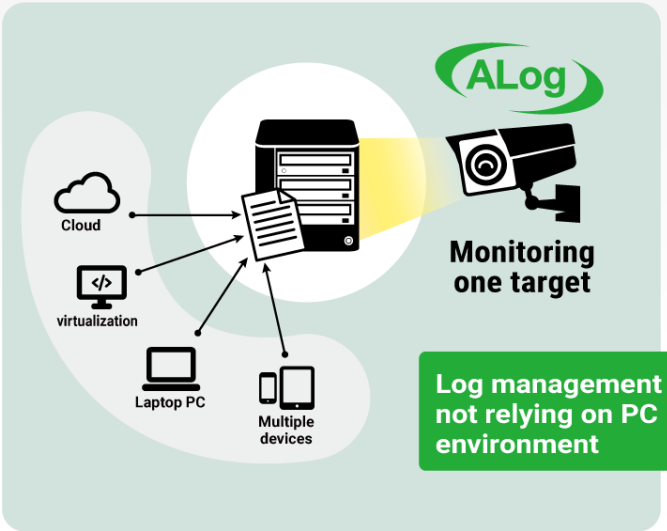
Focus your monitoring target to the vital data

PC asset management ; such as monitor employee's internet browsing and device control is needless to say important.
However you need to consider the long term trouble and strain on systems operations, maintenance and high cost.
ALog monitors and analyzes users' access to servers and databases at the server level that stores all the critical data, which means greatly effective.

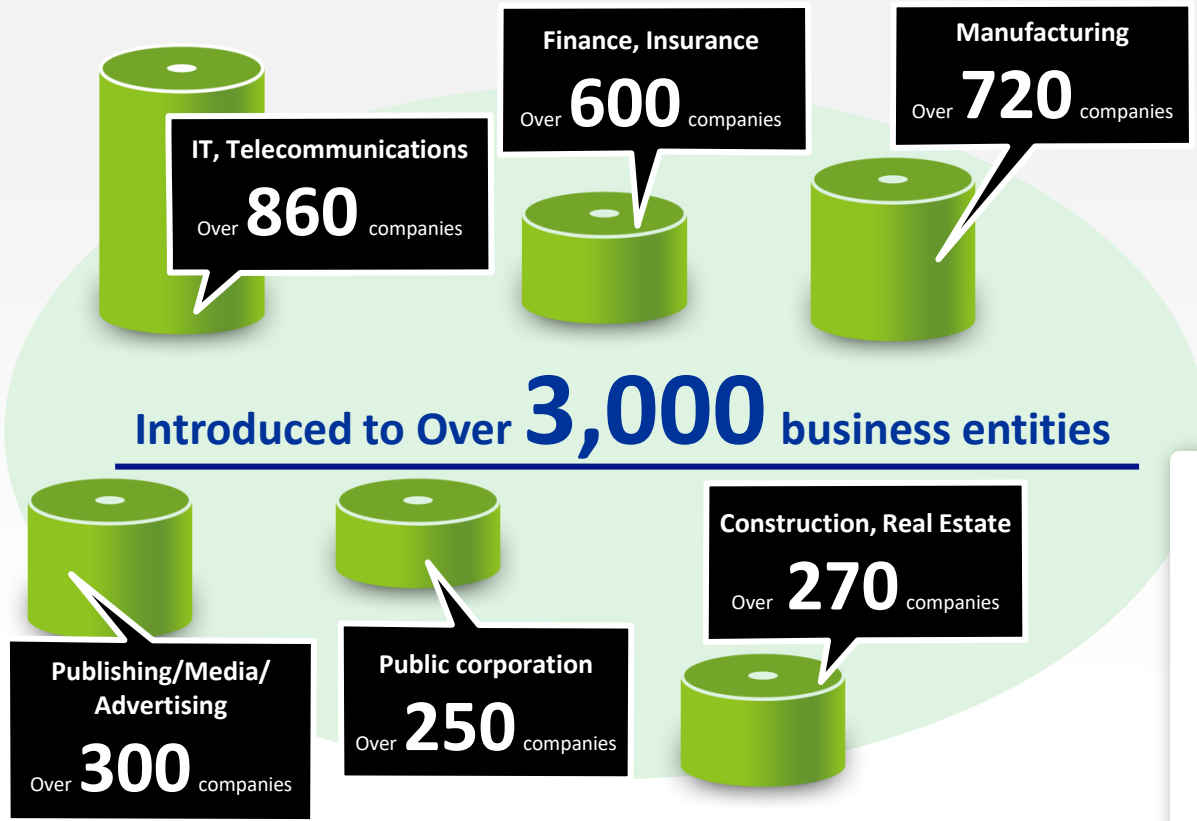
Client PC control/ Monitor

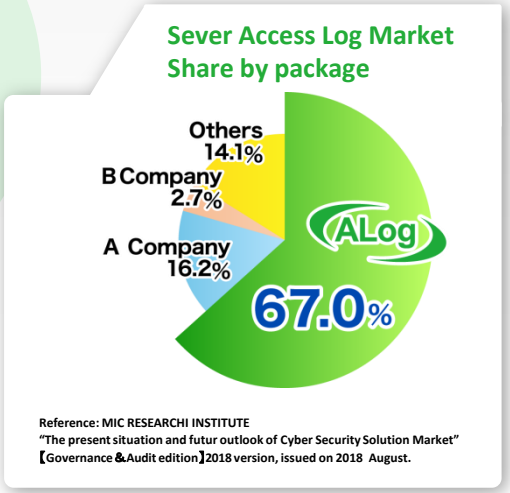


Server data Monitor

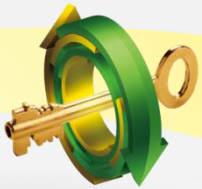


ALog Converter Installations





3 Major benefits of ALog ConVerter®



System Impact — No impact on the Current operating environment

No agent's required to run on either Client PC or the server.

Maintenannce — Lightweight manageability for Long term archive

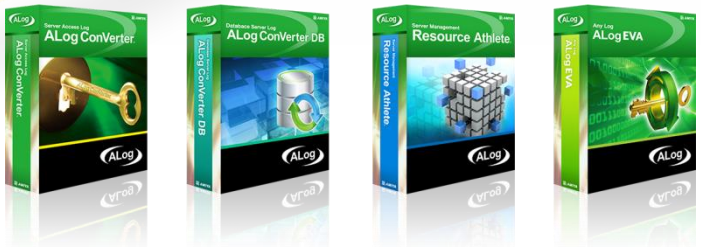
Log archive is compressed to less than 1/ thousands.
Fast speed log search functionality.

Initial Cost — Reasonable pricing

No multiple license for each PC are Required.
Integrated All-in-One functionality.

Other benefits

- No need purchase search database
- Support English/ Chinese OS
- Easy install with simple wizard



Wide range support of ALog

The Advantage of ALog is its wide range support that is able to gather not only operation log for Windows file server but also various records such as Linux/NAS storage server OS log, database application log, syslog from network.

ALog's advantage

It is difficult to comprehend the actual user operation from law event log.
ALog can output 『Actual user operation』

* In the case of un executed log output such as virus scan, back up and file search, it can be stopped with settings.

Easy

Complex log data → **easy to understand log data**

```
S-1-5-21-2910433525-404745982-3962478095-
500/Toshio/2008SP2/0x50b70/Security/File/E:¥DATA¥client
info¥customerlist.xls/0x534/%%4416 /0x1/0x4//
S-1-5-21-2910433525-404745982-3962478095-
500/Toshio/2008SP2/0x50b70/Security/File/E:¥DATA¥client info¥customerlist.xls
/0x534/%%4416 /0x1/0x4//
S-1-5-21-2910433525-404745982-3962478095-
500/Toshio/2008SP2/0x50b70/Security/File/E:¥DATA¥client info¥customerlist.xls
```

Time	User	Server	Object	Action
2016/1/18 15:04:50	amiya.co.jp¥Steve	amiyafs-vol1	E:¥DATA¥client info¥customerlist.xls	READ
2016/1/18 15:05:22	amiya.co.jp¥Steve	amiyafs-vol1	E:¥DATA¥client info¥customerlist.xls	WRITE
2016/1/18 15:05:34	amiya.co.jp¥Steve	amiyafs-vol1	E:¥DATA¥client info¥customerlist.xls	DELETE

Smaller

Inaccurate content → **Accurate operational history**

Accurate

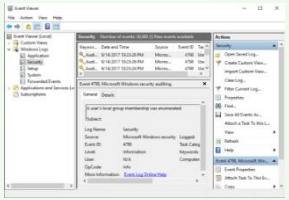
Large volume log → **Super compact**

*Reduce rate will be affected by environment/ folder path length/ OS.

One and only access log -File access log-

AMIYA

With only event logs...



10/25/201713:34:10Microsoft-Windows-Security-AuditingAUDITSUCCESSSomething4656N/AYNS-08R2SP1 S-1-5-21-4117455682-877842489-1775433442-001/testuser/YNS-08R2SP1/0x2ba450/Security/File/C:test 0x1024/{00000000-0000-0000-0000-0000000000}/%%1541 %%4416 %%4423 /%%1541: %%1801 D:(A;OICI;FA;;;WD) %%4416: %%1801 D:(A;OICI;FA;;;WD) %%4423: %%1801 D:(A;OICI;FA;;;WD) /0x100081/-/0/0x4//

Incomprehensible!

In case of regular log products...

E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	DELETE
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	READ
E:\DATA\client info\customerlist.xls	WRITE

Different from actual operation...

But with ALog

Mike	E:\DATA\customerinfo\important_customerlist.xls	READ
Mike	E:\DATA\customerinfo\important_customerlist.xls	WRITE

Mike “opened” the file and “wrote.”

As access logs of actual operation

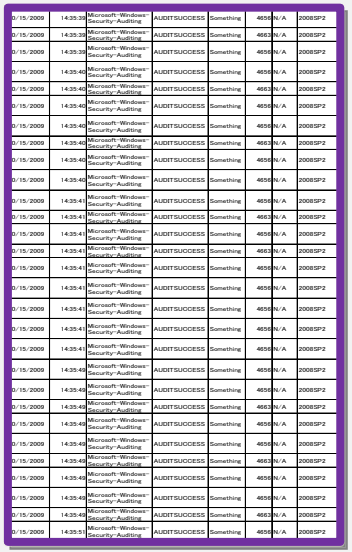
Regular log products only divide cells and display them in a clear way.
But ALog can analyze and interpret complex event logs.
ALog enables input and output corresponding to operations of each user.

One and only access log –DB access log-

Incomprehensible trace logs...

<AuditRecord><Audit_Type>1</Audit_Type><Session_Id>1560282</Session_Id><EntryId>22</EntryId><Extended_Timestamp>2010-03-17T15:28:50.666000</Extended_Timestamp><DB_User>Toshio</DB_User><OS_User>DBSV01\suzuki</OS_User><Userhost>AMIYA.CO.JP\DBSV01</Userhost>

Log amounts are too large to comprehend...



ALog generates simple display of DB operations

User	Target	Operation	Details
Mike_01	User logged on	DB_LOGON	Count:1 DB: Account DB
Mike_01	Data of master table was referred to	DB_SELECT	Count:1 DB: Account DB

Mike logged on and referred to the account DB

Converting logic of ALog is also applicable to database products. ALog interprets a large amount of trace logs, and outputs logs of which manipulation is comprehensible.

Cases of using ALog

LINE Corporation *for Windows*

Background

There used to be a professional security team for monitoring daily internal and external unauthorized access. But recently, they decided to install ALog converter for event logs to be translated and analyzed.

Solution

ALog reduced a work load of log analysis by analyzing and converting complex event logs in a concise style. Simple display promoted efficiency in information system department as well since it can be used for check mistakes in operation and to identify causes of errors.

exp: A search of missing files

Type a missing file name with using ALog.
Then, it was found out that Takagi moved the file into other drive.

Time	User	Object	Operation	Detail
2017/8/7 18:02	Mike	D:\engine development\nextgenerationEVdevelopment\patent technology.xls	DELETE	ClientIP:192.168.7.10 ClientName:takagi-pc・・・
2017/8/7 18:02	Mike	E:\filevo\personalinfo\Takagi\patent technology.xls	WRITE	・・・・・・・・

An automotive company *for SQL Server*

Background

A large automobile enterprise decided to monitor database operation of administrators internal for countermeasures for internal threat.
ALog was chosen due to its small burden on database/network bandwidth and disk storage.

Solution

ALog collects daily database access, and enables to detect unusual access. In addition to monitoring operations of administrators, ALog produced spin-off such as detecting unexpected database access including outsider threats.

exp: Monitoring of direct access

ALog detected “UPDATE” operation from an application outside of the authorized systems.
It was found that Kaneko rewrote payroll section!

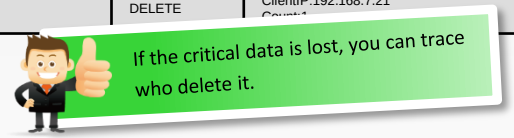
Time	User	Object	Operation	Detail
2014/3/15 22:15	Ken	HR payroll DB table [amount]has been updated	DB_UPDATE	AppName:Microsoft SQL Server Management Studio- query ClientName・・・・
2014/3/15 22:15	Ken	UPDATE [amount] SET salary=3,065,700 WHERE・・・	DB_RAWSQL	・・・・・・・・・・・・・・・

Obtainable log – for Windows

File access log

ALog records access log data for not only success but also failure operational log as well.

Time	User	Server	Object	Operation	Detail
2015/1/18 15:04:50	Domain\David	amiyafs-vol1	D:\engine development\nextgenerationEVdevelopment\patent technology.xls	READ	ClientIP:192.168.7.10 Count:3
2015/1/18 15:05:22	Domain\David	amiyafs-vol1	D:\confidential\personalinfo\personal profile.doc	WRITE	ClientIP:192.168.7.21 Count:1
2015/1/18 15:05:34	Domain\David	amiyafs-vol1	D:\confidential\personalinfo\personal profile.doc	DELETE	ClientIP:192.168.7.21



Log on log

ALog grasps an overview of user activity including when users receive Windows certification from AD server (=when users activate computer). Name of computer machine and IP address are also obtainable

Time	User	Server	Object	Operation	Detail
2015/01/17 08:34:50	Domain\Steve	AMYDC01	steve-pc	LOGON	AuthType:NTLM ClientName:steve-pc Count:1
2015/01/18 02:04:43	Domain\Steve	AMYDC01	steve-pc	LOGON	AuthType:NTLM ClientName:steve-pc Count:1
2015/01/18 08:40:29	Domain\Steve	AMYDC01	steve-pc	LOGON-Failure	AuthType:NTLM ClientName:steve-pc Count:1

Obtainable log – for Windows

Administrator operational log

privileged administrators use such as [new user registration] or [policy change] is recorded through AD server.

Time	User	Server	Object	Operation	Detail
2015/03/15 12:02:13	AMIYA\amiyaadmin	AMYDC01	User account creation: amiya.co.jp\mike	ADMIN	Count:1 EventID:4720
2015/03/15 12:05:14	AMIYA\administrator	AMYDC01	User account creation: amiya.co.jp\john	ADMIN	Count:1 EventID:4720
2015/03/15 12:05:20	AMIYA\amiyaadmin	AMYDC01	Password's change of account amiya.co.jp\mike	ADMIN	Count:1 EventID:4723

*Obtainable item: user creation/ deletion, user permission change, user password change, group member change

Access permission change log

Access permission change log able to record changes made to privileged users and authorizations.

Time	User	Server	Object	Operation	Detail
2015/12/09 09:21:50	AMIYA\john	amiyafs-vol1	D:\DATA\share\sales\quote\quotebook	P-ACCESS	ClientIP:192.168.0.21 Count:1
2015/12/09 15:22:10	AMIYA\steve	amiyafs-vol3	D:\DATA\accounting\salary\employee payslip	P-ACCESS	ClientIP:192.168.0.45 Count:1
2015/12/09 23:50:25	AMIYA\administrator	amiyafs-vol3	D:\DATA\accounting\salary\employee payslip	P-ACCESS	ClientIP:192.168.0.33 Count:1

*Access permission changed detail can not be discribed. Access permission detail can be obtained with ALog series [Resource Athlete].

Obtainable log – for Windows

Print log

If printer server is targeted, print record is obtainable; which includes [When] [Who] [Which files]

Time	User	Server	Object	Operation	詳細
2015/03/17 17:48:43	Mike	amiyaps401\Epson-LP9000	Y2012 sales _byshop _list.xls	PRINT	Count:1 Page:4 Printer:Epson-LP9000
2015/03/17 17:49:22	John	amiyaps401\Epson-LP9000	By industory-top income earner data.xls	PRINT	Count:1 Page:4 Printer:Epson-LP9000
2015/03/17 17:51:21	Mike	amiyaps401\Epson-LP9000	Clientdata (credit info).mdb	PRINT	Count:1 Page:4 Printer:Epson-LP9000

Logon/ Logoff log (script)

Script is set in domain controller without using event log , and user's logon and logoff events are recorded by using script.

Time	User	Server	Object	Operation	Detail
2015/01/21 09:04:03	amiya.co.jp\mike	AMYDC01	mike-pc [192.168.10.75]	LOGON	ClientIP:192.168.10.75 ClientName:mike-pc Count:1 LogonType:Script
2015/01/21 21:04:08	amiya.co.jp\mike	AMYDC01	mike-pc	LOGOFF	ClientIP:192.168.10.75 ClientName:mike-pc Count:1 LogonType:Script

*Obtain more accurate information for logon/logoff, as information from event log is not always accurate.

You can comprehend work actual condition of employees through domain log on/ log off.

Obtainable logs– for SQL Server

DB access log

ALog records manipulations such as reading or updating tables.

Time	User	Server	Object	Operation	Detail
2015/7/23 20:03:32	Domain\David	DC001\ins01	master table 「t_user」 Date has been referred	DB_SELECT	AppName:Microsoft SQL Server Management Studio – query ClientName:pc01

DB logon/logoff

ALog records user database logging activities.

Time	User	Server	Object	Operation	Detail
2015/7/23 20:01:00	Domain\David	DC001\ins01	pc1	DB_LOGON	AppName:Microsoft SQL Server Management Studio ・・・・・

DB Administration operational log

ALog records manipulations of database operational administrators such as adding/deletion of users and revision of tables.

Time	User	Server	Object	Operation	Detail
2015/8/15 21:00:00	Domain\Administrator	DC011\DB53	master table 「t_user」 Date has been created	DB_ADMIN	AppName:OSQL-32 ClientName:pc01 Count:1 DB:master

※for Oracle can acquire manipulation logs of SYSDBA users as well

Obtainable log list

ALog ConVerter

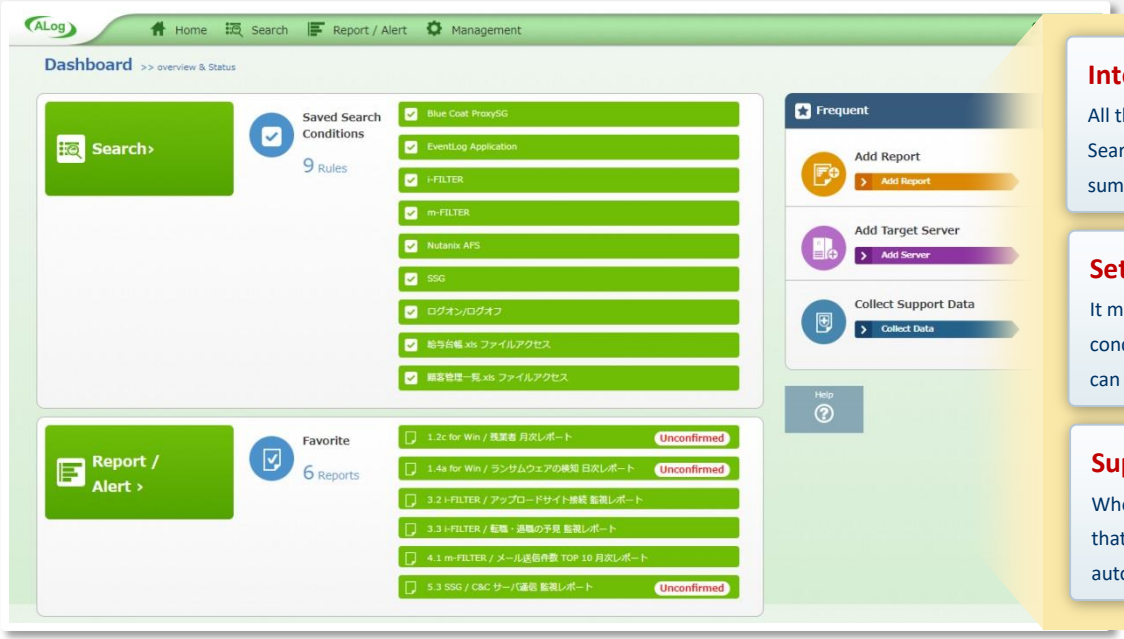
	Windows	NetApp	EMC	Isilon	Linux
File access log	○	○	○	○	○
Logon log	○	-	-	-	-
Logon Logoff log (script)	○	※	※	※	-
Administrator operational log	○	※	※	※	-
Print log	○	-	-	-	-
Access permission change log	○	○	○	○	○
Application execution log	○	-	-	-	-
Logon Logoff log	-	-	-	-	○
Command execution log	-	-	-	-	○
Syslog	-	-	-	-	○

*In the case of using ALog ConVeter for NAS or ALog ConVeter for Windows AE, log can be obtained through AD server.

ALog ConVerter DB

	SQL Server	Oracle
DB access log	○	○
DBLogon log・Logoff log (script)	○	○
DB Administrator operational log	○	○
RAWSQL log	○	○
SYSDBA log	–	○

ALog *interface*



Integrated interface

All the function Search/Summary/Monitoring/Management are summarized on top page as dash board.

Setting condition save function

It memorizes once defined “search filter condition” and “Monitoring report”, so that you can find them from top display.

Support data collect function

When the trouble occurs, necessary setting file that needs to be sent to support center will be automatically generated.

ALog V7 *interface*

viewing user restriction

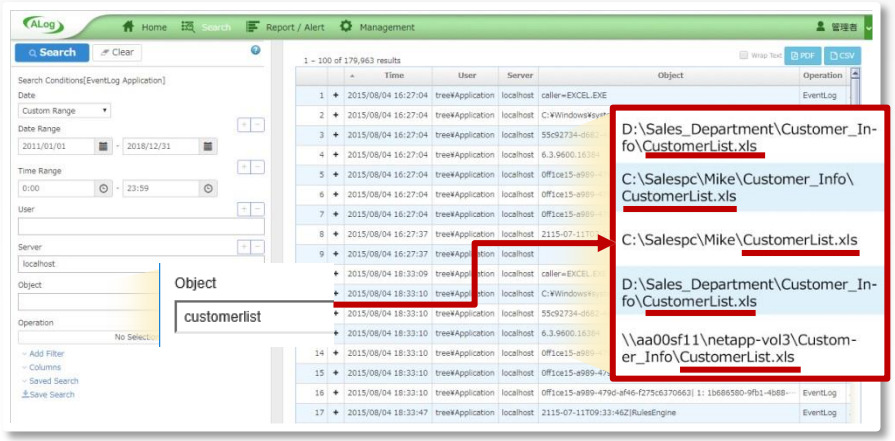
Ex: Let Branch manager A refer to access Log only under Tokyo Branch folder.

Active Directory coordination

Authorized user who logs in will be coordinated with Active Directory.

High speed transaction for search

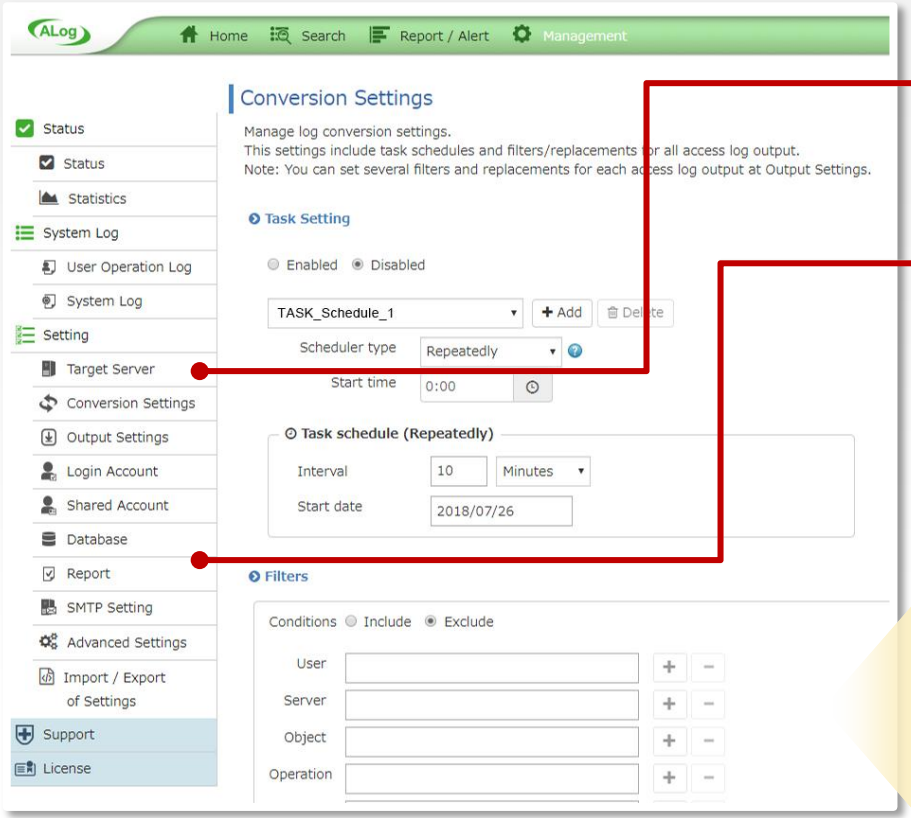
realized high speed search transaction from V7, and become faster and easier than ever.



Log filter

- Only want to search for the file named “customer management”.
- Want to know Mr. B’s monthly access history.
- Want to search the user who deleted C file.

ALog V7 *Interface*



Management Function

Target server/status confirmation for manager serve and each system configuration

Management Function

When the trouble occurred, alert mail will be sent to the designated mail address.

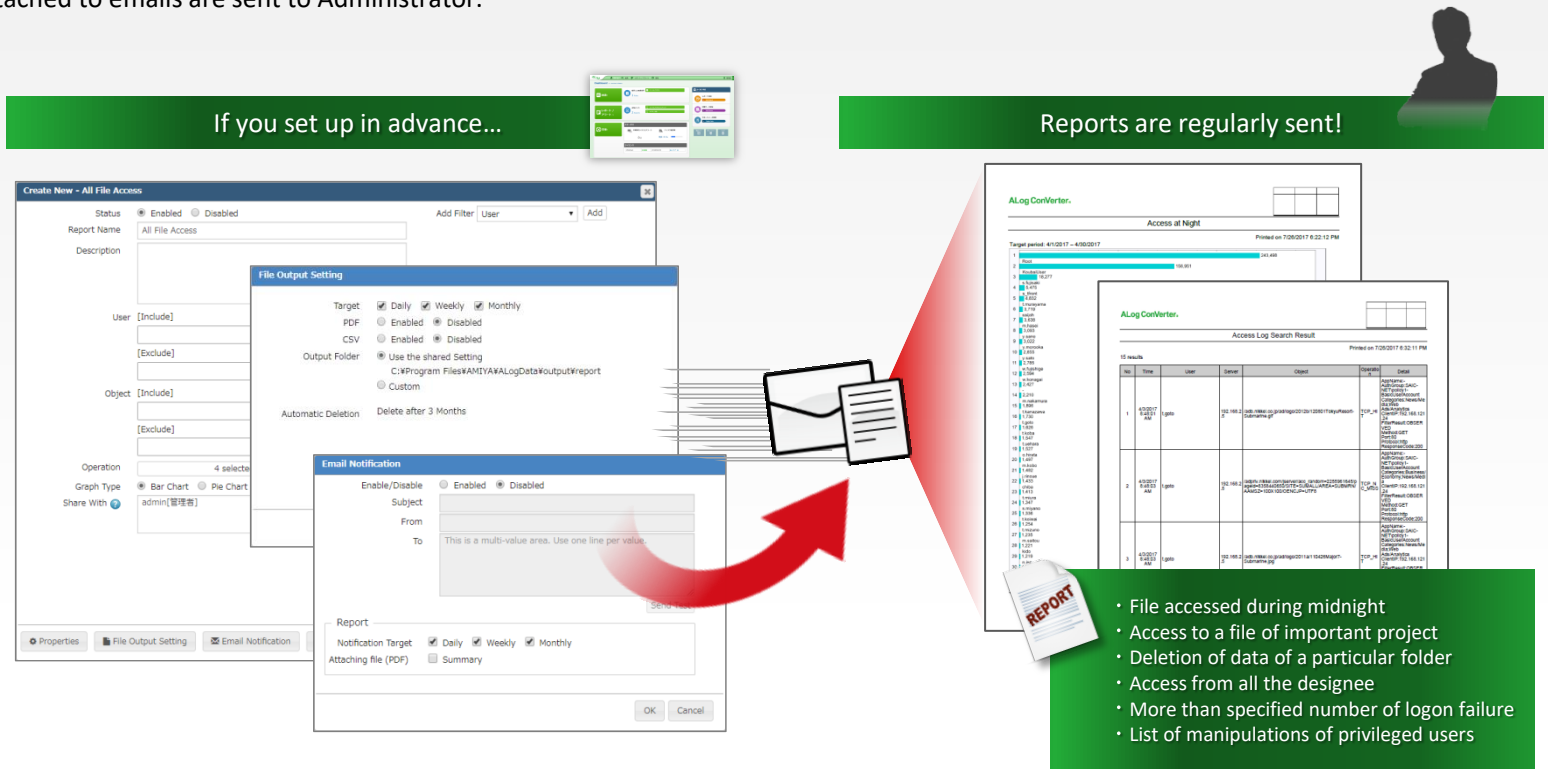
Filter Setting

Able to stop the output of unfollowing log

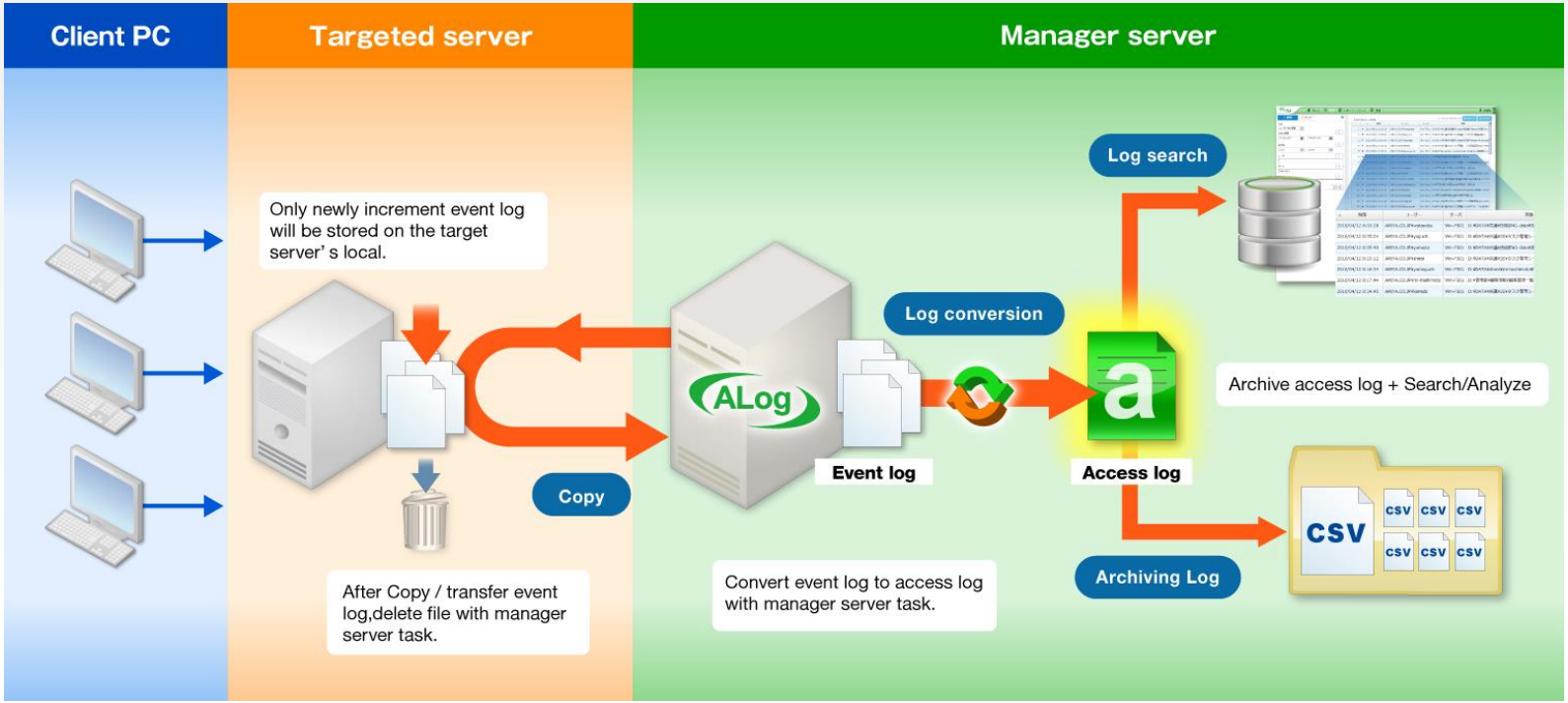
- System file log such as Thumbs.db
- Temporary file log of office application
- Antivirus and backup execution user log

Automatic report creation system

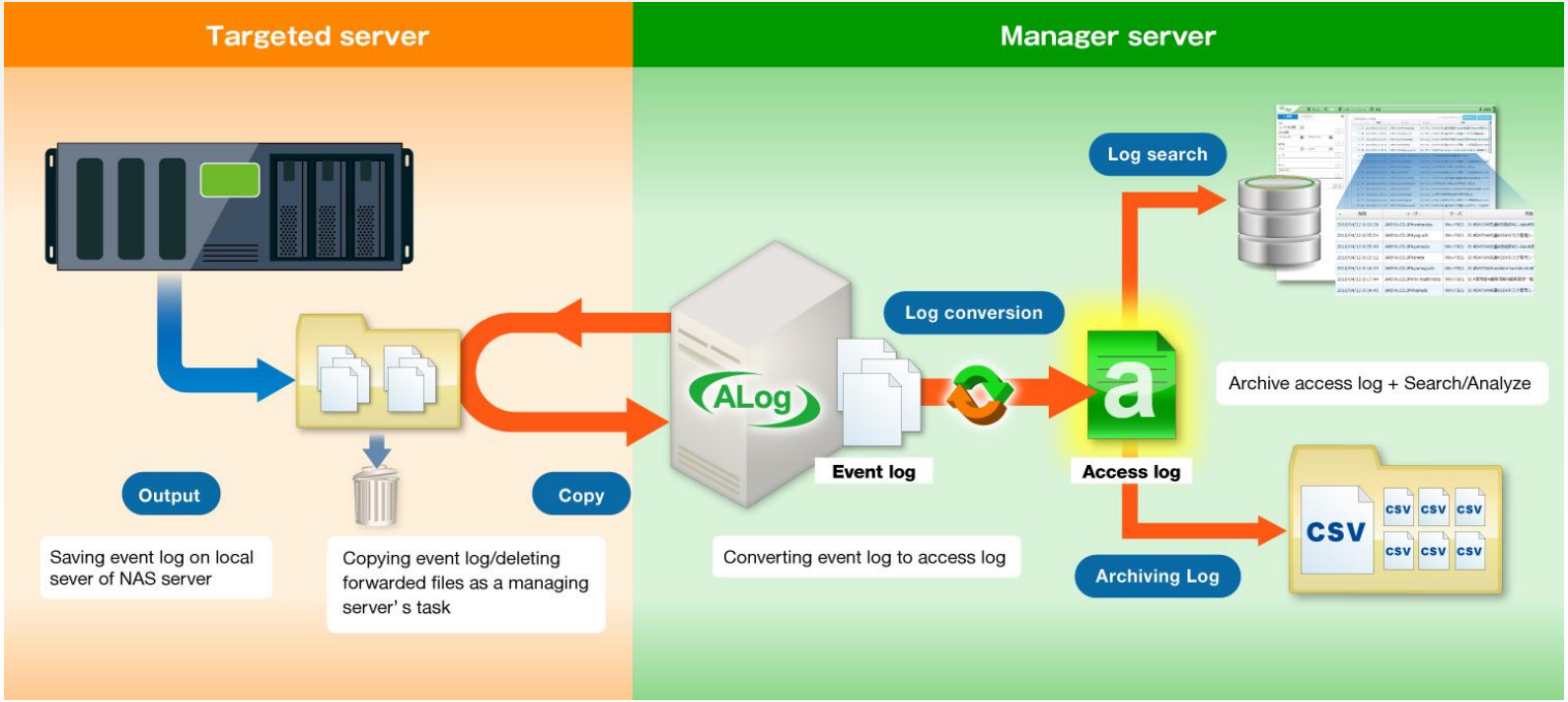
ALog automatically creates regularly reports. The contents of monitoring reports need be set up by users in advance.
Also files attached to emails are sent to Administrator.



Operation flow 【for Windows】

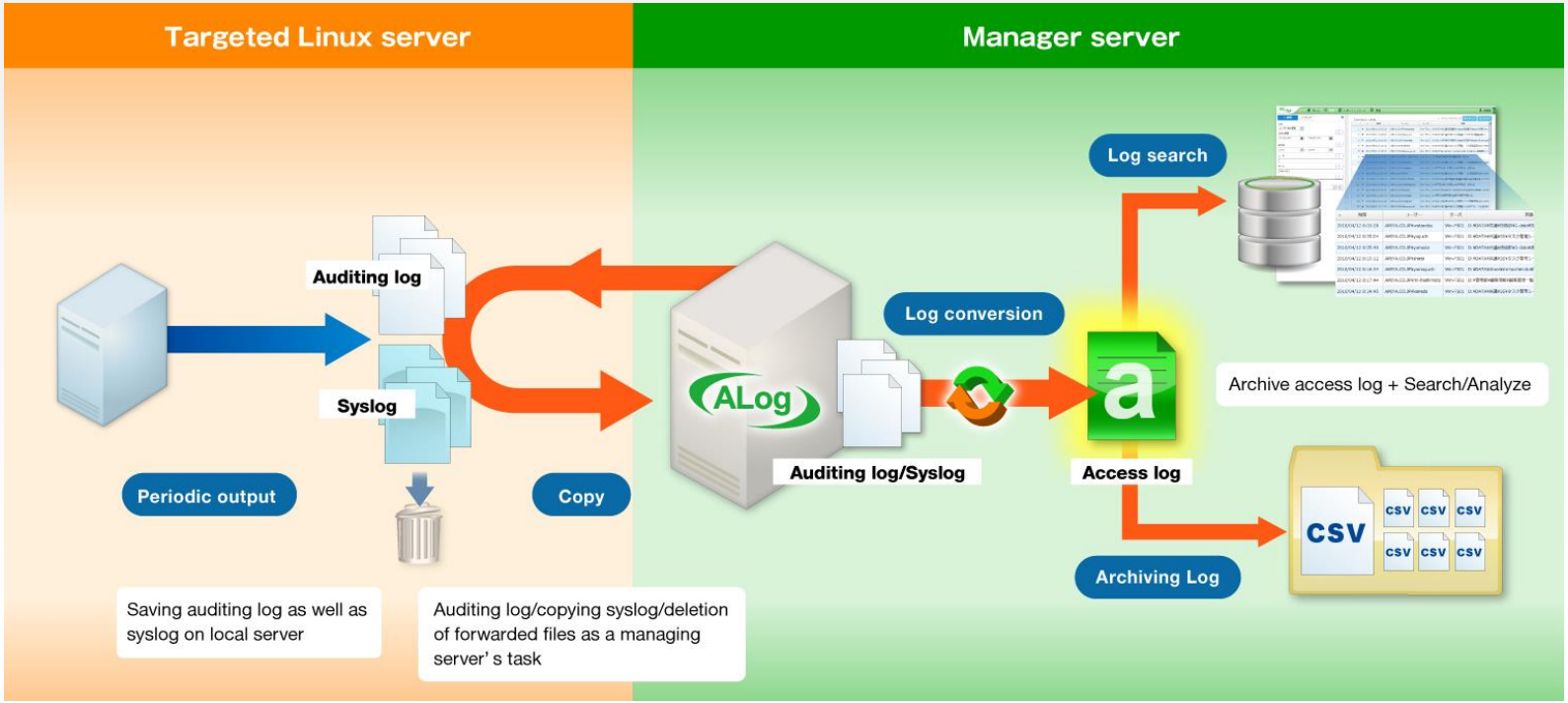


Operation Flow 【for NetApp / EMC / Isilon】



* clustered Data ONTAP outputs logs at 10 minute intervals
* VNX OE（archive mode） outputs logs hourly or by each 1GB.
* In case that a targeted server is Isilon, logs are output by node.
* Any NAS server supports only CIFS log collection and conversion. Please contact in case you want to target NFS logs.

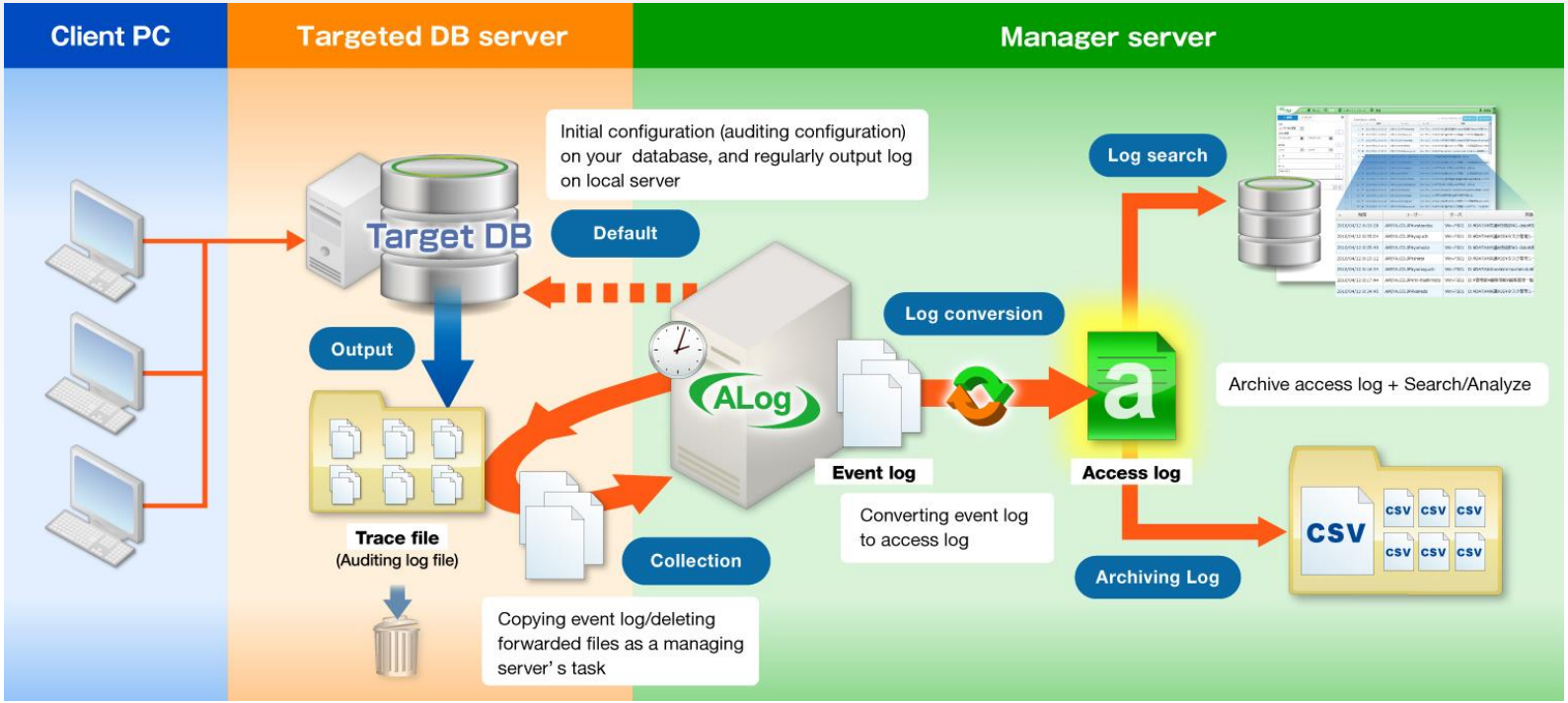
Operation Flow 【for Linux】



*ALog can obtain logs of users/administrator access activity to files, logs of updated access privilege, syslog, command execution logs, and logs of logon/logoff activity.

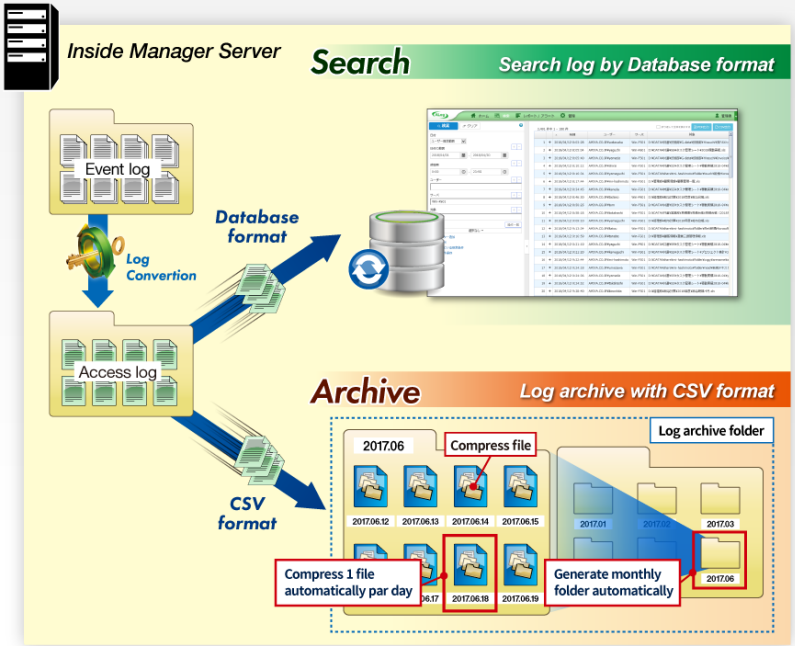
*You need to be able to log in a target Linux server with password. （Public key is not supported.）

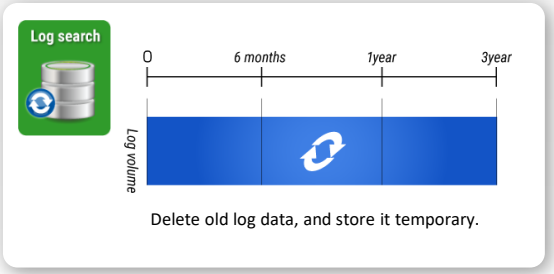
Operation Flow 【for SQL Server / Oracle】

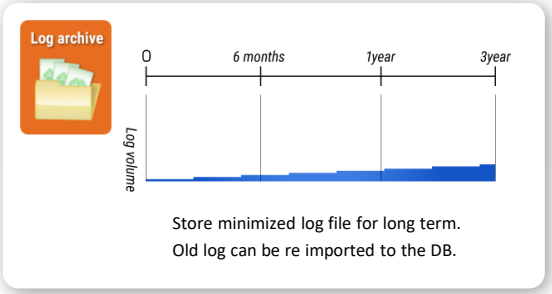


Manager server Architecture

ALog ConVerter is designed to manage logs stored in large quantities for extended periods.
The Manager server component distributes outputs to separate locations in CSV and Database format and realize the **high speed log search functionality** and **large volume log storage**.







Hard ware Requirements - Manager Server

for Windows/for NetApp/for EMC

OS： Windows Server 2008 (x64) / 2008R2 / 2012 / 2012R2 / 2016

*32bit version OS is not supported
*Service pack of each OS(SP)is supported
*Each edition of（Standard / Enterprise / Datacenter）supported
*Virtualized environment (VMWare, Hyper-V, Citrix XenServer)supported.

CPU： Dual Core, or higher (Quad Core or above is recommended)

Memory： 8GB, or higher (16GB, or higher is recommended)

HDD： 500GBor higher disk space.
(Please refer to[HDD calculation ex])

*There is a case that more disk space is required depending on the number of the target server and access log storing term.

Software： .NET Framework 4.5 or later version ※1

Either of following web browser
- Internet Explorer 10 or later version
- Firefox version 40 or later version
- Google Chrome version 44 or later version

Microsoft SQL Server（Only when target server is SQL Server）※2
Oracle Client（ Only when target server is Oracle Database）

HDD calculation example

[Case for Windows case]

prerequisite：1000 parsons access for each 1 server
Daily access times for 1 user is 150 times.
* Normally approximately 100-200 times

CSV file (CAB compression) = 1.5GB / par year

DB file for search = 120GB / par year

Total =122GB per year

[for NetApp case]

prerequisite：1000 parsons access for each 1 server
log data volume for 1 user par day is 15MB

CSV file (CAB compression) = 4.5GB / par year

DB file for search = 360GB / par year

Total =365GB per year

This value was the sample data calculated based on the existing users environment. Please be notified that outputted event log volume will be changed depending on the users environment and server usage Please contact us for the detail.

*To use ALog EVA.net Framework 4.6 or higher is required.
*For SQL server, we are using SQL server function to convert trace log, will require to install same version or higher compare to SQL server.
(ex : IF target server is SQL server 2008, manager server will require to install sql server 2008 or higher version)

Hardware Requirements -Target Server

Target OS for Windows

Windows

OS： Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016
Windows Storage Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016

*Service pack of each OS(SP)is supported
*Each edition of (Standard / Enterprise / Datacenter)
*Virtualized environment (VMWare, Hyper-V, Citrix XenServer) supported.

Software： .NET Framework 2.0 SP1 or above (Only for Agent Type)

Hardware Requirement

- Output target file is required to be NTFS format. (FAT is not supported)
- In the case of log collecting methodology is agent methodology, the ability to write to shared folders hosted from the Manager server through target server.
- It is needed that a manager server access to shared folder on target server
- Client PC OS must be in Windows 7 ／8.1／10 (Only when using Attend Manager)

Hardware requirement -Target server

Target OS for NetApp/for EMC

NetApp

[CIFS]

Data ONTAP 7.0～8.2.5

*Except 7.2.1 ～ 7.2.2p2,7.2.4L1

*The company tested the following version

7.0.1 , 7.0.2 , 7.0.3 , 7.0.4 , 7.0.5 , 7.0.6 , 7.0.7 , 7.1.1 , 7.2 , 7.2.2(p3 or later version) , 7.2.3 , 7.2.4 , 7.2.5.1 , 7.2.6 , 7.2.6.1 , 7.2.7 , 7.3 , 7.3.1 , 7.3.1.1 , 7.3.2 , 7.3.3 , 7.3.4 , 7.3.5 , 7.3.5.1 , 7.3.6 , 7.3.7 , 8.0 , 8.0.1 , 8.0.2 , 8.0.3 , 8.0.5 , 8.1 , 8.1.1 , 8.1.2 , 8.1.3 , 8.1.4 , 8.2 , 8.2.1 , 8.2.2 , 8.2.3, 8.2.4, 8.2.5

clustered Data ONTAP 8.2.4 ～ 9.4

*AMIYA tested the following version

8.2.4 , 8.3 , 8.3.1 , 8.3.2p3 , 9.0 , 9.1 , 9.2 , 9.3 , 9.4

Requirement NetApp

- File area as output location for file access log should be CIFS area.
- In the case of Data ONTAP, rsh command (or SSH command) can be executed from manager server toward target server.
- In the case of clusterd Data ONTAP, ssh command can be executed from manager server toward target server.
- Log format is configure as evtx type(xml type is not supported)
- LDAP authentication for NetApp should be through Active Directory(Using other option then Active Directory for LDAP authentication will cause NTFS file system unable to complete audit configuration and unable to use ALog.)

EMC

VNX OE 7.0.14 ～ 8.1.9

*AMIYA tested the following version

7.0.14.0,7.0.51.3,7.0.54.501,7.0.54.6,7.1.55.31,7.1.65.8,7.1.71.1,7.1.72.1,7.1.76.4,7.1.76.405,7.1.79.8,7.1.80.7,8.1.1.33,8.1.2.51,8.1.3.79,8.1.6.101,8.1.8.121,8.1.9.155

VNXe OE 2.4～3.1

*AMIYA tested the following version

2.4.4.22283,3.1.1.5395470,3.1.1.6207002,3.1.8.9340299

Unity 4.0.0 ～ 4.4

*AMIYA tested the following version

4.0.0,4.0.1,4.0.2,4.1.0,4.1.1,4.1.2,4.2,4.3, 4.4

Requirement EMC

- File area which is targeted to get file access log must be CIFS area
- It is required to use Event Log Auto Archive function

*For product that Maker stops support, or the version is not fully supported, we highly recommend to use maker support product / version..

Hardware requirement -Target server

Target OS for Isilon / Linux

Isilon

OneFS OneFS 7.1.0.4 ～ 8.1.2

*AMIYA tested the following version

7.1.0.4,7.1.0.5,7.1.0.6,7.1.1.1,7.1.1.2,7.1.1.4,7.1.1.5,7.1.1.7,7.1.1.8,7.1.1.9,7.1.1.11,7.2.0,7.2.0.3,7.2.0.4,7.2.1.0,7.2.1.1,7.2.1.2,7.2.1.3,7.2.1.4,7.2.1.5,7.2.1.6,8.0.0,8.0.0.2,8.0.0.3,8.0.0.4,8.0.0.5,8.0.0.6,8.0.0.7,8.0.1,8.0.1.1,8.0.1.2,8.1,8.1.0.1,8.1.0.2,8.1.0.3,8.1.0.4,8.1.1.0,8.1.2

Requirement **Isilon**

・File area which is targeted to get file access log must be CIFS area
(not supported NFS area)

Linux

Red Hat Enterprise Linux 6 / 7

CentOS 6 / 7

*the following types of log are supported

File access log / Access permission change log / syslog /
Command execution log

Requirement **Linux**

・Auditd, sshd, zip, unzip, openssh-clients must be installed
・It is required to login to sshd with password authentication
(Public key authentication is not supported)
・In the case to get syslog, “time”, “host name” and “the other info” must be separated with space
(the initial condition of Linux syslog)
・Log file is text base file, and uncompressed or compressed by zip/gzip format.

Hardware requirement -Target server

Target OS for SQL Server

OS：	Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 *Service pack of each OS(SP)is supported *Each edition of (Standard / Enterprise / Datacenter) *Virtualized environment (VMWare, Hyper-V, Citrix XenServer) supported.
SQL Server：	Microsoft SQL Server 2005 / 2008 / 2008R2 / 2012 / 2014 / 2016 / 2017 *Each edition Express / WorkGroup / Standard / Business Intelligence / Enterprise） supported *Both x86, x64 supported
Software ：	.NET Framework 2.0 SP1 or later version

Hardware Requirement

- Please confirm that remote access to SQL server can be done from ALog server.
- Please confirm that “Stored procedure automatic execution” is permitted.
- If AWE is activated, please confirm that “lock pages in memory” privilege is granted to Windows account that activates SQL Server.
- In the case of log collecting methodology is agent methodology, the ability to write to shared folders hosted from the Manager server through target server.
- It is required that a manager server access to shared folder on target server

Hardware requirement -Target server

Target OS for Oracle

OS：	Windows Server 2008 / 2008R2 / 2012 / 2012R2 / 2016 Red Hat Enterprise Linux 5 / 6 / 7 Oracle Linux 6.8 *UKE is supported　※VMware, Cloud environment is supported
Oracle Database：	Oracle Database 10.1.x / 10.2.x /11.1.x / 11.2.x / 12.1.x / 12.2.x
software：	.NET Framework 2.0 SP1 or later version （in case the OS is Windows and use agent type）

*Please contact us in case you use Solaris or MIRACLE LINUX.

*ALog ConVerter for Oracle suppotrs only RAC clustering.
Please contact us in case you use other clustering methods

*For product that Maker stops support, or the version is not fully supported,
we highly recommend to use maker support product / version..

Supported Log output by each Oracle version

version	Log output
Oracle 10.1.x, 10.2.X	OS/DB
Oracle 11.1.x, 11.2.X	OS/XML/DB
Oracle 12.1.x, 12.2.x	OS/XML/DB

* In the case of event logout put is OS, “RAW_SQL by normal user”
and “The time intervals in milliseconds output” cannot be executed.

Hardware Requirement

-We are using「AUDIT_TRAIL」to configure Audit on Database(if already configured it, current configure maybe modified)
- In the case of log collecting methodology is agent methodology(only supported windows os), the ability to write to shared folders hosted from the Manager server through target server.
- In case of Windows OS It is needed that a manager server access to shared folder on target server
- In case of Linux OS, it is require to use FTP/SFTP server.
- Agent type is only support Windows 64bit OS.