How to Leverage User Access Logging for Forensic Investigations

crowdstrike.com/blog/user-access-logging-ual-overview/

Patrick Bennett

June 8, 2021

CrowdStrike analysts recently began researching and leveraging User Access Logging (UAL), a newer forensic artifact on Windows Server operating system that offers a wealth of data to support forensic investigations. UAL has proven beneficial to help correlate an account and the source IP address with actions performed remotely on systems.

To help your investigations, this blog post provides an overview of UAL databases and offers examples of interpreting the treasure trove of data that they contain.

What Is User Access Logging?

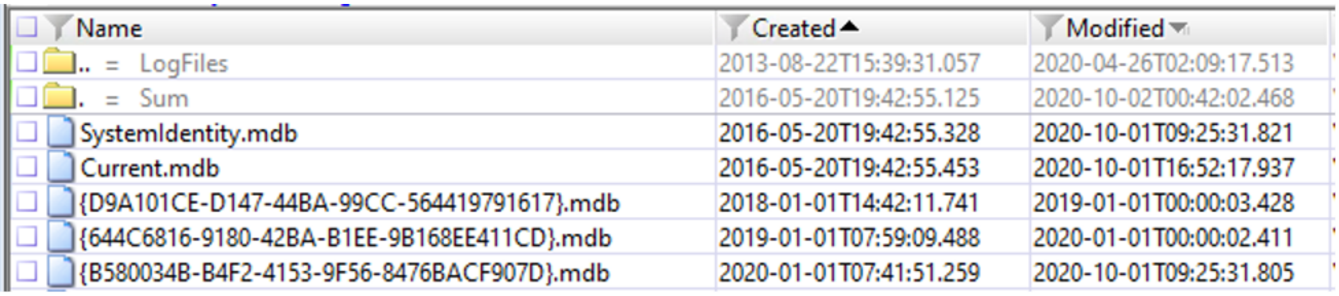
UAL is a feature included by default in Server editions of Microsoft Windows, starting with Server 2012. As defined by Microsoft, UAL is a feature that “logs unique client access requests, in the form of IP addresses and user names, of installed products and roles on the local server.”

This means that UAL records user access to various services running on a Windows Server. The access is logged to databases on disk that contain information on the type of service accessed, the user account that performed the access and the source IP address from which the access occurred. One key element of UAL is that each record is based on the combination of username, source IP and service accessed — so it’s naturally suited for identifying anomalous or rare access to a system.

With default settings, this information is retained for up to three years. Naturally, this data can be extremely valuable in forensic investigations. Unfortunately, there’s a marked lack of awareness of this type of artifact in the digital forensic community. Many forensic solutions do not parse these databases, and therefore threat analysts could potentially miss data relevant to an investigation.

Where to Find UAL Data

UAL database files are stored under the directory C:\Windows\System32\LogFiles\Sum. Inside this directory, you'll find up to five Extensible Storage Engine (ESE) database files with .mdb extensions. The screenshot in Figure 1 provides an example of what the contents might look like.



Name	Created	Modified
.. = LogFiles	2013-08-22T15:39:31.057	2020-04-26T02:09:17.513
. = Sum	2016-05-20T19:42:55.125	2020-10-02T00:42:02.468
SystemIdentity.mdb	2016-05-20T19:42:55.328	2020-10-01T09:25:31.821
Current.mdb	2016-05-20T19:42:55.453	2020-10-01T16:52:17.937
{D9A101CE-D147-44BA-99CC-564419791617}.mdb	2018-01-01T14:42:11.741	2019-01-01T00:00:03.428
{644C6816-9180-42BA-B1EE-9B168EE411CD}.mdb	2019-01-01T07:59:09.488	2020-01-01T00:00:02.411
{B580034B-B4F2-4153-9F56-8476BACF907D}.mdb	2020-01-01T07:41:51.259	2020-10-01T09:25:31.805

Figure 1. C:\Windows\System32\LogFiles\Sum sample contents

The files shown above include:

- Current.mdb (UAL database — current year; active copy)
- <GUID>.mdb (UAL database — current year)
- <GUID>.mdb (UAL database — previous year)
- <GUID>.mdb (UAL database — two years prior)
- Systemidentity.mdb (database containing information about the server, including a map of RoleGuid values to Role names – more on this below)

The Current.mdb file contains UAL data for the current year, while the two previous years are stored in .mdb files with GUID-style filenames. Per Microsoft:

"UAL makes a copy of the active database file, current.mdb, to a file named GUID.mdb every 24 hours. On the first day of the year, UAL will create a new GUID.mdb. The old GUID.mdb is retained as an archive. After two years, the original GUID.mdb will be overwritten."

This means there can be up to three years of historical data stored on the UAL (i.e., data from the previous year, two years prior and the current year up to the present).

Following the above, Current.mdb and the GUID-style files contain the same set of tables. These files will include the CLIENTS table, where some of the juiciest forensic data is stored — this is where you'll find the historical records of users accessing various services.

Table 1 shows a sample record from the CLIENTS table. Please note that some of the fields are omitted for visibility (see Appendix for a full listing of all tables and fields in the UAL databases).

RoleGuid	TotalAccesses	InsertDate	LastAccess	Address	AuthenticatedUserName
10a9226f-50ee-49d8-a393-9a501d47ce04	1	2019-03-12T18:06:56Z	2019-03-12T18:06:56Z	0a0a0cc8	DOMAIN\User1

Table 1. Sample UAL CLIENTS table record

In the above example, the UAL record indicates that the user DOMAIN\User1 accessed the system via SMB on 2019-03-12 at 18:06:56 UTC, coming from the source IP address 10.10.12.200.

The source IP address is stored in the **Address** field in hexadecimal (0a 0a 0c c8 = 10 10 12 200). The **InsertDate** field contains the UTC timestamp of the first access for the year for the combination of user, RoleGuid and source IP. **LastAccess** is similar but represents the most recent access for the year.

The **TotalAccesses** value of 1 indicates that this was the only access for the year (again, based on the combination of user, source IP and RoleGuid). If access occurred on additional days between the **InsertDate** and **LastAccess**, the total count would be included in this field. In addition, a daily count of the number of accesses per day would be included in additional fields named **Day1** up to **Day366**, which represent the day of the year the access occurred (see Appendix for more details). Unfortunately, a full timestamp is only included for **InsertDate** and **LastAccess** — nothing in between. But as will be shown, this is plenty.

The **RoleGuid** field represents the type of service that was accessed. In this case, it was 10a9226f-50ee-49d8-a393-9a501d47ce04, which corresponds with what is known as the File Server Role. This typically represents SMB access, though it's possible other protocols may be logged here as well.

RoleGuid values are mapped to human-readable Role Names in the SystemIdentity.mdb database, under the ROLE_IDS table. Table 2 shows a sample ROLE_IDS table.

RoleGuid	ProductName	RoleName
c50fcc83-bc8d-4df5-8a3d-89d7f80f074b	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Active Directory Certificate Services
b4cdd739-089c-417e-878d-855f90081be7	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Active Directory Rights Management Service
48eed6b2-9cdc-4358-b5a5-8dea3b2f3f6a	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	DHCP Server
7cc4b071-292c-4732-97a1-cf9a7301195d	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	FAX Server
10a9226f-50ee-49d8-a393-9a501d47ce04	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	File Server
bbd85b29-9dcc-4fd9-865d-3846dcba75c7	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Network Policy and Access Services
7fb09bd3-7fe6-435e-8348-7d8aefb6cea3	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Print and Document Services
d6256cf7-98fb-4eb4-aa18-303f1da1f770	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Web Server
4116a14d-3840-4f42-a67f-f2f9ff46eb4c	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Windows Deployment Services
d8dc1c8e-ea13-49ce-9a68-c9dca8db8b33	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Windows Server Update Services
c23f1c6a-30a8-41b6-bbf7-f266563dfcd6	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	FTP Server
910cbaf9-b612-4782-a21f-f7c75105434a	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	BranchCache
952285d9-edb7-4b6b-9d85-0c09e3da0bbd	0997dbd9-4db4-49aa-8ec5-8f5c6ae1c870	Remote Access

Table 2. Sample ROLE_IDS table

A Note on Roles

The Roles referenced by UAL data are tied directly to Server Roles installed on Windows Server systems. This is done via the Server Manager application, by clicking on Manage → Add Roles and Features.

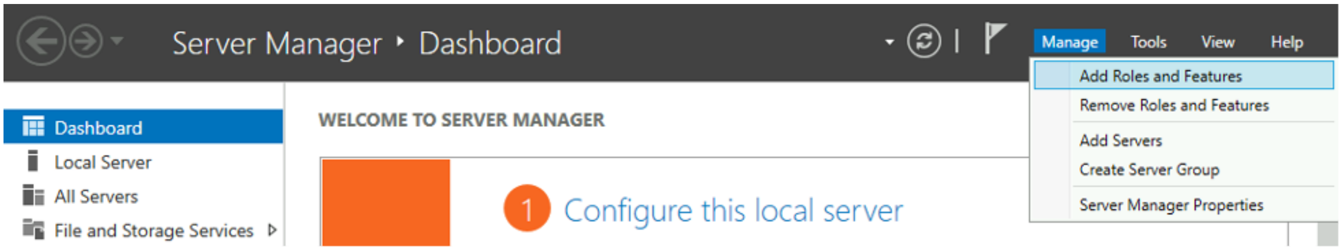
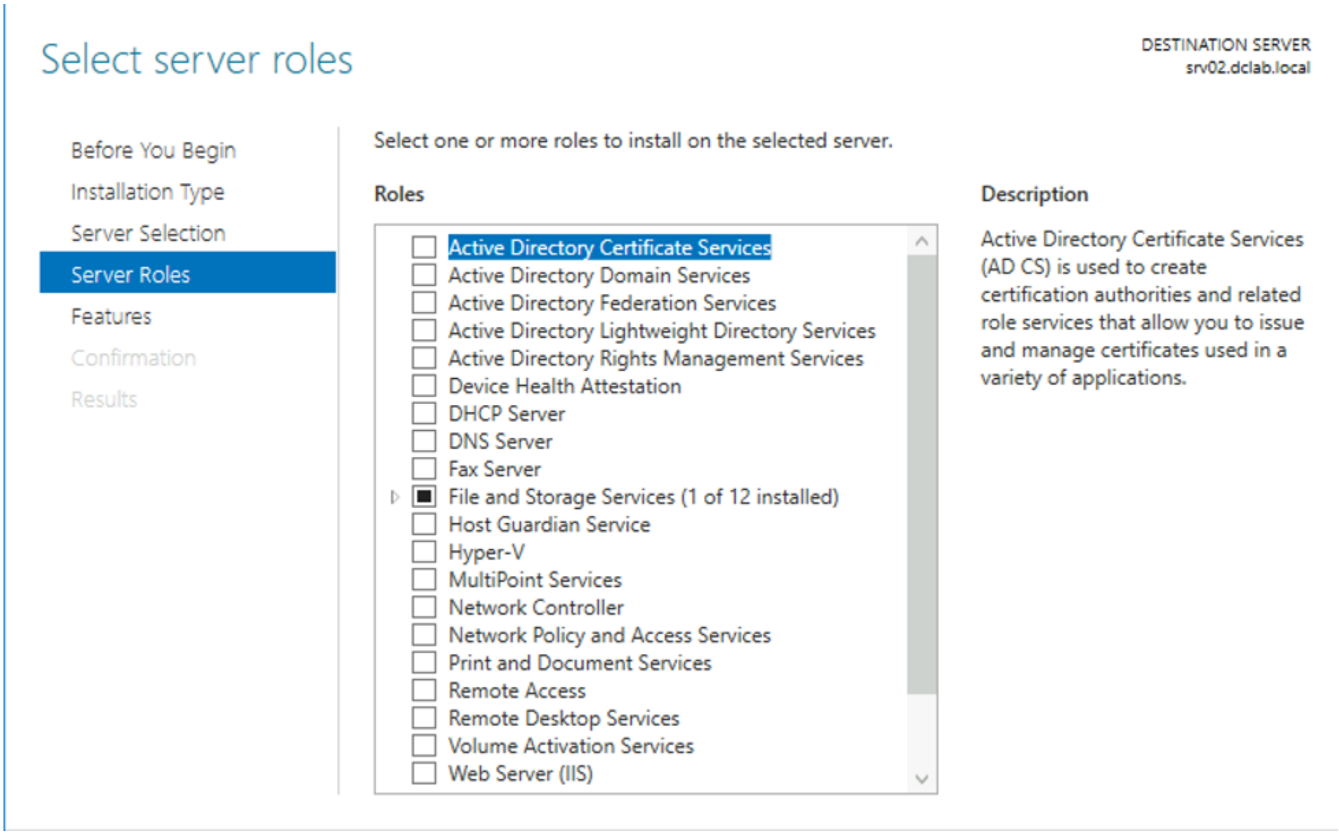

Server Manager ▸ Dashboard
Manage
Tools
View
Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services ▷
WELCOME TO SERVER MANAGER
1 Configure this local server

Figure 2. Server Manager Roles and Features menu

This will bring up a menu that lists available Roles that can be installed, which will look similar to what's shown in Figure 3.



Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▷ ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)

Description

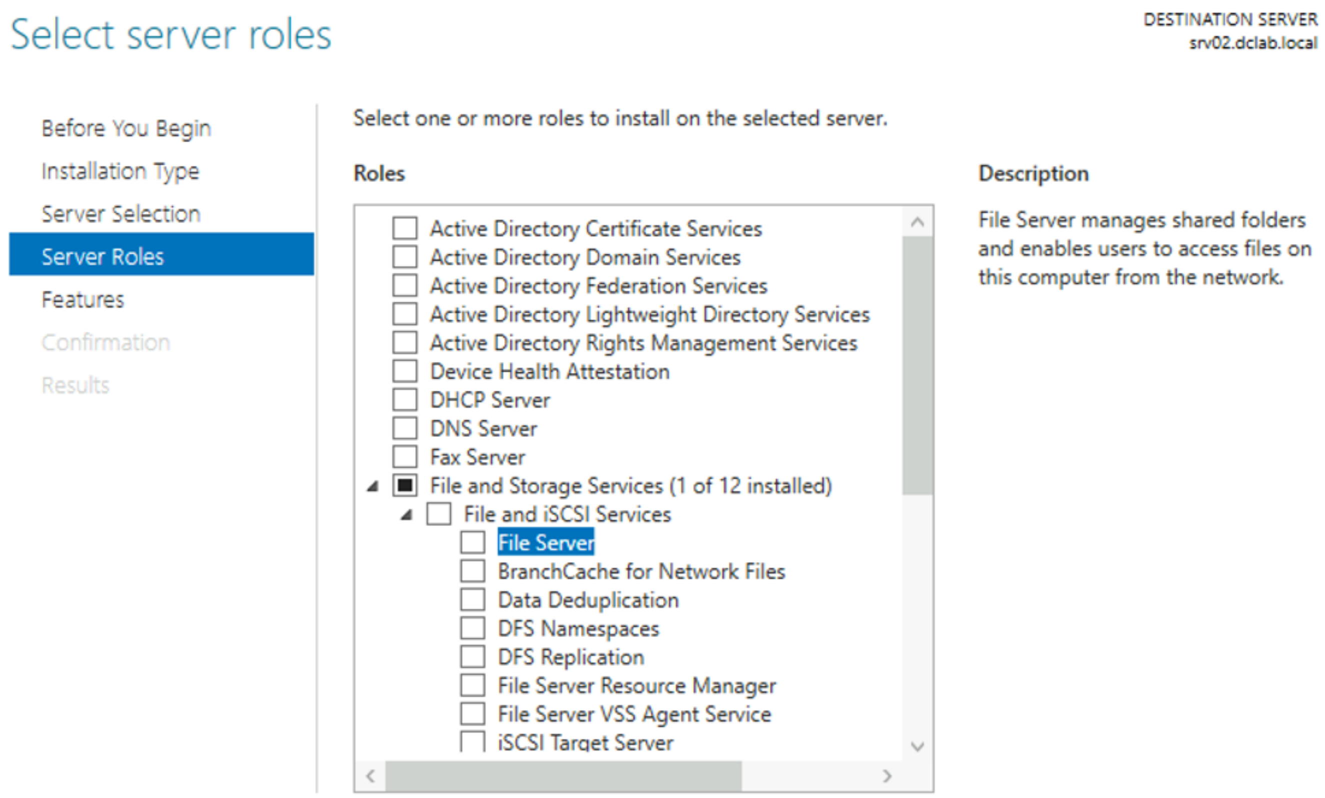
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Figure 3. Server Manager Server Roles menu

Certain Roles are included in the ROLE_IDS table by default, regardless of whether or not they are enabled. Other Roles may get added to the bottom of the ROLE_IDS table when they are installed via the Server Manager. For example, when making a server into a Domain Controller, one would install the **Active Directory Domain Services** Role, at which point this server would be added to the bottom of the ROLE_IDS table, and access under this Role would start being logged in the CLIENTS table. However, not every installed Role will necessarily end up being tracked by UAL.

File Server Role

From a forensic perspective, one of the most fruitful Roles in UAL analysis is the **File Server** Role. It can be found as a subitem under File and Storage Services in the Server Manager menu.



Select server roles

DESTINATION SERVER
srv02.dclab.local

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- Confirmation
- Results

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
  - □ File and iSCSI Services
    - □ File Server
    - □ BranchCache for Network Files
    - □ Data Deduplication
    - □ DFS Namespaces
    - □ DFS Replication
    - □ File Server Resource Manager
    - □ File Server VSS Agent Service
    - □ iSCSI Target Server

Description

File Server manages shared folders and enables users to access files on this computer from the network.

Figure 4. File and Storage Services

As shown in Figure 4, Microsoft notes that the File Server Role “manages shared folders and enables users to access files on [a] computer from the network.” The consequence is that SMB access is logged in UAL databases under the **File Server** RoleGuid. This means UAL databases potentially contain up to three years of historical SMB access. This data can be extremely valuable during investigations, as we’ll demonstrate in the next section.

It’s important to note that this SMB logging includes when, for example, a user maps a file share and performs actions that use SMB under the hood, including SMB named pipes. For example, remotely interacting with a service using sc.exe will result in File Server UAL entries on the target system, because an SMB named pipe (\\.\PIPE\svcctl) is used. Similarly, a UAL File Server entry for a user doesn’t necessarily mean that the user purposefully used SMB.

As a side note, even if the File Server Role is not explicitly enabled, SMB access will still be logged by UAL (as long as the firewall rules to allow SMB access are enabled). When the File Server Role is installed, these firewall rules are automatically enabled.

Interpreting UAL Data

Let’s step through some quick examples to demonstrate just how powerful UAL analysis can be. Please note that the following data is simulated, but this information is very similar to what you’d see in real-world scenarios when analyzing UAL data.

In this first example, we’re analyzing a system called WEBSRV01. We already know that PsExec was used to execute the malicious file C:\Windows\malware.exe on 2020-11-04 at 19:53:08 UTC through analysis of host artifacts. However, all event logs have rolled and were not forwarded elsewhere. We’re trying to understand which user account executed PsExec targeting WEBSRV01 and from which system the activity originated. After parsing the UAL CLIENTS table (from the 2020 database file), the following results are returned.

RoleGuid	TotalAccesses	InsertDate	LastAccess	Address	AuthenticatedUserName
10a9226f-50ee-49d8-a393-9a501d47ce04	686	2020-01-01T05:16:43Z	2020-12-31T23:30:33Z	::1	WEBSRV01\Administrator

10a9226f-50ee-49d8-a393-9a501d47ce04	942	2020-01-12T13:11:46Z	2020-12-31T23:41:31Z	10.20.49.101	CORP\WEBSVC
10a9226f-50ee-49d8-a393-9a501d47ce04	14	2020-03-23T07:50:48Z	2020-12-08T12:22:43Z	10.15.100.249	CORP\lstevens
10a9226f-50ee-49d8-a393-9a501d47ce04	35	2020-03-23T08:30:01Z	2020-12-12T03:48:12Z	10.20.100.100	CORP\lstevens-adm
10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-08-12T23:42:08Z	2020-08-12T23:42:08Z	10.15.100.103	CORP\rsmith
10a9226f-50ee-49d8-a393-9a501d47ce04	3	2020-11-04T19:53:07Z	2020-11-04T19:53:08Z	10.20.49.201	CORP\banderson
10a9226f-50ee-49d8-a393-9a501d47ce04	33	2020-11-12T02:01:42Z	2020-12-30T15:28:07Z	10.20.115.32	CORP\CORPSVC
10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-13T13:03:13Z	2020-11-13T13:03:13Z	10.20.100.142	WERSRV01\Administrator
10a9226f-50ee-49d8-a393-9a501d47ce04	273	2020-12-01T18:46:12Z	2020-12-25T04:00:00Z	10.1.73.48	CORP\hconway

Table 3. Sample CLIENTS table

The first thing that immediately jumps out is the row related to the account CORP\banderson that has a **LastAccess** value matching precisely the time of PsExec usage identified via other artifacts. This record's address value is 10.20.49.201, meaning the activity originated from a device with this IP. We also note that the **TotalAccesses** value is 3. This means that for all of 2020, the CORP\banderson account only accessed WEBSRV01 via SMB from this IP address three times — and what's more, all three occurred around the time of the PsExec activity (because all of the accesses would have occured between the **InsertDate** and **LastAccess** times).

Another anomaly in the above is we have the local Administrator account for WEBSRV01 accessing it from the IP address of another system. Based on the **TotalAccesses** value, this is a rare activity, having only occurred once in 2020, with all of the other local Administrator access coming from localhost.

UAL at Scale

Things get even more exciting when you start pulling UAL at scale from many systems at once. Even simply sorting the output by **InsertDate** can quickly identify suspicious activity. When aggregating CLIENTS table data from multiple systems, it's not uncommon to observe scenarios similar to the example in Table 4.

System Name	RoleGuid	TotalAccesses	InsertDate	LastAccess	Address	AuthenticatedUserName
APPSRV01	10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-30T14:26:17Z	2020-11-30T14:26:17Z	10.20.52.40	CORP\abcsvc
APPSRV02	10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-30T14:26:17Z	2020-11-30T14:26:17Z	10.20.52.40	CORP\abcsvc

DC01	10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-30T14:26:17Z	2020-11-30T14:26:17Z	10.20.52.40	CORP\abcsvc
FILESRV01	10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-30T14:26:18Z	2020-11-30T14:26:18Z	10.20.52.40	CORP\abcsvc
FILESRV02	10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-30T14:26:18Z	2020-11-30T14:26:18Z	10.20.52.40	CORP\abcsvc
WEBSRV01	10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-30T14:26:19Z	2020-11-30T14:26:19Z	10.20.52.40	CORP\abcsvc
WEBSRV02	10a9226f-50ee-49d8-a393-9a501d47ce04	1	2020-11-30T14:26:19Z	2020-11-30T14:26:19Z	10.20.52.40	CORP\abcsvc

Table 4. Sample UAL data from multiple systems

In this example, the account CORP\abcsvc accessed eight systems in rapid succession via SMB, coming from the IP address 10.20.52.40. Further, in each case the **TotalAccesses** value is 1, meaning this was the only time for the year that this account accessed each system via SMB from the source IP address.

When combined with other indicators to pivot from, UAL analysis at scale can help drive the direction of the investigation. For example, if there is a known compromised user account, UAL analysis can quickly identify other (Server 2012+) systems that the account accessed, by searching for records where the **AuthenticatedUserName** value matches the compromised user name.

Similarly, if there is a system that's known to be compromised, analyzing UAL at scale can provide rapid insights into threat actor lateral movement activities. This can be accomplished by finding UAL entries where the **Address** field matches the IP address of the compromised system. This can quickly provide an overview of which accounts a threat actor was using from the compromised server, as well as systems targeted for lateral movement. (Did we mention this data is retained for up to 3 years by default?)

Armed with pivot points like these as a starting point, one can quickly glean critical insights from UAL data. Even without any other indicators to go on, it's possible to spot anomalous activity by looking out for rare combinations of user, source IP address and RoleGuid via the **TotalAccesses** field.

Correlating UAL Data

Correlating UAL data with other artifacts can also help fill in the blanks when event log data is unavailable. An investigation timeline populated via host artifact analysis may yield something like that shown in Table 5.

System Name	Timestamp	Event	Details
APPSRV01	2020-12-01T04:10:50Z	File created	C:\Windows\malware.exe
APPSRV02	2020-12-01T04:10:50Z	File created	C:\Windows\malware.exe
DC01	2020-12-01T04:10:50Z	File created	C:\Windows\malware.exe
FILESRV01	2020-12-01T04:10:51Z	File created	C:\Windows\malware.exe
FILESRV02	2020-12-01T04:10:51Z	File created	C:\Windows\malware.exe

WEBSRV01	2020-12-01T04:10:52Z	File created	C:\Windows\malware.exe
WEBSRV02	2020-12-01T04:10:52Z	File created	C:\Windows\malware.exe

Table 5. Sample timeline before UAL enrichment

By adding UAL data to the timeline and sorting by timestamp, everything falls into place, as shown in Table 6.

System Name	**Timestamp**	**Event**	**Details**
APPSRV01	2020-12-01T04:10:50Z	UAL entry	RoleGuid: File Server | AuthenticatedUserName: CORP\rsmith-adm | Address: 10.100.2.201 | TotalAccesses: 1
APPSRV01	2020-12-01T04:10:50Z	File created	C:\Windows\malware.exe
APPSRV02	2020-12-01T04:10:50Z	UAL entry	RoleGuid: File Server | AuthenticatedUserName: CORP\rsmith-adm | Address: 10.100.2.201 | TotalAccesses: 1
APPSRV02	2020-12-01T04:10:50Z	File created	C:\Windows\malware.exe
DC01	2020-12-01T04:10:50Z	UAL entry	RoleGuid: File Server | AuthenticatedUserName: CORP\rsmith-adm | Address: 10.100.2.201 | TotalAccesses: 1
DC01	2020-12-01T04:10:50Z	File created	C:\Windows\malware.exe
FILESRV01	2020-12-01T04:10:51Z	UAL entry	RoleGuid: File Server | AuthenticatedUserName: CORP\rsmith-adm | Address: 10.100.2.201 | TotalAccesses: 1
FILESRV01	2020-12-01T04:10:51Z	File created	C:\Windows\malware.exe
FILESRV02	2020-12-01T04:10:51Z	UAL entry	RoleGuid: File Server | AuthenticatedUserName: CORP\rsmith-adm | Address: 10.100.2.201 | TotalAccesses: 1
FILESRV02	2020-12-01T04:10:51Z	File created	C:\Windows\malware.exe
WEBSRV01	2020-12-01T04:10:52Z	UAL entry	RoleGuid: File Server | AuthenticatedUserName: CORP\rsmith-adm | Address: 10.100.2.201 | TotalAccesses: 1
WEBSRV01	2020-12-01T04:10:52Z	File created	C:\Windows\malware.exe
WEBSRV02	2020-12-01T04:10:52Z	UAL entry	RoleGuid: File Server | AuthenticatedUserName: CORP\rsmith-adm | Address: 10.100.2.201 | TotalAccesses: 1
WEBSRV02	2020-12-01T04:10:52Z	File created	C:\Windows\malware.exe

Table 6. Sample timeline after UAL enrichment

After adding UAL data, we can now clearly see that malware.exe was copied to all of these systems by CORP\rsmith-adm; and that this activity originated from the IP address 10.100.2.201. Aside from subsequently focusing analysis efforts on that system, you can also identify additional systems of interest by searching the aggregated UAL data for entries with matching **Address** or **AuthenticatedUserName** values from around the same timeframe.

UAL Analysis Tools

On live systems, analysts can access UAL data via PowerShell cmdlets or WMI. In image analysis, UAL databases can be parsed with any tool that supports parsing ESE databases, such as esedbexport, which is part of Joachim Metz's libesedb project.

At least two recently developed solutions are used for parsing UAL data from a forensic perspective: Eric Zimmerman's SumECmd and Brian Moran's KStrike. These tools add value by automatically converting RoleGuids to Role Names and automatically parsing the **Address** field to a human-readable IP address.

More to Come

These examples are only a tiny glimpse into the many powerful applications of UAL data in forensic investigations. The forensic analysis of UAL databases can provide exceptional insights to the forensic analyst. Currently, it's an understudied artifact that's also under-represented by forensic tools. We hope that this information is helpful for your analyses; additional research and testing are needed to learn more about this artifact and the valuable insights it can provide.

Appendix: UAL Databases and Tables

Here is a description of all tables included with the UAL database files.

Current.mdb (and <GUID>.mdb files)

CLIENTS

As mentioned, this table stores the heart of the UAL data. It includes the information on user accounts accessing services on the server. Each row is based on the combination of user + source IP + RoleGuid. (In other words, if a user accesses a system via SMB from two different source IP addresses, each will get their own row). The CLIENTS table includes nine fields.

Field Name	Description
AuthenticatedUserName	Domain\User account performing the access. Can include local accounts and domain accounts, including computer accounts.
Address	Source IP address from which access occurred. Can include IPv4 or IPv6, as well as localhost values.
RoleGuid	The type of service accessed. RoleGuids are mapped to Role names in SystemIdentity.mdb.
InsertDate	UTC timestamp of the first access for the year
LastAccess	UTC timestamp of the most recent access for the year
TotalAccesses	Count of accesses for the year (based on RoleGuid + AuthenticatedUserName + Address)
Day1 … Day366	Count of accesses per day for each day of the year
TenantId	Have seen this populated in relation to the Active Directory Domain Services RoleGuid, but interpretation is unclear. Microsoft defines it as "a unique GUID for a tenant client of an installed role or product that accompanies the UAL data, if applicable."
ClientName	Unknown, have not seen it populated in the wild

Table 7. CLIENTS table fields

DNS

The DNS table contains historical IP to hostname mappings. It appears this table is only populated if the server being analyzed has the DNS Server Role installed. The hostnames and IPs are likely related to clients of the DNS server, but more research is needed to determine what specifically causes this table to be populated. This table can aid in determining previous IP addresses associated with systems in instances where DHCP logs are not available. The DNS table includes three fields.

Field Name	Description
LastSeen	UTC timestamp
Address	IP address
HostName	Hostname associated with the IP address

Table 8. DNS table fields

ROLE_ACCESS

The ROLE_ACCESS table contains a high-level view of the types of Roles that have been accessed on the system, and when the first and last accesses occurred. It contains three fields.

Field Name	Description
RoleGuid	RoleGuid value (associated with human-readable Role Name in SystemIdentity.mdb)
FirstSeen	UTC timestamp of the earliest access to the Role type for the year
LastSeen	UTC timestamp of the most recent access to the Role type for the year

Table 9. ROLE_ACCESS table fields

VIRTUALMACHINES

The VIRTUALMACHINES table contains information on HyperV virtual machines running on the system. As of this writing, we have not come across it populated in the wild. It contains the following fields:

Field Name
VmGuid
BIOSGuid
CreationTime
LastSeenActive
SerialNumber

Table 10. VIRTUALMACHINES table fields

SystemIdentity.mdb

ROLE_IDS

As mentioned, the ROLE_IDS table contains a mapping of RoleGuid values to human-readable Role Names. It includes three fields.

Field Name	Description
RoleGuid	RoleGuid (GUID value)
ProductName	Typically related to the OS edition, it can be GUID value or human-readable. Microsoft defines as "*The name of the software parent product, such as Windows, that is providing UAL data.*"
RoleName	Human-readable Role Name for the RoleGuid

Table 11. ROLE_IDS table fields

CHAINED_DATABASES

This table provides a mapping associated with the year for storing the <GUID>.mdb files. Each row contains two fields.

Field Name	Description
Year	Year associated with database filename (e.g., 2021)
Filename	Database filename associated with the year

Table 12. CHAINED_DATABASES table fields

SYSTEM_IDENTITY

This table contains information related to the operating system and hardware of the system. It contains the following fields, most of which are self-explanatory.

Field Name	Field Name
CreationTime	OSSuiteMask
PhysicalProcessorCount	OSProductType
CoresPerPhysicalProcessor	SystemManufacturer
LogicalProcessorsPerPhysicalProcessor	SystemProductName
MaximumMemory	SystemSerialNumber
OSMajor	SystemDNSHostName
OSMinor	SystemDomainName
OSBuildNumber	OSSerialNumber
OSPlatformId	OSCountryCode
ServicePackMajor	OSLastBootUpTime

Table 13. SYSTEM_IDENTITY table fields

One interesting aspect of the SYSTEM_IDENTITY table is that it appears to have a new entry created each time one of the fields changes. For example, when changing a system's hostname or domain, a new row will be created showing the new **SystemDNSHostName** and **SystemDomainName,** while the old data will still be available in previous rows. The LastBootUpTime field will then only continue to be updated for the latest row. Table 14 provides an example of this.

CreationTime	SystemDNSHostName	SystemDomainName	LastBootUpTime
2020-02-12T15:06:23.632Z	DESKTOP-A3F2BCF9	WORKGROUP	20210315092316.243752+000
2020-03-15T10:06:12.742Z	WEBSRV01	CORP	20211207021136.195304+000

Table 14. Sample SYSTEM_IDENTITY table data

Links

- *Microsoft TechNet page on UAL: https://docs.microsoft.com/en-us/windows-server/administration/user-access-logging/get-started-with-user-access-logging*
- *Microsoft TechNet page on Server Roles: https://docs.microsoft.com/en-us/windows-server/administration/server-core/server-core-roles-and-services*
- *UAL PowerShell cmdlets: https://docs.microsoft.com/en-us/powershell/module/useraccesslogging/?view=windowsserver2019-ps*