Reference: MonAzureActiveDirService

Last updated by | Vitor Tomaz | Oct 20, 2022 at 3:53 AM PDT

Contents

Explanation of important columns in MonAzureActiveDirService

1. sql_connection_id -- Represent the connection id in the server side. Can be used to co-relate MonLogin, MonFedAuthTicketService and MonAzureActiveDirectory Tables

2. error_state -- Represents the state in which a particular error occurred (details in table below).

3. error_code -- Represents the system error(in most cases) which happened in that state

4. operation_type -- Represents the Operation happening (refer to the Operation Types table below)

5. error_message -- Contains error messages mostly around interaction with Graph Server failed with particular http status codes which are standard.

6. Please use **LogicalServerName** in case you want to join on **logical_server_name** from tables like MonLogin and MonFedAuthTicketService.

```
MonAzureActivDirService
| where TIMESTAMP  >= ago(2d)
| where error_state > 0
| join kind = inner(MonLogin) on $left.sql_connection_id == $right.connection_id and $left.LogicalServerN
//| where is_success == 0 and error == 18456
| project logical_server_name, is_success, is_user_error, state, error, lookup_error_state, lookup_error_
```

Different Operation Types Possible

No.	State	Explanation
1	AADOperationGetFederatedContextFromOrgIdPuid	Old Code from BEC; should not be hit
2	AADOperationGetObjectIdByPrincipalName	Old Code from BEC; should not be hit
3	AADOperationGetFederatedContextFromObjectId	Building the federated Context
4	AADOperationGraphFetchGroupIDsByPrincipalName	Fetching the member groups of a user from Graph (Client Operation:- Group Expansion needed when login token does not contain the groups inside it
5	AADOperationGraphGetObjectIdByPrincipalName	Fetching the objectID given the principal name (Client operation : Create user [name] from external provider)
6	AADOperationGraphGetObjectIdAndNameByOnPremSID	
7	AADOperationESTSGetJWTForKerberosTicket	For Windows Auth, issue during Kerberos token exchange for AAD token (JWT)
8	AADOperationGraphCheckMemberGroups	
9	AADOperationUnsupportedScenario	

Possible States in MonAzureActiveDirService Table

Event: azure_active_directory_service_failure Create user failure Correlation id is used to join with MonLoginUserDDL

State	Explanation	IsUse
0	AADDefault = 0,	
1	AADCertOpenStore,	
2	AADCertFindInStore,	
3	AADInitializeErrorForProxy,	
4	AADCreateServiceProxy,	
5	AADOpenServiceProxy,	
6	AADGetMaxHeapSizeForGroupLookupFromConfig,	
7	AADCreateHeapForGroupLookup,	
8	AADCreateHeapForObjectIdLookup,	
9	AADInitializeErrorForGroupLookup,	
10	AADInitializeErrorForObjectIdLookup,	
11	AADObjectIdLookup,	
12	AADObjectIdLookupPrincipalNotExist,	
13	AADObjectIdLookupPrincipalNonUnique,	Yes
14	AADObjectIdLookupPrincipalInValid,	Most
15	AADGroupLookup,	
16	AADValidateFederatedContext,	
17	AADGroupObjectIdNoMemoryBecwsProxy,	
18	AADNoMemoryPrincipalName,	

State	Explanation	IsUser
19	AADNoMemoryGraphHandle,	
20	AADDownLoadGraphServerFailed,	
21	AADGraphServerReturns500Status,	
22	AADGraphServerResponseNoBody,	
23	AADNoMemoryDownloadedGraphContents,	
24	AADJSONParsingFailed,	
25	AADJSONNoMemoryForSID,	
26	AADDownloadGraphNullRequest,	
27	AADDownloadGraphBadHeaders,	
28	AADDownloadGraphSendReqError,	
29	AADDownloadGraphReceiveRespError,	
30	AADDownloadGraphQueryHeaderError,	
31	AADDownloadGraphGetBodyLengthError,	
32	AADDownloadGraphQueryDataError,	
33	AADDownloadGraphNoMemoryBuffer,	
34	AADDownloadGraphNoMemoryTempBuffer,	
35	AADDownloadGraphNoMemoryBufferResize,	
36	AADDownloadGraphReadDataError,	
37	AADGraphHandleInitSessionFailed,	
38	AADGraphHandleInitConnectFailed,	
39	AADOperationGetFederatedContextFromGraphServer,	

State	Explanation	IsUse
40	AADFetchOIDsFromGraphClaimGroupCollectionAbsent,	
41	AADFetchOIDsFromGraphWideCharConversionFailed,	
42	AADGraphServiceNoMemory,	
43	AADFederatedContextNoMemoryForCacheEntry,	
44	AADTryAddContextToCacheNoMemoryForCacheEntry,	
45	AADServerAdminSidLookupFailed,	
46	AADGraphGroupLookupFailed,	
47	AADGraphGroupLookupPrincipalNotExist,	
48	AADGraphGroupLookupErrorMessageNoMemory,	
49	AADGraphGroupLookupBearerTokenNoMemory,	
50	AADGraphGroupLookupPostUserRequestNoMemory,	
51	AADGraphObjectIdLookupFailedWithUnexpectedStatusCode,	
52	AADGraphObjectIdLookupNotFederatedUser,	
53	AADObjectIdLookupExtractDetailsNoMemory,	
54	AADFetchOIDsFromGraphExtractionObjectIDFailed,	
55	AADFetchOIDsFromGraphExtractionObjectTypeFailed,	
56	AADFetchOIDsFromGraphExtractionGroupSecurityFlagFailed,	
57	AADFetchOIDsFromGraphExtractionGroupNotSecurityEnabled,	Yes
58	AADGetPrincipalNameAllowAppIdFailed,	
59	AADGraphDownloadGroupOIDsGetContentLengthBufferLengthUnexpectedResult,	
60	AADGraphDownloadUserOIDGetContentLengthBufferLengthUnexpectedResult,	

State	Explanation	IsUser
61	AADGraphDownloadGroupOIDsGetContentLengthBufferLengthUnexpectedErrorCode,	
62	AADGraphDownloadUserOIDGetContentLengthBufferLengthUnexpectedErrorCode,	
63	AADGraphDownloadGroupOIDsGetContentLengthNoMemory,	
64	AADGraphDownloadGroupOIDsGetContentLengthAfterBufferAllocationFailed,	
65	AADGraphDownloadUserOIDGetContentLengthAfterBufferAllocationFailed,	
66	AADGraphDownloadUserOIDGetContentLengthNoMemory,	
67	AADGraphDownloadGroupOIDsDownloadedContentsNoMemory,	
68	AADPrimaryAADTenantIdNotSet,	
69	AADTenantIdFabricLookupNoMemory,	
70	AADClientDisconnectDuringAADGraphAPIGroupLookup,	
71	AADGraphHandleInitGraphEndPointLookupFailed,	
72	AADGetAccessTokenForGroupLookup,	Yes
73	AADGetOnBehalfOfAccessTokenForGroupLookup	
74	AADDownloadGroupOIDsFromGraphServerBadTokenInHeaders	
75	AADDownloadGroupOIDsFromGraphServerBadRequestIdInHeaders	
76	AADDownloadGroupOIDsFromGraphServerControllerRequestIdNoMemoryBuffer	
77	AADDownloadUserOIDFromGraphServerBadTokenInHeaders	

State	Explanation	IsUser
78	AADDownloadUserOIDFromGraphServerBadRequestIdInHeaders	
79	AADDownloadUserOIDFromGraphServerControllerRequestIdNoMemoryBuffer	
80	AADGraphDownloadUserOIDsGetContentLengthBufferLengthUnexpectedErrorCode	
81	AADGraphDownloadUserOIDsGetContentLengthBufferLengthUnexpectedResult	
82	AADGraphDownloadUserOIDsGetContentLengthNoMemory	
83	AADGraphDownloadUserOIDsGetContentLengthAfterBufferAllocationFailed	
84	AADDownloadGraphForUserSendReqError	
85	AADDownloadGraphForGroupSendReqError	
86	AADDownloadGraphForUserReceiveRespError	
87	AADDownloadGraphForGroupReceiveRespError	
88	AADDownloadGraphForUserQueryHeaderError	
89	AADDownloadGraphForGroupQueryHeaderError	
90	AADDownloadGraphForUserQueryDataError	
91	AADDownloadGraphForGroupQueryDataError	
92	AADDownloadGraphForUserNoMemoryBuffer	
93	AADDownloadGraphForGroupNoMemoryBuffer	
94	AADDownloadGraphForUserNoMemoryTempBuffer	
95	AADDownloadGraphForGroupNoMemoryTempBuffer	
96	AADDownloadGraphForUserNoMemoryBufferResize	
97	AADDownloadGraphForGroupNoMemoryBufferResize	
98	AADDownloadGraphForUserReadDataError	
99	AADDownloadGraphForGroupReadDataError	

State	Explanation	IsUser
100	AADGraphDownloadUserOIDDownloadedContentsNoMemory	
101	AADNoMemoryGraphFetchObjecttIDByPrincipalName	
102	AADFetchOIDsFromGraphExtractionUserPrincipalNameFailed	
103	AADFetchOIDsFromGraphExtractionDisplayNameFailed	
104	AADNoMemoryGraphFormGuestUserRequest	
105	AADGraphObjectIdLookupFailedWithForbiddenStatusCode	
106	AADFormMSGraphRequestGlmUserByUPNStringCatFailed	
107	AADFormMSGraphRequestGlmMemberObjectsByUserStringCatFailed	
108	AADFormMSGraphRequestDefaultStringCatFailed	
109	AADFormMSGraphRequestAPIVersionStringCatFailed	
110	AADFormMSGraphRequestTenantIDStringCatFailed	
111	AADFormMSGraphRequestNoMemoryForRequest	
112	AADGetFederatedContextFromMSIDObjectIdGuidToStringEConvertError	
113	AADGertCertNodeError	
114	AADBadRequestEncodeError	
115	AADGraphObjectIdLookupFailedWithDeniedStatusCode	
116	AADEscapeSingleQuoteInPrincipalNameNoMemory	
117	AADEscapeSingleQuoteInPrincipalNameCopyError	
118	AADGetAccessTokenForAppOnlyOBO	
119	AADESTSPostDataNoMemory	
120	AADESTSBase64EncodeFailed	
121	AADESTSGetAzureKerberosClientIdFailed	

State	Explanation	IsUser
122	AADESTSGetAzureKerberosClientSecretFailed	
123	AADESTSFetchJWTForKerberosNullRequest	
124	AADESTSFetchJWTForKerberosControllerRequestIdNoMemory	
125	AADESTSFetchJWTForKerberosBadRequestIdInHeader	
126	AADESTSFetchJWTForKerberosSendRequestError	
127	AADESTSFetchJWTForKerberosRecieveResponseError	
128	AADESTSFetchJWTForKerberosQueryHeadersError	
129	AADESTSFetchJWTForKerberosGetContentLengthBufferUnexpectedResult	
130	AADESTSFetchJWTForKerberosGetContentLengthUnexpectedErrorCode	
131	AADESTSFetchJWTForKerberosGetContentLengthNoMemory	
132	AADESTSFetchJWTForKerberosGetContentLengthAfterBufferAllocationFailed	
133	AADESTSFetchJWTForKerberosQueryDataFailed	
134	AADESTSFetchJWTForKerberosDataBufferNoMemory	
135	AADESTSFetchJWTForKerberosDataTempBufferNoMemory	
136	AADESTSFetchJWTForKerberosDataBufferResizeNoMemory	
137	AADESTSFetchJWTForKerberosReadDataFailed	
138	AADESTSFetchJWTForKerberosDownloadedContentsNoMemory	
139	AADESTSExtractDataServerResponseNoBody	
140	AADESTSExtractDataDownloadedContentsNoMemory	
141	AADESTSExtractDataWideCharConversionFailed	
142	AADESTSExtractDataJSONParseFailed	
143	AADESTSExtractDataGetAccessTokenPropertyFailed	

State	Explanation	IsUser
144	AADESTSExtractDataGetExpiresInPropertyFailed	
145	AADESTSExtractDataGetExtExpiresInPropertyFailed	
146	AADESTSExtractDataGetExpiresOnPropertyFailed	
147	AADESTSExtractDataGetNotBeforePropertyFailed	
148	AADESTSExtractDataGetResourcePropertyFailed	
149	AADESTSExtractDataGetScopePropertyFailed	
150	AADESTSExtractDataGetTokenTypePropertyFailed	
151	AADESTSConnectionAllocationFailed	
152	AADESTSConnectionInitializationFailed	
153	AADESTSHandleInitSessionFailed	
154	AADESTSHandleInitConnectFailed	
155	AADESTSServerReturns500Status	
156	AADESTSBadRequestError	
157	AADESTSTokenExchangeFailedWithForbiddenStatusCode	
158	AADESTSTokenExchangeWithUnexpectedStatusCode	
159	AADESTSAPIServiceAllocationFailed	
160	AADESTSGetSTSUrlFailed	
161	AADESTSUrlEncodingNoMemory	
162	AADESTSGetTenantIdFailed	
163	AADESTSRequestUrlNoMemory	
164	AADESTSPostDataCharNoMemory	
165	AADESTSRedirectUriNoMemory	

State	Explanation	IsUse
166	AADESTSGetAzureKerberosClientAssertionLifetimeFailed	
167	AADESTSGenerateClientAssertionGetCryptoContextFailed	
168	AADESTSGenerateClientAssertionCertificateNoMemory	
169	AADESTSGenerateClientAssertionCertificateInitFailed	
170	AADESTSGenerateClientAssertionGetSTSUrlFailed	
171	AADESTSGenerateClientAssertionAudicityNoMemory	
172	AADESTSGenerateClientAssertionTokenGenerationFailed	
173	AADPrincipalNameDoesNotContainDisplayName	
174	AADCheckGroupMembershipsUnexpectedResult1	
175	AADCheckGroupMembershipsUnexpectedResult2	
176	AADNoMemoryGraphCheckMemberGroups	

How good have you found this content?

🙂 🙁