The Case of Exchange Logs – A Deep Dive

Qasim T. Zaidi[1]

Saudi Arabian Oil Company, Dhahran, Kingdom of Saudi Arabia

Abstract: **This article gives you important guidelines for analyzing the logs of Microsoft Exchange Servers. Microsoft Exchange Server is an On-Premises email service which is often deployed by large organizations to have autonomy over business communication. Logs are an important part of any Information Technology's analysis of any tracking, troubleshooting, and incident handling; email server logs analysis is key to getting to the bottom line faster and more efficiently. While not all logs are useful, some can be very handy for any case and email administrator may be working on. This research paper dives into those critical logs of Exchange Server which every administrator must be familiar with.**

Keywords: **Exchange Server Logs, Log Analysis, Email Service troubleshooting, Client Connectivity, Exchange Commandlet History, Exchange Admin Center.**

I. INTRODUCTION

Microsoft Exchange Server is the most common email service used by organizations on premises. Every email service Administrator often has to track email messages, check client connectivity, perform log analysis and review activity logs. This research paper is intended to provide high level summary of the important logs created by Microsoft Exchange Servers, their location, and how to interpret them thus helping in making conclusive remarks regarding any and all usage of the email service. The paper does not cover every log but the ones which are most commonly needed by email administrators to validate message tracking, verify connectivity, and troubleshoot during an incident.
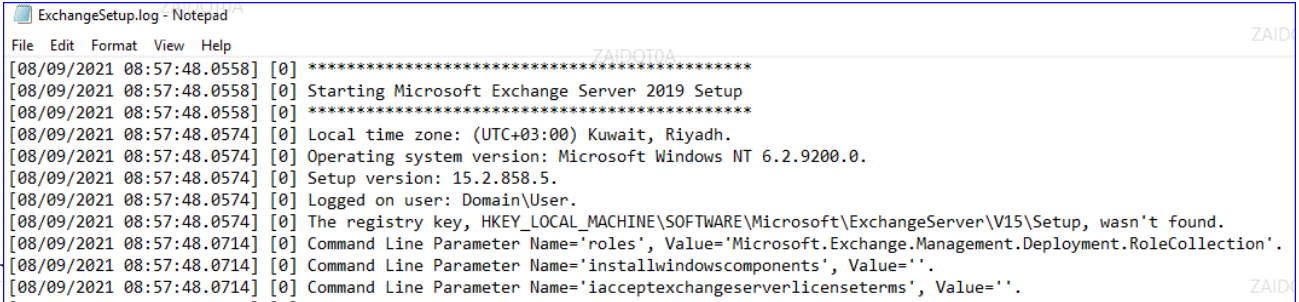
II. LOGS AND HOW TO DECIPHER THEM

Exchange Setup Logs

First and foremost, the Exchange Setup logs are created during the installation of Microsoft Exchange Server. These logs are located in *C:\ExchangeSetupLogs* of a Windows Server, and store valuable information related to the progress of every task during the Exchange installation. System readiness and all activity performed by the Microsoft Exchange Setup is recorded in these logs such as installation progress, components which are installed by the setup files, and configuration changes which are made during the installation. These logs are especially useful if the installation ends prematurely or something goes wrong during the process. Administrators can review these logs and take necessary steps to troubleshoot the issue before re-running the Microsoft Exchange setup. The

Below figure shows first few lines of ExchangeSetup.log with date and time of the start of the setup as well as the user who initiated the installation. Note the Setup version: 15.2.858.5 which refers to Microsoft Exchange Server 2019 CU 9

Fig. I


```
ExchangeSetup.log - Notepad
File  Edit  Format  View  Help
[08/09/2021 08:57:48.0558] [0] ******************************************
[08/09/2021 08:57:48.0558] [0] Starting Microsoft Exchange Server 2019 Setup
[08/09/2021 08:57:48.0558] [0] ******************************************
[08/09/2021 08:57:48.0574] [0] Local time zone: (UTC+03:00) Kuwait, Riyadh.
[08/09/2021 08:57:48.0574] [0] Operating system version: Microsoft Windows NT 6.2.9200.0.
[08/09/2021 08:57:48.0574] [0] Setup version: 15.2.858.5.
[08/09/2021 08:57:48.0574] [0] Logged on user: Domain\User.
[08/09/2021 08:57:48.0574] [0] The registry key, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ExchangeServer\V15\Setup, wasn't found.
[08/09/2021 08:57:48.0714] [0] Command Line Parameter Name='roles', Value='Microsoft.Exchange.Management.Deployment.RoleCollection'.
[08/09/2021 08:57:48.0714] [0] Command Line Parameter Name='installwindowscomponents', Value=''.
[08/09/2021 08:57:48.0714] [0] Command Line Parameter Name='iacceptexchangeserverlicenseterms', Value=''.
```

The version is 15.2.986.5

Fig. II

```
[10/15/2021 07:22:23.0272] [0] *******************************************
[10/15/2021 07:22:23.0283] [0] Starting Microsoft Exchange Server 2019 Setup
[10/15/2021 07:22:23.0283] [0] *******************************************
[10/15/2021 07:22:23.0292] [0] Local time zone: (UTC+03:00) Kuwait, Riyadh.
[10/15/2021 07:22:23.0292] [0] Operating system version: Microsoft Windows NT 6.2.9200.0.
[10/15/2021 07:22:23.0296] [0] Setup version: 15.2.986.5.
[10/15/2021 07:22:23.0297] [0] Logged on user: Domain\User.
```

At the end of the ExchangeSetup.log, the completion is reported. This log provides insight into all steps taken by the Exchange Server installation files and any issues with successful completion.

Fig. III

```
[10/15/2021 09:52:12.0138] [2] Ending processing Set-ServerComponentState
[10/15/2021 09:52:12.0139] [2] Beginning processing Write-ExchangeSetupLog
[10/15/2021 09:52:12.0144] [2] Install is complete.  Server state has been set to Active.
[10/15/2021 09:52:12.0144] [2] Ending processing Write-ExchangeSetupLog
[10/15/2021 09:52:12.0145] [1] Finished executing component tasks.
[10/15/2021 09:52:12.0154] [1] Ending processing Start-PostSetup
[10/15/2021 09:52:12.0155] [0] The Exchange Server setup operation completed successfully.
```

Message Tracking Logs

Message tracking logs are a valuable source of information for any Exchange administrator. Message tracking logs record the email message activity as it flows through the transport layer. The logs are detailed with many valuable and common attributes such as sender, recipient, message subject, date/time, message id, connectors, server names etc. These logs not only show the path an email message took from a user submitting it to delivery to the intended recipient, but also show the success and failure of the delivery in form of different events i.e. Deliver and Fail or Drop.

While email Administrators rely on Exchange command let of **Get-MessageTrackingLog** which takes many parameters to search for a particular criterion, these logs are stored on each transport layer in *C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking* and are of the form MSGTRKYYYYMMDDHH.LOG. For instance, MSGTRK2023020804-1.LOG is message tracking log for mail flow on an Exchange Server during 2023, Feb 08 at 0400 hours.

The structure of Message Tracking log file is

#Software: Microsoft Exchange Server

#Version: 15.02.0986.037

#Log-type: Message Tracking Log

#Date: 2023-02-08T04:00:04.344Z

#Fields: date-time,client-ip,client-hostname,server-ip,server-hostname,source-context,connector-id,source,event-id,internal-message-id,message-id,network-message-id,recipient-address,recipient-status,total-bytes,recipient-count,related-recipient-address,reference,message-subject,sender-address,return-path,message-info,directionality,tenant-id,original-client-ip,original-server-ip,custom-data,transport-traffic-type,log-id,schema-version

The data in the log is read as

date-time	08T04:00:04.390Z
client-ip	fe80::53c0:3370:6093:103d
client-hostname	Server.Domain.com
server-ip	fe80::53c0:3370:6f90:103d%5
server-hostname	ServerName

source-context	MDB:xxxxx, Mailbox:xxxx, Event:51734158, MessageClass:IPM.Note, CreationTime:2023-02-08T04:00:04.238Z, ClientType:MOMT, SubmissionAssistant:MailboxTransportSubmissionEmailAssistant, ServerMdbConnectionId:xxxx
connector-id	
source	STOREDRIVER
event-id	RECEIVE
internal-message-id	156759
message-id	<9aaacb2477b54171b558efa68bc5b22b@domain.com>
network-message-id	73e477a5-6a09-4b91-20d3-08db0988f59c
recipient-address	Recipient-email-address@domain.com
recipient-status	To
total-bytes	14396
recipient-count	1
related-recipient-address	
reference	
message-subject	RE: SBB
sender-address	senders-email-address@domain.com
return-path	senders-email-address@domain.com
message-info	04I:
directionality	Originating
tenant-id	
original-client-ip	<Client IP Address>
original-server-ip	<Server IP Address>
custom-data	S:MailboxDatabaseGuid=xx-xx-xx;S:DeliveryPriority=Normal;S:AccountForest=ROOT.Domain
transport-traffic-type	Email
log-id	37fa6cfa-7dee-4fc3-20d3-08db0988f59c
schema-version	15.02.0986.037

SMTP Receive and SMTP Send Logs

SMTP stands for Simple Mail Transfer Protocol. All email on the internet use SMTP to transport from one mail server to another. Applications and Printers may also use this protocol within an organization to send emails to recipients. Exchange Servers keep logs of all SMTP activity and details including the sender's IP address, sender's email address, recipient's email address and so on.

SMTP Receive logs are stored in *C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd\ ProtocolLog\SmtpReceive* as RECVYYYYMMDDHH-1.LOG whereas SMTP Send logs are available in *C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\FrontEnd\ProtocolLog\SmtpSend* as SENDYYYYMMDDHH -1.LOG

The format of these logs is:

#Software: Microsoft Exchange Server

#Version: 15.0.0.0

#Log-type: SMTP Receive Protocol Log   -or-   SMTP Send Protocol Log

#Date: 2023-02-08T05:00:02.060Z

#Fields: date-time,connector-id,session-id,sequence-number,local-endpoint,remote-endpoint,event,data,context

The data in the log is read as:

date-time	2021-10-22T05:45:04.722Z	2021-10-22T05:45:04.722Z	2021-10-22T05:45:04.722Z	2021-10-22T05:45:04.722Z	2021-10-22T05:45:04.723Z
connector-id	Client Proxy Send Connector	Client Proxy Send Connector	Client Proxy Send Connector	Client Proxy Send Connector	Client Proxy Send Connector
session-id	08D98FC209415028	08D98FC209415028	08D98FC209415028	08D98FC209415028	08D98FC209415028
sequence-number	3	4	5	5	6
local-endpoint	LocalServerIP:31929	LocalServerIP:31929	LocalServerIP:31929	LocalServerIP:31929	LocalServerIP:31929
remote-endpoint	ReceivingServerIP:465	ReceivingServerIP:465	ReceivingServerIP:465	ReceivingServerIP:465	ReceivingServerIP:465
event	>	<	>	>	<
data	EHLO Server.Domain.com	250 Server.Domain.com Hello [ServerIP] SIZE 37748736 PIPELINING DSN ENHANCEDSTATUS CODES STARTTLS X-ANONYMOUSTLS AUTH GSSAPI NTLM X-EXPS GSSAPI NTLM 8BITMIME BINARYMIME CHUNKING XEXCH50 SMTPUTF8 XRDST XSHADOWREQUEST	X-ANONYMOUSTLS	X-ANONYMOUSTLS	220 2.0.0 SMTP server ready
context					

IIS Logs

Microsoft Exchange server installs Internet Information Service (IIS) as the email servers offer web based services such as Outlook Web App and Exchange Web Service amongst others. The IIS stores its logs for any activity in *C:\Inetpub\logs\Logfiles* folder, divided into subfolders of W3SVC1, W3SVC2 and so on. As the name suggests, W3SVC1 means world wide web service 1 and is the front-end web service. Similarly, W3SVC2 is the second service component and is the back-end of the web service. Both of these IIS log files contain all the GET and POST requests that are made. It also includes basic items such as IP and username, request date and time, service status and number of bytes received, as well as detailed items of target files.

The structure of IIS log file looks like the below

#Software: Microsoft Internet Information Services 10.0

#Version: 1.0

#Date: 2021-06-13 06:15:10

#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-substatus sc-win32-status time-taken

Fig. IV

The above figure shows GET and POST calls made to the IIS service on the Exchange Server with response of 401 or 200. This data can help troubleshoot common issues related to client connectivity, offline address book, Outlook Web App and many other type of requests supported by the Exchange Server.

Exchange Control Panel Logs

Exchange Servers also provide a web-based management interface known as Exchange Admin Center (EAC) or Exchange Control Panel (ECP). This page is hosted within Internet Information Service of the Exchange Server as a virtual directory. All actions taken on this page are recorded in activity logs of ECP in the following location *C:\Program Files\Microsoft\ Exchange Server\V15\Logging\ECP\Activity* as ECPActivity_2724_YYYYMMDD-1.LOG

The structure of ECP logs are:

#Software: Microsoft Exchange Server

#Version: 15.0.0.0

#Log-type: ECP Activity Context Log

#Date: 2021-11-13T00:01:18.295Z

#Fields: TimeStamp,ServerName,EventId,EventData

In the below figure of the ECP log, an administrator Admin1 is creating a new user mailbox in ECP. Similarly, all activities performed in the Exchange Control Panel are recorded in these log files stored on the Exchange Servers.

Fig. V

```
2021-11-13T01:47:36.658Z,
EXCHANGE,Request,S:PSA=<PII>Admin1@Domain.com</PII>;S:FE=EXCHANGE.DOMAIN.COM;S:URL=https://exchange.domain.com:444/
ecp/UsersGroups/NewMailboxOnPremises.aspx?pwmcid=3&ReturnObjectType=1
(https://exchange.domain.com/ecp/UsersGroups/NewMailboxOnPremises.aspx?
pwmcid=3&ReturnObjectType=1);S:Bld=15.1.1713.5;S:ActID=3bbbf798-1dc1-40f8-a56b-0611baa1065d;Dbl:BudgUse.T
[]=7.00040006637573;I32:ADS.C[DC]=1;F:ADS.AL[DC]=1.592;I32:ATE.C[DC.domain.com]=0;F:ATE.AL
[DC.domain.com]=0;S:WLM.Bal=2.147484E+09;Dbl:WLM.TS=259
```

Exchange PowerShell History Logs

Exchange Servers provide Exchange Management Shell (EMS), a PowerShell interactive environment to run commands for any activity such as get values, set values, modify values etc. of a mailbox, distribution group, mailbox database and any object available to Exchange. The activity of commands run in EMS are logged in *C:\Program Files\Microsoft\Exchange Server\V15\Logging\CmdletInfra\LocalPowerShell\Cmdlet* and have file names in the format of powershell.exe_155704_Cmdlet_YYYYMMDDHH-1.LOG.

The structure of these logs is:

#Software: Microsoft Exchange Server

#Version: 15.02.0986.037

#Log-type: Rps Cmdlet Logs

#Date: 2023-02-08T07:28:01.971Z

#Fields:
DateTime,StartTime,RequestId,ClientRequestId,MajorVersion,MinorVersion,BuildVersion,RevisionVersion,ServerHost

Name,ProcessId,ProcessName,ThreadId,CultureInfo,Organization,AuthenticatedUser,ExecutingUserSid,EffectiveOrganization,UserServicePlan,IsAdmin,ClientApplication,Cmdlet,Parameters,CmdletUniqueId,UserBudgetOnStart,ContributeToFailFast,RunspaceSettingsCreationHint,ADViewEntireForest,ADRecipientViewRoot,ADConfigurationDomainControllers,ADPreferredGlobalCatalogs,ADPreferredDomainControllers,ADUserConfigurationDomainController,ADUserPreferredGlobalCatalog,ADuserPreferredDomainControllers,ThrottlingInfo,DelayInfo,ThrottlingDelay,IsOutputObjectRedacted,CmdletProxyStage,CmdletProxyRemoteServer,CmdletProxyRemoteServerVersion,CmdletProxyMethod,ProxiedObjectCount,CmdletProxyLatency,OutputObjectCount,ParameterBinding,BeginProcessing,ProcessRecord,EndProcessing,StopProcessing,BizLogic,PowerShellLatency,UserInteractionLatency,ProvisioningLayerLatency,ActivityContextLifeTime,TotalTime,ErrorType,ExecutionResult,CacheHitCount,CacheMissCount,GenericLatency,GenericInfo,GenericErrors,ObjectGuid,ExternalDirectoryOrganizationId,ExternalDirectoryObjectId,NonPiiParameters

The figure below shows different commands run in the Exchange Management Shell on an Exchange server

Fig. VI

2023-02-08T05:04:55.822Z,2023-02-08T05:04:55.738Z,f5ec1f6b-ab27-4359-a2bb-2aed1c9c4b1a,,15,2,986,37,ExchangeServer,129976,powershell.exe,10,,,,,,,,,Get-TransportService
2023-02-08T05:04:56.095Z,2023-02-08T05:04:55.847Z,04936413-38a0-43bf-a959-da114b949ae2,,15,2,986,37,ExchangeServer,129976,powershell.exe,10,,,,,,,,,Get-OrganizationConf
2023-02-08T05:04:59.488Z,2023-02-08T05:04:58.984Z,e5a5e8fa-94e9-4831-8eac-bff7615237a7,,15,2,986,37,ExchangeServer,129976,powershell.exe,10,,,,,,,,,Test-ServiceHealth,"
2023-02-08T05:05:00.056Z,2023-02-08T05:05:00.045Z,7312a6b6-c9ef-40b0-828d-b075ad6ab7dd,,15,2,986,37,ExchangeServer,129976,powershell.exe,10,,,,,,,,,Get-ClientAccessArra
2023-02-08T05:05:00.123Z,2023-02-08T05:05:00.071Z,1a2273b0-2c83-4ca1-b565-84a7cbe25880,,15,2,986,37,ExchangeServer,129976,powershell.exe,10,,,,,,,,,Get-MailboxServer,"-
2023-02-08T05:05:00.917Z,2023-02-08T05:05:00.131Z,bc74363a-72bb-4235-aafb-f23470b41a06,,15,2,986,37,ExchangeServer,129976,powershell.exe,10,,,,,,,,,Get-DatabaseAvailabi
2023-02-08T05:05:08.931Z,2023-02-08T05:05:00.956Z,7a84a88e-e96d-4e5c-850c-f33b6adbd986,,15,2,986,37,ExchangeServer,129976,powershell.exe,10,,,,,,,,,Get-MailboxDatabase,

Exchange Administrative Audit Logs

Exchange Admin Audit Logs show the operational activities that were performed in Exchange. The logs record everything from creating a new Database Availability Group (DAG) or removing a Mailbox database, creating, removing, or modifying mailbox properties, putting the Exchange server in maintenance mode, and so on. These logs are located in C:\Program Files\Microsoft\Exchange Server\V15\Logging\CosmosQueue and have a similar filename such as audit20221004-4.

The structure of these logs is:

#Software: Microsoft Exchange

#Version: 15.02.0986.037

#Log-type: audit

#Date: 2023-02-04T02:57:40.759Z

#Fields:
Timestamp,Server,TenantId,RecordType,Data,UserKey,RecordId,Operation,Workload,ResultStatus,Version,Scope

The figure below shows Administrative actions such as Mount-Database, Set-Mailbox, New-Mailbox, and associated objects such as the users the operation was performed on etc.

Fig. VII

"{""CreationTime"":""2022-10-04T13:29:11"",""Id"":""5dfba6f1-20c4-489f-0f2d-08daa60c6cad"",""Operation"":""Mount-Database"",""OrganizationId""
"{""CreationTime"":""2022-10-04T15:48:50"",""Id"":""92b8a041-b8d9-43ce-75f2-08daa61fee8a"",""Operation"":""Set-Mailbox"",""OrganizationId"":""
"{""CreationTime"":""2022-10-04T15:49:43"",""Id"":""5d20741f-b96e-4788-8545-08daa6200e46"",""Operation"":""New-Mailbox"",""OrganizationId"":""
tted>""]}]",NT AUTHORITY\SYSTEM (MSExchangeHMHost),5d20741f-b96e-4788-8545-08daa6200e46,New-Mailbox,Exchange,True,1,Online
"{""CreationTime"":""2022-10-04T18:01:40"",""Id"":""9ad837a6-dd63-4e15-afa1-08daa6327d0d"",""Operation"":""Set-Mailbox"",""OrganizationId"":""
"{""CreationTime"":""2022-10-04T18:13:42"",""Id"":""7c96c5d6-af89-411d-3305-08daa6342bd2"",""Operation"":""New-DatabaseAvailabilityGroup"",""O
"{""CreationTime"":""2022-10-04T18:17:03"",""Id"":""d1b91413-b6d2-4d58-29e1-08daa634a374"",""Operation"":""Set-Mailbox"",""OrganizationId"":""
"{""CreationTime"":""2022-10-04T18:26:40"",""Id"":""57bea2ef-3ce4-442a-c39c-08daa635fb33"",""Operation"":""Remove-DatabaseAvailabilityGroup"",
"{""CreationTime"":""2022-10-04T18:35:38"",""Id"":""a01b9f54-77f6-4d98-5afe-08daa6373bd0"",""Operation"":""Remove-DatabaseAvailabilityGroup"",
"{""CreationTime"":""2022-10-04T18:42:07"",""Id"":""934e6770-0ac0-41a4-3a88-08daa63823f1"",""Operation"":""Remove-DatabaseAvailabilityGroup"",
"{""CreationTime"":""2022-10-04T18:45:16"",""Id"":""ef2ffa60-cb5e-4a8f-7e15-08daa638945f"",""Operation"":""Add-DatabaseAvailabilityGroupServer
"{""CreationTime"":""2022-10-04T20:15:59"",""Id"":""8c93505f-a592-45eb-aaf7-08daa645409c"",""Operation"":""Set-ServerComponentState"",""Organi

III.   CONCLUSION

Email service Administrators are required to understand logging capabilities of the Microsoft Exchange Server. While this research paper does not review all types of logs created by the Exchange Server, it highlights key components of the values logged by different components and the ability to decipher them. The research paper is intended to provide high level summary of the important logs created by Microsoft Exchange Servers, their location, and how to interpret them thus helping in making conclusive remarks regarding any and all usage of the email service. By successfully reviewing the information stored in these logs for any activity, email administrators can validate message tracking, verify connectivity, and troubleshoot scenarios to conclusively arrive at outcomes.

REFERENCES

[1]   Location of Exchange Server Logs, https://support.microfocus.com/kb/doc.php?id=7019070

[2]   Transport Logs in Exchange Server, https://learn.microsoft.com/en-us/exchange/mail-flow/transport-logs/transport-logs?view=exchserver-2019

[3]   Message Tracking, https://learn.microsoft.com/en-us/exchange/mail-flow/transport-logs/message-tracking?view=exchserver-2019

[4]   Connectivity logging in Exchange Server https://learn.microsoft.com/en-us/exchange/mail-flow/transport-logs/connectivity-logging?view=exchserver-2019

[5]   How to use administrator audit logging in Exchange Server, https://learn.microsoft.com/en-us/exchange/policy-and-compliance/admin-audit-logging/admin-audit-logging?view=exchserver-2019.