

Administration Auditing

Chris Cobbold

24/03/2021



Contents



- **Introduction to Administration Auditing**
- **Setup/Viewing Screens in X3**
- **Capturing Information**
- **Demo Scenaio**
- **More Information**
- **Q & A**

Introduction

Introduction



The X3 application utilises the MongoDB for :-

1. The storage of Administration Module data
2. Syracuse user information
3. Batch server configuration from V11

It is a free (community edition) no-SQL database – instance, collections, documents

When to and Why Collect Data



Enable this feature if :-

Users are notifying of problems with X3 - performance issues, reports not showing correct data, session disconnects

New users have been added to the application

A new requirement to regularly import/export data

Authentication changes , security updates, certificates etc

The auditing will allow you to keep track of who made specific changes within administration and when.

Information Gathering



AUDITING: tells us "who did what and when" (e.g who accessed user information)

PROFILING: collects information about "what, when and how information was queried + how much time it took + what was DB engines solution" (Primarily used for performance issues)

LOGGING: is higher level information telling what DB did and when. When client makes/closes connection, new index is created, data is replicated, engine errors happened (e.g what specific error messages are seen)

Setup/Viewing Information in X3

Global Settings - History Log



sage X3 Super administrator Super administrator X3ERP12_SEED

All > Administration > Administration > Settings

Settings

General settings Authentication Proxy Mailer CTI Service Licence Logs Patch Synchronisation **History** Global variables

History

History maximum days: 365

Maximum number of days to keep history records.

History log

8 Records Page size: 50

Code	Description	Enable
authoring	Personalization	✘
collaborationArea	Teams, documents and storage, Office integration	✘
exportData	Export data	✘
importData	Import data	✘
pages	Navigation : dashboards, vignettes, menus, pages	✘
statusAndUsage	System status and logs, maintenance actions	✘
technicalSettings	Setup servers, endpoints, schedulers and authentication	✘
users	Users, groups and roles management	✔

Admin/ Usage/ Logs



sage X3 Super administrator Super administrator X3ERP12_SEED

All > Administration > Usage > Logs

History logs

130 Records Page size: 20

Created on	Created by	Operation	Entity name	Value
10/02/2021 16:48	admin	Modified	<u>user</u>	ukadmin
09/02/2021 10:41	admin	Modified	<u>setting</u>	Global settings
08/02/2021 16:06	admin	Created	<u>user</u>	chris
08/02/2021 15:02	admin	Modified	<u>group</u>	Runtime users
08/02/2021 14:58	admin	Created	<u>group</u>	Runtime users
08/02/2021 14:58	admin	Modified	<u>user</u>	carol
08/02/2021 14:56	admin	Modified	<u>group</u>	Super administrators
21/12/2020 10:43	admca	Modified	<u>user</u>	admca
21/12/2020 10:42	admin	Created	<u>user</u>	admca
21/12/2020 10:37	admin	Modified	<u>group</u>	Super administrators
21/12/2020 09:35	ukadmin	Modified	<u>user</u>	tommy
21/12/2020 09:35	ukadmin	Modified	<u>user</u>	thierry

[Index](#) [Home](#)

MongoDB Traceability

[Administration Page](#) [Application/Contract](#) [Syracuse/Collaboration](#) [Class](#) *historyLog* [Representation](#) *historyLog*

Principles of traceability

The administrator can decide to follow modifications in the MongoDB database made by users over a period of time. The entities to follow are chosen in [global settings](#) and for any modification to these entities, a log with modified attributes will be written to the database.

History log view - query

This menu displays all operations made to your entities.
Every operation on a tracked entity will be displayed with :

Created on

The date time when the entity has been modified

Created by

The login of user that did the modification

Operation

The type of operation

1. Created
2. Modified
3. Deleted

You can follow different groups of entities:

Group	Description	Entities
authoring	Personalization	PageDef
collaborationArea	Teams, documents and storage, Office integration	team, document, documentTag, documentTagCategory, msoMailMergeDocSel, msoReportMode, msoWordTemplateDocument, msoExcelReportMode, msoExcelTemplateDocument
exportData	Export data	exportProfile, personalizationManagement, resourcePack
importData	Import data	importTool, x3UserImport, profileMenuImport
pages	Navigation : dashboards, vignettes, menus, pages	mobileApplication, mobileMigrateDashboard, mobileDashboard, mobileDashboardVignette, mobileGadget, mobileGadgetParam, navigationPage, landingPage, menuModule, menuItem, menuBlock, menuSubblock, menuCategory
statusAndUsage	System status and logs, maintenance actions	automate
technicalSettings	Setup servers, endpoints, schedulers and authentication	Globalsettings, localePreference, proxyConfiguration, ldap, oauth2, SAML2, notificationServer, boProfile, certificate, caCertificate, application, endPoint, host, x3solution, boServer, hrmServer, hrmSite, storageVolume
users	Users, groups, and role management	group, role, user

The history log configuration entities are always logged, whether the `technicalSetting` group is enabled or not.

Global variables

This block is used to set global variables. These variables are usually set automatically and we highly recommended that you **do not change them manually**.

Capturing Information

Auditing



Auditing within MongoDB itself can be enabled if you have the 'Enterprise Edition' of the product available.

It provides the ability to audit events in these areas :-

Authentication and Authorization

Create/Read/Update/Delete operations etc

with additional filtering for granularity by collection

Can be configured to audit to the console or output a JSON file to a specific destination

Auditing



ps Sage Bookmarks Home Sage University UKI File sharing Dashbo... MyX3 Sage Knowledgebase Chatter Home | Sal... LinkedIn Learning... K Knova Sage Learning Imported »

mongoDB | Documentation ▾ SERVER DRIVERS CLOUD TOOLS GUIDES Get MongoDB Search Documentation

Available only in [MongoDB Enterprise](#) and [MongoDB Atlas](#).

Audit Message

The [event auditing feature](#) can record events in JSON format. To configure auditing output, see [Configure Auditing](#).

The recorded JSON messages have the following syntax:

```
{
  atype: <String>,
  ts : { "$date": <timestamp> },
  local: { ip: <String>, port: <int> },
  remote: { ip: <String>, port: <int> },
  users : [ { user: <String>, db: <String> }, ... ],
  roles: [ { role: <String>, db: <String> }, ... ],
  param: <document>,
  result: <int>
}
```

Field	Type	Description
atype	string	Action type. See Audit Event Actions, Details, and Results .
ts	document	Document that contains the date and UTC time of the event, in ISO 8601 format.

Profiling



Information is recorded in a document collection called `system.profile` – Primarily used for monitoring performance but can be used for any administration maintenance

Is enabled by the Mongo shell command :-

```
Db.setProfilingLevel(level) - level can be 0(off), 1(slow operations), 2(all operations)
```

It's status can be determined by:-

```
Db.getProfilingStatus()
```

Key fields recorded in the collection are

`ns` – name space `op` – operation `query.$query` – query clause `nreturned` – stats `query.id` – record being operated on e.g the information command

```
Db.getCollection('system.profile').find({}, {op:1, ns:1, ts:1})
```

Logging



All > Administration > Administration > Settings

Settings

General settings Authentication Proxy Mailer CTI Service Licence **Logs** Patch Synchronisation History

Enable web client logs **Web client logs I...** Error

Server logs
Expand all

Code	Description	Level
login		
memory	Memory usage information	Info
notifications	Notification service	Error
orm	Object-relational mapping	
factory	Syracuse entity management	Error
mongodb	MongoDB interactions	Info
rights	Entity rights	Error
x3	X3 entity management	Error
patch	Patch integration	Error
pubsub	Publish/Subscriber messaging	Error
sage rr		Error

Mongo Export



Used to export a Mongo collection to an external JSON file

Easier interpretation and review of information

Export command can be run from the Mongo shell

Can use a free Mongo utility GUI such as Robo 3T to view collections

Tracking Admin Changes - Demo

Demo Scenario



Objective: To find information regarding an administration change to a User

Ensure Global Settings History Logs are set to Enable for the Users group

Ensure Global Settings Logs – Orm/Mongodb set to Debug

Ensure Mongo profiling level is set to 2 `db.setProfilingLevel(2)`

Login to X3 as User: Admin

Add a new Security Group to User : Tabatha called - erpfull

Note: Data capturing methods can be used in non V12 versions of X3

Data Collected – X3



localhost:8124/syracuse-main/html/main.html?url=http%3A%2F%2Flocalhost%3A8124%2Fdata%2Fsyracuse%2Fcollaboration%2Fsyracuse...

Apps Sage X3 External 443

Import Payment / Receipt Entry Orders Export Invoices Customer BP Invoices Reports Printouts Script editor Invoices

sage X3 Super administrator Super administrator X3ERP12_SEED

All > Administration > Usage > Logs

History log

Created on	Created by	Entity name
10/03/2021 10:46	admin	user

Value thierry **Operation** Modified

Changes

Property	New value	Previous value
Groups	1 added, 0 deleted, 0 modified	

Description

Groups:
erpdis (added):

Data Collected – Mongo Export



```
15 null,"sync_ldap":{"_uuid":
"97c7e070-cda8-4aa3-8721-0c04db647dd1"},"title":"mr"
,"userOAuth2s":[]}
{"_id":"f4a5ba09-795e-4d5a-a0c2-ae497b771824",
"creDate":{"$date":"2020-09-02T08:14:07.707Z"},
"creUser":"admin","_endpoint":null,"_tick":null,
"updDate":{"$date":"2021-03-04T17:54:00.438Z"},
"updUser":"admin","active":true,"authentication":
"ldap","authenticationName":"frank","boProfiles":[],
"bookmarks":{},"changePassword":null,"email":
"frank@example.com","endpoints":[{"deactivated":
false,"code":"FRANK","login":"FRANK","user":{"_uuid":
"f4a5ba09-795e-4d5a-a0c2-ae497b771824"},"endpoint":
{"_uuid":"5903900d-5fbf-460f-a4b4-930f4624d782"},
"_uuid":"cb47fbd2-f994-42a6-9159-6adac226d0ff",
"creUser":"admin","_updUser":"admin","_updDate":{"
$date":"2020-09-22T14:48:45.386Z"}},{"deactivated":
false,"code":"FRANK","login":"FRANK","user":{"_uuid":
"f4a5ba09-795e-4d5a-a0c2-ae497b771824"},"endpoint":
{"_uuid":"541851ce-dd35-4275-9e53-6cc86a932326"},
"_uuid":"3791e0df-abf8-4916-982d-58dbba6358af",
"creUser":"ukadmin","_updUser":"ukadmin","_updDate":
{"$date":"2020-09-22T14:48:45.879Z"}},{
"deactivated":false,"code":"ZTG0D","login":
"FRANK-ZTG0D","user":{"_uuid":
"f4a5ba09-795e-4d5a-a0c2-ae497b771824"},"endpoint":{"
_uuid":"b3de9540-3ea0-4136-b7d5-bc1293d43748"},
"_uuid":"ea5a8052-d30a-4444-b4e0-6f3ea79851c9",
"creUser":"ukadmin","_updUser":"ukadmin"}],
"firstName":"A","groups":[{"_uuid":
"9fe6867a-617d-414c-8244-7cc8835edf6b","_creUser":
"admin","_creDate":{"$date":
"2020-09-02T08:10:37.466Z"},"_updUser":"ukadmin",
"_updDate":{"$date":"2020-09-22T15:23:24.315Z"},
"_index":0},{"_uuid":
"4a87a142-f7cb-46d5-a1e1-b2d9b83bb134","_creUser":
"anonymous","_creDate":{"$date":
```

Data Collected – Mongo Export

```
ba09-793e-4a5a-abc2-ae497b771624"}, "endpoint": {
  "id": "b3de9540-3ea0-4136-b7d5-bc1293d43748"},
  "id": "ea5a8052-d30a-4444-b4e0-6f3ea79851c9",
  "eUser": "ukadmin", "_updUser": "ukadmin"}},
  "stName": "A", "groups": [{ "_uid":
    6867a-617d-414c-8244-7cc8835edf6b", "_creUser":
    in", "_creDate": {"$date":
      0-09-02T08:10:37.466Z"}, "_updUser": "ukadmin",
      dDate": {"$date": "2020-09-22T15:23:24.315Z"},
      dex": 0}, {" "_uid":
        7a142-f7cb-46d5-a1e1-b2d9b83bb134", "_creUser":
        nymous", "_creDate": {"$date":
          0-05-04T14:16:23.015Z"}, "_updUser": "admin",
          dDate": {"$date": "2021-02-08T14:56:38.312Z"},
          dex": 1}], "infov6": false,
    "passwordExpirationDisabled": false, "lastName":
    nk", "ldap": {" "_uid":
      7e070-cda8-4aa3-8721-0c04db647dd1"}, "locales"
      "login": "frank", "oauth2": {}, "password": null,
      "passwordHistory": null, "passwordUpdated": null,
      "photo": {}, "preferences": {" "_uid":
        21f1f-13e9-43cf-8a07-e0a12c01473a"}, "salt":
        nk", "saml2": {}, "securityLevel": 0, "signature":
        , "sync_ldap": {" "_uid":
          7e070-cda8-4aa3-8721-0c04db647dd1"}, "title": "mr"
          erOAuth2s": [], "ctiId": ""}
        d": "12b87142-62ea-4ead-b600-0aff8dd6f1af",
        eDate": {"$date": "2020-09-02T08:14:08.772Z"},
        eUser": "admin", "_endpoint": null, "_tick": null,
        dDate": {"$date": "2020-12-21T09:35:09.142Z"},
        dUser": "admin", "active": true, "authentication":
        p", "authenticationName": "carey", "boProfiles": [],
        kmarks": {}, "changePassword": null, "email":
```

16

```
91e6867a-617d-414c-8244-7cc8835edf6b", "_creUser":
  "admin", "_creDate": {"$date":
    "2020-09-02T08:10:37.466Z"}, "_updUser": "ukadmin",
    "_updDate": {"$date": "2020-09-22T15:23:24.315Z"},
    "_index": 0}, {" "_uid":
      "4a87a142-f7cb-46d5-a1e1-b2d9b83bb134", "_creUser":
      "anonymous", "_creDate": {"$date":
        "2020-05-04T14:16:23.015Z"}, "_updUser": "admin",
        "_updDate": {"$date": "2021-02-08T14:56:38.312Z"},
        "_index": 1}, {" "_uid":
          "3d237ea2-91ed-4341-90a2-f94e4d485cd9", "_creUser":
          "ukadmin", "_creDate": {"$date":
            "2020-08-28T13:48:39.909Z"}, "_updUser": "ukadmin",
            "_updDate": {"$date": "2020-08-28T13:48:39.909Z"},
            "_index": 2}], "infov6": false,
        "isPasswordExpirationDisabled": false, "lastName":
        "frank", "ldap": {" "_uid":
          "97c7e070-cda8-4aa3-8721-0c04db647dd1"}, "locales"
          : [], "login": "frank", "oauth2": {}, "password": null,
          "passwordHistory": null, "passwordUpdated": null,
          "photo": {}, "preferences": {" "_uid":
            "54721f1f-13e9-43cf-8a07-e0a12c01473a"}, "salt":
            "frank", "saml2": {}, "securityLevel": 0, "signature":
            null, "sync_ldap": {" "_uid":
              "97c7e070-cda8-4aa3-8721-0c04db647dd1"}, "title": "mr"
              , "userOAuth2s": [], "ctiId": ""}
            {" "_id": "12b87142-62ea-4ead-b600-0aff8dd6f1af",
              "_creDate": {"$date": "2020-09-02T08:14:08.772Z"},
              "_creUser": "admin", "_endpoint": null, "_tick": null,
              "_updDate": {"$date": "2020-12-21T09:35:09.142Z"},
              "_updUser": "admin", "active": true, "authentication":
              "ldap", "authenticationName": "carey", "boProfiles": [],
              "bookmarks": {}, "changePassword": null, "email":
```

Data Collected - Syracuse



```
\\Sage\Safex3\X3V12SYRSVR\syracuse\logs\2021-03-20.X3ERP12VM_N0.log - Notepad++
Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
DERS.xml x3 nodelocal.js x3 Userjson x3 Userjson x3 2021-03-20.X3ERP12VM_N0.log x3
4 x3ParentFolder: null,
5 x3RightsIgnore: false,
6 x3ServerFolder: 'SEED',
7 x3solution: { _uuid: '6e7a9f5e-21d3-40aa-bea3-52ecf3516e72' },
8 helpBaseUrl: '',
9 x3ReferenceFolder: '' }
0 2021-03-20T13:30:49.275Z | | | 98 | http.in | info | 200 179ms (176ms processing) GET
/sdata/syracuse/collaboration/syracuse/groups?representation=group.$select&role=8acdfd37-edde-4f32-b12d-a7581e5e4b5b&trackingId=58f397b1-
dd71-4eae-9925-68e56e10c240&parent=user('616a3855-66be-4b02-9a43-159ed7a1266f')&binding=groups&count=50&profile=~(loc~'en-GB~role~'8acdfd
37-edde-4f32-b12d-a7581e5e4b5b~ep~'5903900d-5fbf-460f-a4b4-930f4624d782~appConn~())&browserTabId=59a574320ed4-1616247029143
1 2021-03-20T13:30:50.907Z | | | | orm.mongodb | debug | Updating lock 82d4c6a9-5f1c-4671-9690-486d064b8508
2 2021-03-20T13:30:54.053Z | | | 99 | http.in | info | PUT
/sdata/syracuse/collaboration/syracuse/$workingCopies('58f397b1-dd71-4eae-9925-68e56e10c240')?representation=user.$edit&role=8acdfd37-edd
e-4f32-b12d-a7581e5e4b5b&profile=~(loc~'en-GB~role~'8acdfd37-edde-4f32-b12d-a7581e5e4b5b~ep~'5903900d-5fbf-460f-a4b4-930f4624d782~a
ppConn~())&trackingId=2d6be76a-385f-41ab-8a7d-6306b680eda3&retryId=edb7c5669faf432382e6220ea5d83682&browserTabId=59a574320ed4-16162470291
43
3 2021-03-20T13:30:54.055Z | bd03b61413a1 | | 99 | orm.mongodb | debug | Mongo got connection in pool for
X3ERP12VM/27017/syracuse/undefined
4 2021-03-20T13:30:54.063Z | bd03b61413a1 | | 99 | orm.mongodb | debug | mongodb.fetchInstance filter { _id:
'55691675-d724-4d14-8328-323494344b2b' }
5 2021-03-20T13:30:54.065Z | bd03b61413a1 | | 99 | orm.mongodb | debug | mongodb.fetchInstance found group
'55691675-d724-4d14-8328-323494344b2b' { _id: '55691675-d724-4d14-8328-323494344b2b',
6 _createDate: 2020-08-28T13:47:57.266Z,
7 _createUser: 'ukadmin',
8 _endpoint: null,
9 _tick: null,
0 _updateDate: 2020-08-28T13:47:57.266Z,
1 _updateUser: 'ukadmin',
2 defaultX3Endpoint: { _uuid: '5903900d-5fbf-460f-a4b4-930f4624d782' },
3 description: { default: 'erpfin', 'en-gb': 'erpfin' },
4 endPoints:
5 [ { _uuid: 'b3de9540-3ea0-4136-b7d5-bc1293d43748',
6 _createUser: 'admin',
7 _createDate: 2020-08-28T07:10:57.506Z,
8 _updateUser: 'admin',
```

Data Collected - Syracuse



```
LDERS.xml | nodelocal.js | Userjson | Userjson | 2021-03-20.X3ERPv12VM_NO.log
57     boProfiles: 1,
58     userOAuth2s: 1 } }
59 2021-03-20T13:30:59.477Z | bd03b61413a1 | | 100 | orm.mongodb | debug | mongodb.save enter: opRef 1
60 2021-03-20T13:30:59.478Z | bd03b61413a1 | | 100 | orm.mongodb | debug | mongodb.save delta: opRef 1 { login: 'charles',
61   title: 'mr',
62   firstName: 'A',
63   lastName: 'Charles',
64   salt: 'charles',
65   active: true,
66   authentication: 'ldap',
67   authenticationName: 'charles',
68   passwordHistory: undefined,
69   passwordUpdated: undefined,
70   password: undefined,
71   signature: undefined,
72   email: 'charles@example.com',
73   photo: { '$uuid': '' },
74   infov6: false,
75   changePassword: undefined,
76   isPasswordExpirationDisabled: false,
77   securityLevel: 2,
78   ctiId: '',
79   groups:
80     [ { '$uuid': '9fe6867a-617d-414c-8244-7cc8835edf6b',
81       '$creUser': 'admin',
82       '$creDate': 2020-09-02T08:10:37.466Z,
83       '$updUser': 'ukadmin',
84       '$updDate': 2020-09-22T15:23:24.315Z,
85       '$index': 0 },
86       { '$uuid': '55691675-d724-4d14-8328-323494344b2b',
87         '$creUser': 'ukadmin',
88         '$creDate': 2020-08-28T13:47:57.266Z,
89         '$updUser': 'ukadmin',
90         '$updDate': 2020-08-28T13:47:57.266Z,
91         '$index': 1 } ],
```


Data Collected – Mongo Profiler



```
C:\Windows\system32\cmd.exe
ageX3:PRIMARY>
ageX3:PRIMARY>
ageX3:PRIMARY> db.getCollection('system.profile').find({ns:'syracuse.User'},{op:1,ns:1,ts:1}).pretty()

  "op" : "query",
  "ns"  : "syracuse.User",
  "ts"  : ISODate("2021-03-20T13:50:42.420Z")

  "op" : "query",
  "ns"  : "syracuse.User",
  "ts"  : ISODate("2021-03-20T13:50:42.463Z")

  "op" : "query",
  "ns"  : "syracuse.User",
  "ts"  : ISODate("2021-03-20T13:50:43.900Z")

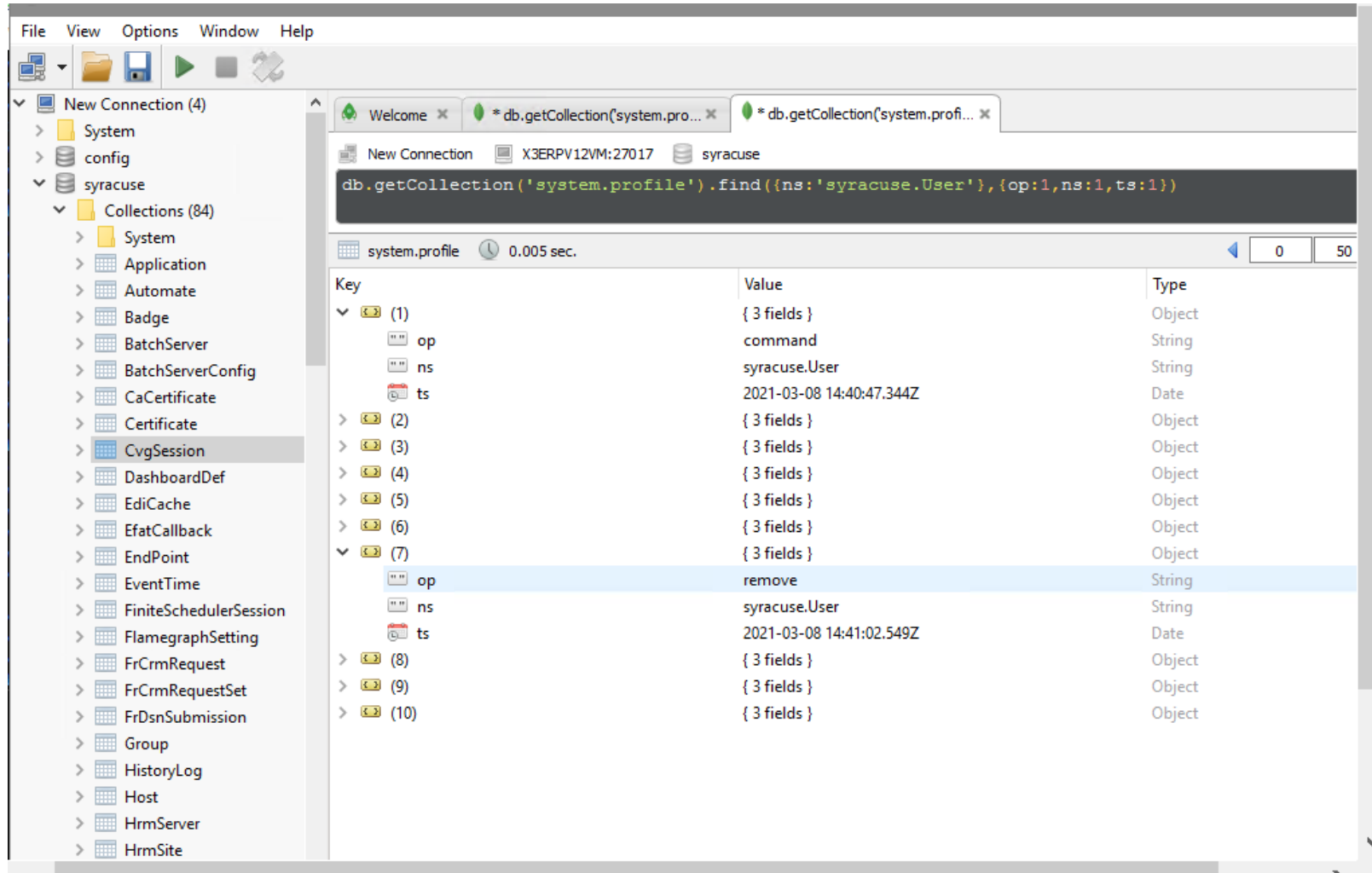
  "op" : "query",
  "ns"  : "syracuse.User",
  "ts"  : ISODate("2021-03-20T13:50:54.155Z")

  "op" : "command",
  "ns"  : "syracuse.User",
  "ts"  : ISODate("2021-03-20T13:51:06.660Z")

  "op" : "query",
  "ns"  : "syracuse.User",
  "ts"  : ISODate("2021-03-20T13:51:06.664Z")

  "op" : "query",
  "ns"  : "syracuse.User",
```

Data Collected – Mongo Profiler



The screenshot shows the MongoDB Profiler interface. On the left, a tree view shows the database structure: 'System', 'config', and 'syracuse'. Under 'syracuse', there are 84 collections, with 'CvgSession' highlighted. The main window shows a query: `db.getCollection('system.profile').find({'ns':'syracuse.User'}, {op:1, ns:1, ts:1})`. The results are displayed in a table with columns 'Key', 'Value', and 'Type'. The table shows 10 rows of data, with the 7th row highlighted. The 7th row has 'op' set to 'remove', 'ns' set to 'syracuse.User', and 'ts' set to '2021-03-08 14:41:02.549Z'.

Key	Value	Type
(1)	{ 3 fields }	Object
op	command	String
ns	syracuse.User	String
ts	2021-03-08 14:40:47.344Z	Date
(2)	{ 3 fields }	Object
(3)	{ 3 fields }	Object
(4)	{ 3 fields }	Object
(5)	{ 3 fields }	Object
(6)	{ 3 fields }	Object
(7)	{ 3 fields }	Object
op	remove	String
ns	syracuse.User	String
ts	2021-03-08 14:41:02.549Z	Date
(8)	{ 3 fields }	Object
(9)	{ 3 fields }	Object
(10)	{ 3 fields }	Object

More information

Information Sources



Sage University - targeted training courses at :-

<https://sageu.com/access/su/home.html>

Sage City – Information/Blogs/Videos etc on Technical specifics at:-

<https://www.sagecity.com/gb/sage-x3-uk/>

MongoDb Documentation at :-

<https://docs.mongodb.com/>

Q & A

Thank you

The Sage logo, consisting of the word "sage" in a lowercase, rounded, sans-serif font. The letters are a vibrant green color.