IT Operating Manual

<Service-ID> - ITOM – Manage Engine – AD Audit Plus

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Main IT Service Catalogue Service** | <Service Catalogue ID : X.0.0 > |
| **Related IT Service Catalogue Service(s)** | <Service Catalogue ID : X.0.0 > |
|  | <Service Catalogue ID : X.0.0 > |
|  |  |
| **Prepared by** | < Author of this document> |
| **Date** | <dd.mm.yyyy> |
| **Version** | <V x.y> |
| **Status** | <Draft or Final> |
|  |  |
|  |  |

Content

[Administration 4](#_Toc488915800)

[1 Introduction 4](#_Toc488915801)

[2 Service Description 5](#_Toc488915802)

[2.1 System Layout 5](#_Toc488915803)

[2.2 Functional Layout 5](#_Toc488915804)

[2.3 Design Decisions 5](#_Toc488915805)

[3 Installing the Service 6](#_Toc488915806)

[3.1 Installation Prerequisites 6](#_Toc488915807)

[3.2 Installation 6](#_Toc488915808)

[3.3 Post-Installation Processing 6](#_Toc488915809)

[3.4 Configuration 6](#_Toc488915810)

[3.5 Verifying the Installation 6](#_Toc488915811)

[3.6 Uninstalling the Service 6](#_Toc488915812)

[4 Startup and Shutdown of Service 7](#_Toc488915813)

[4.1 Startup 7](#_Toc488915814)

[4.2 Shutdown 7](#_Toc488915815)

[5 Maintenance 8](#_Toc488915816)

[5.1 Maintenance Activities 8](#_Toc488915817)

[5.2 Frequency 8](#_Toc488915818)

[5.3 Maintenance Windows 8](#_Toc488915819)

[6 Back Up and Restore 9](#_Toc488915820)

[6.1 Redundancy 9](#_Toc488915821)

[6.2 Backup 9](#_Toc488915822)

[6.3 Recovery 9](#_Toc488915823)

[6.4 Data Retention/Archiving 9](#_Toc488915824)

[7 Database Requirements 10](#_Toc488915825)

[7.1 Database Product 10](#_Toc488915826)

[7.2 Configuration 10](#_Toc488915827)

[7.3 Maintenance 10](#_Toc488915828)

[8 Error Messages and Troubleshooting 10](#_Toc488915829)

[9 Security and Controls 11](#_Toc488915830)

[9.1 Security and Controls Concept 11](#_Toc488915831)

[9.2 SOX Requirements 11](#_Toc488915832)

[10 Internal Key User / Business Application Owner 12](#_Toc488915833)

[11 External Support 12](#_Toc488915834)

[12 Service responsibilities / Operational Modell 12](#_Toc488915835)

[12.1 GUS 12](#_Toc488915836)

[12.2 GITO 12](#_Toc488915837)

[12.3 GAD 12](#_Toc488915838)

[12.4 Business 12](#_Toc488915839)

[Solution Architecture Overview 13](#_Toc488915840)

Administration

**Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Change ID | Changes |
| <version> | <dd.mm.yyyy> | <author> | <USU change number stated as CID\_xxxx > | <changes> |
| <version> | <dd.mm.yyyy> | <author> | <USU change number stated as CID\_xxxx > | <changes> |

# Introduction

The purpose of this IT operations manual is to provide all necessary information for proper operation of the service / application.

The intended audience of the operating manual is the IT support organization (GUS / GITO).

# Service Description

## System Layout

## Functional Layout

## Design Decisions

# Installing the Service

## Installation Prerequisites

### System Requirements

**Hardware Requirements**

| **Hardware** | **Recommended** |
| --- | --- |
| Preocessor | P4 - 1.5 GHz or Better |
| RAM | 4 GB or better |
| Disk Space | 50 GB |

Note: The additional disk space used by database will vary depending on the number of Users/Files and audited events captured.

**Software Requirements**

| **Software** | **Support** |
| --- | --- |
| Operating System | Windows Vista and up |
|  | Windows Server 2008 and up |
| Browsers | IE 9 and up, Firefox, Chrome, Edge |
| Resolution | Preferred screen resolution is 1024x768 or higher |
| Databases | SQL Server 2005 and up |

| **Supported Platforms** |
| --- |
| Active Directory 2003 and above |
| Windows File Server 2003 and above |
| NetApp Filer - Data ONTAP 7.2 and above |
| NetApp Cluster - Data ONTAP 8.2.1 and above |
| EMC Storage Systems |
| Windows Security Log Settings |
| Disk Space Management |

### Windows Security Log Settings

ADAudit Plus periodically collects the audit-data from the configured servers and stores  
the information in the database for reporting. To avoid data loss, we recommend the  
below Event Log Settings

| **Operating System of Server** | **Role** | **Security Log Size (Mb)** | **Security Log Retention** |
| --- | --- | --- | --- |
| Windows Server 2003 | Domain Controller | 307.2 | Overwrite Events As Needed |
| Windows Server 2008 and above | Domain Controller | 1048.5 | Overwrite Events As Needed |
| Windows Server 2003 | File Server | 307.2 | Overwrite Events As Needed |
| Windows Server 2008 and above | File Server | 4194.3 | Overwrite Events As Needed |
| Windows Server 2003 | Member Server | 307.2 | Overwrite Events As Needed |
| Windows Server 2008  and above | Member Server | 1048.5 | Overwrite Events As Needed |

### Hard Disk Space Management

As events occur across Domains & Servers, the event logs get filled with data, that are processed for meaningful information (reports /  
forensics) and later archived (save disk space & historical reporting); the disk space required to store the ever growing event log data is  
unique & depends on the number of domain controllers, file servers, workstations...

Disk Space Requirement

The hard disk requirements computation for Active Directory Auditing & File Server Auditing are detailed in the tables below.  
The numbers reached are with a simple calculation based on the number of users, number of days and the approx size of an event log.

**AD Auditing**

| **Number of Users** | **No of Days** | **Total Size** |
| --- | --- | --- |
| 1 | 1 | 15 Kb |
| 10000 | 90 | 15 \* 10000 \* 90 = 13500000 Kb (13 GB) |

**SIG Estimation**(Rough calculation I've done during install)

-**No of Domain Contollers**: 45

-**No of users**: 5000

-**No of Days**: 90

-**Average log size**: 15kb

**Disk Space** : AverageLogSize \* NoOfUsers \* NoOfDays = 15 \* 5000 \* 90 = 6750000 kb = 6.75 GB

**Archive** : DiskSpace/10 = 0.675 GB

**Total Disk Space** = DiskSpace + Archive = aprox 7.5 GB

### File Server Auditing

| **Number of Users** | **No of Files** | **No of Days** | **Total Size** |
| --- | --- | --- | --- |
| 1 | 1 | 1 | 4 Kb |
| 100 | 1 | 1 | 400 Kb |
| 100 | 100 | 1 | 40000 Kb (40 MB) |
| 100 | 100 | 90 | 3.5 GB (40000 \* 90) |
| 100 | 100 | 720 | 29 GB |

**Total Disk Space** =Average Log Size \* No of Users \* No of Files \* No of Days + Archive

Archive = DiskSpace/10

**Disk Space Alerts**

An administrator can configure a threshold value for free disc space. When the free space on the Server goes below the threshold, an alert will be sent to the configured email address.

1. Check size of ev\_temp & temp folder & ensure it is empty or having very few files.
2. Check logs folder size is not more than 1 GB.

## Installation

ADAudit Plus is distributed in the EXE format and available in 32 bit (ADAudit Plus.exe) & 64 bit (ADAudit Plus\_x64.exe) versions for Windows and can be installed in any machine in a Domain

## Post-Installation Processing

ADAudit Plus can be started either in the system account (when run as service) or in the user account (when run as application).

Installing ADAudit Plus as a Service allows it to be started from the system account.

To start ADAudit Plus Service:

Start > Control Panel > Administrative Tools > Services > ManageEngine ADAudit Plus

or

Start > All Programs > ADAudit Plus > Start ADAudit Plus Server

On starting ADAudit Plus, the client is automatically launched in the default browser.

Open a Web browser and type <http://localhost:8081/#/home>  (also saved as bookmark in IE on 627) in the address bar. Here the hostname refers to the DNS name of the machine, where ADAudit Plus is running.

## Configuration

### ADAudit Plus Service Account Configuration

User,Groups and GPO - creation and settings in extra document

### Migrating DB/Data: PostgreSQL/MySQL to MS SQL Migration

By default, ADAudit Plus comes bundled with PostgreSQL database. To move the DB and/or data from PostgreSQL/MySQL to MS SQL, set-up the prerequisites first and then initiate movement.

1. **Configuring the MS SQL server**

* Open the SQL Server Configuration Manager on the computer running the MS SQL instance (to which the DB and/or data is to be moved).  
  In the left pane, click SQL Server Services --> Ensure that the SQL Server Browser is running.  
  In the left pane, click SQL Server Network Configuration --> Select Protocols for (the given instance) --> Enable TCP/IP.

**Note:** The given instance refers to the MS SQL instance to which the DB and/or data is to be moved.

* In the left pane, click SQL Native Client Configuration --> Select Client Protocols for (the given instance) --> Enable TCP/IP.
* Restart the SQL Server Service.

1. **Providing permissions to the MS SQL instance**

The user account associated with ADAudit Plus must have access and appropriate permissions to the MS SQL instance (to which the DB and/or data is to be moved).

**Note:** If SQL Server Autentication is used to move the DB and/or data, access and permissions to the MS SQL instace are automatically provided. However, when Windows Authentication is used, access and permissions have to be granted, as explained below-

To grant access Login to Microsoft SQL Server Management Studio with a sysadmin account, select the server instance to which you will be migrating and check whether the user running ADAudit Plus is on the list.

If the user is not listed create a new login

To grant permissionsfirst check whether the user has sysadmin permission.

If the user does not Select sysadmin in the checkbox and click OK

**Note:** To grant the user only the minimum permissions required instead of sysadmin permission, right click on the user --> Properties --> User Mapping --> Select db\_datareader, db\_datawriter, db\_ddladmin in the checkbox and click OK.

Also, execute the below query in the database: Right click on DB --> New Query -->

GRANT CONTROL ON CERTIFICATE::[ZOHO\_CERT] TO [newly\_created\_user]

1. **Enabling communication with the MS SQL server**

If ADAudit Plus and the MS SQL instance are running on different computers-

Download and install SQL native client (sqlncli.msi), command line utilities (SqlCmdLnUtils.msi), and ODBC Driver (msodbcsql.msi); in the computer on which ADAudit Plus is running.  
Download the above files from the respective MS SQL server feature packs:

* For [2008](https://www.microsoft.com/en-in/download/details.aspx?id=26728)
* For [2012](https://www.microsoft.com/en-in/download/details.aspx?id=35580)
* For [2014](https://www.microsoft.com/en-us/download/details.aspx?id=46696)
* For [2016](https://www.microsoft.com/en-us/download/details.aspx?id=54279)

**Note:** Native client, command line utilities, and ODBC driver version has to be the same as the MS SQL version (to which the DB and/or data is to be moved).

Copy the following 2 files from the MS SQL server installation folder to the ADAudit Plus bin folder:

* bcp.exe- \Tools\Binn\bcp.exe
* bcp.rll- \Tools\Binn\Resources\1033\bcp.rll

**Note:** If ADAudit Plus and the MS SQL instance are running on the same computer copy the following 2 files from the MS SQL server installation folder to the ADAudit Plus bin folder:

* bcp.exe- \Tools\Binn\bcp.exe &
* bcp.rll- \Tools\Binn\Resources\1033\bcp.rll

1. **Opening UDP and TCP ports (applicable only if the firewall is enabled in the MS SQL Server computer)**

UDP port number is 1434.

To find the TCP port number, open SQL Server Configuration Manager on the computer where the MS SQL instance to which the DB and/or data is to be moved, resides. --> SQL Server Network Configuration --> Protocols for . Right click on TCP/IP --> Properties --> IP Addresses --> IPALL --> TCP Port Number.

Open the UDP and TCP ports under firewall settings.

1. **Move DB and/or data**

Stop ADAudit Plus.

Invoke (ADAudit Plus Home)\bin\ChangeDB.bat in command prompt. Make sure that the user running the command prompt is same as the one running ADAudit Plus.

DB Configuration wizard will pop-up --> Select server type as MS SQL --> Select the Host Name, Instance Name, and Database Name. iv. If you want to migrate existing data from the PostgreSQL/MySQL to MS SQL, then select Yes for the Migrate Data option. Otherwise, select No (for a new installation of ADAudit Plus).v. Select the Authentication type. If you have selected Windows Authentication, the credentials are automatically taken. If you have selected SQL Server Authentication, enter the corresponding credentials.

**Note:** If SQL Server Autentication is used to move the DB and/or data, access and permissions to the MS SQL instace are automatically provided. However, when Windows Authentication is used, access and permissions have to be granted, as explained in point 2 under pre-requisites.

Click Test Connection to check whether the credentials are correct.

Click Save.

The migration procedure will start and it will take a few minutes to complete.

## Dashboard View

The Home Tab which is the default Dashboard for ADAudit Plus provides a quick snapshot of essential audit data. Audit data of all configured Domains can be viewed from an intuitive graphic display. The graphic display helps in easier understanding of information from the dashboard view itself.

The display information is grouped by Domains and Desired / Undesired Audit activities like

**Logon Failures** - Graphically represents the logon failures of all users in a domain, with the help of trend-line connecting logon failures on each day.

**Account Management** - Account management includes User, Computer and Group - Creation, Deletion and modification graphically represented with the help of Bar charts on a single interface.

**Logon Failure - Error Code** - The Error code of a logon failure for the last 7 days or 30 days are highlighted with the help of a PIE Chart.

**Logon Peak hour usage** - Trend line of the logon counts at each hour is displayed. This will help in determining the logon peak hour for the past 7 or 30 days.

**Account locked out users** - Bar charts highlight the day to day Account Lockouts in a domain.

**Password Changed /Set Users** - Bar charts highlight the day to day Password Changed or Password Set users.

are displayed on the dashboard by default.

A 7 day or 30 day snapshot from the graphic display makes it easier for an administrator to identify when a desired / undesired audit event has occurred.

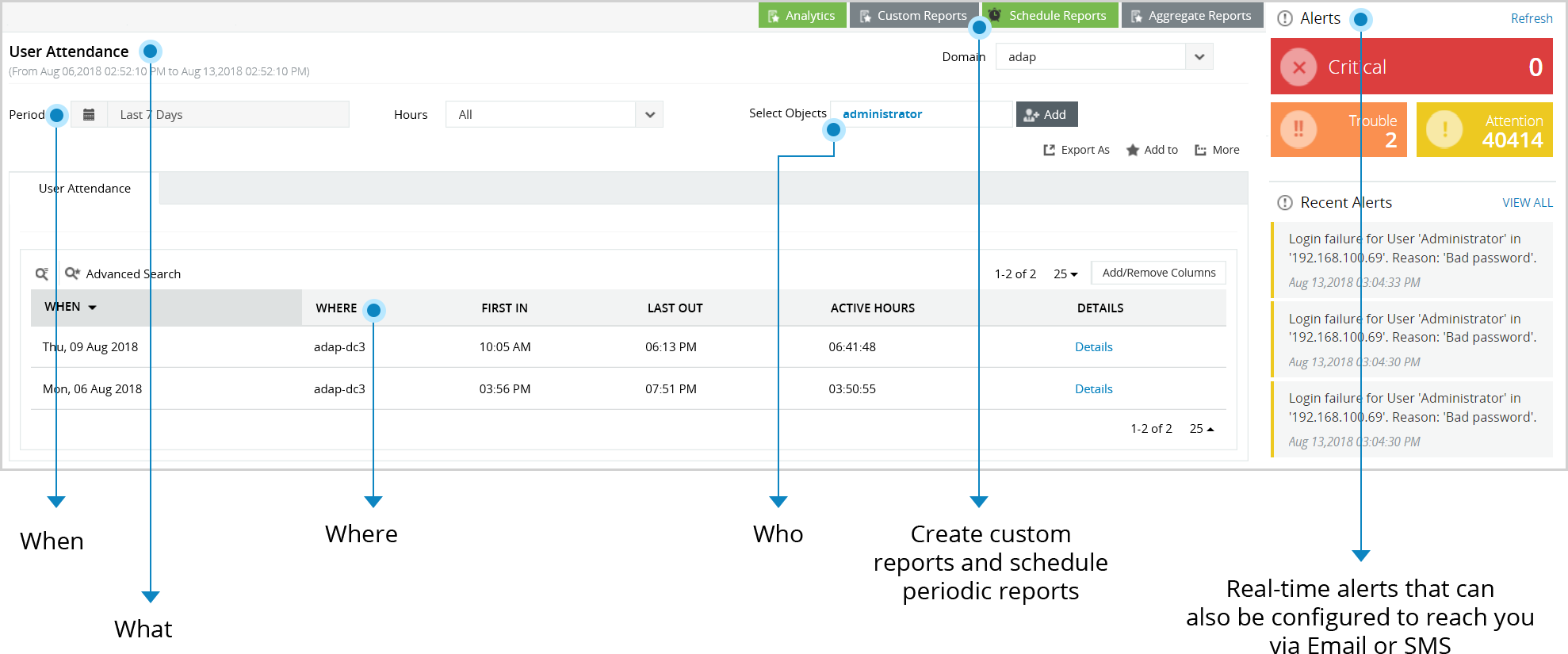
Trend lines for 7 day and 30 days helps easier understanding the trends over a period of time.

Administrators can click on the graphs to view its underlying data.

Any graph can be added to the dashboard via the "+" icon present in them in the reports tab.  
The Home page provides the complete snapshot for all domains configured.

Use the refresh icon for ADAudit Plus to fetch latest data.

# Bird’s-eye view of ADAudit Plus



# Additional Information

## Member servers

Our license does not include member server auditiong.

## Frequency

## Maintenance Windows

# Back Up and Restore

The SIG standard procedures are defined in the “ITGC Document for IT Backup and Restore”

## Redundancy

## Backup

**Windows Operating system**: VMware ESX - Image backup daily incremental

**Windows Data partition**: daily incremental

**Windows SQL:** Agent or Script daily -> see ITOM S.5.3

**AIX Operating system:** MKSYSB weekly

**AIX Data partition:** daily incremental

**AIX Oracle database:** SAP      ->  TSM with backint daily -> see ITOM S.5.1

Non-SAP -> local disk with RMAN daily  -> see ITOM S.5.2

## Recovery

## Data Retention/Archiving

# Database Requirements

**For the configuration and operation of databases the following ITOM's are also valid.**

**The documents describe the SIG standards for databases.**

AIX Oracle SAP database: see ITOM S.5.1

AIX Oracle Non-SAP: see ITOM S.5.2

Windows SQL: see ITOM S.5.3

## Database Product

## Configuration

## Maintenance

# Error Messages and Troubleshooting

**In case of a separate Troubleshooting Guide should be used, please refer to it.**

<Service-ID> - Troubleshooting Guide - <short name IT-Service> - <SiteCode>

# Security and Controls

## Security and Controls Concept

## SOX Requirements

# Internal Key User / Business Application Owner

# External Support

# Service responsibilities / Operational Modell

## GUS

## GITO

## GAD

## Business

Solution Architecture Overview

Include a graphical overview of the solution architecture.

Fügen Sie eine graphische Darstellung der Solution Architecture ein