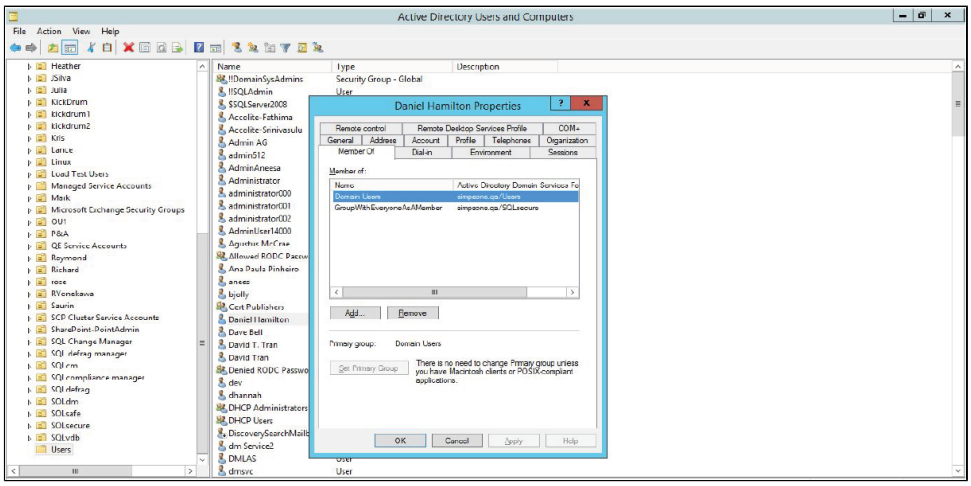
# Active Directory Permissions Exceptions

## SID account

| | |
|---|---|
| Corresponds to warning on UI/Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this |
| Type of exception: | ERROR - this SID is not a group |
| Cause: | Account corresponding to this SID is not part of the global group accounts or well-known group accounts (such as Everyone). |

| | |
|---|---|
| Solution: | One can try changing the scope of the account through Programs<br>• Administrative Tools.<br>• Active Directory Users and Computers.<br>  |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects<br>• User account [SID group] is not part of the global group accounts/well-known group accounts. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are acc<br><br>To get users and group account details, LookupAccountSid is executed which is a windows API, and since the account exists and is accessib account is an alias, group, or a well-known group. So in a normal functioning environment, the user or group return will always be amongst th reproduced in a normal functioning environment.<br><br>Source: https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-lookupaccountsida |

# Active Directory account table

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to lookup account for |
| Cause: | System error encountered when _LookupAccountSid() for given group SID is called. |
| Solution: | Add a user to the active directory using the given steps :<br>• Go to Start.<br>• Select “Administrative Tools”.<br>• Select “Active Directory Users and Computers”.<br>• Either right-click the "Users" folder on the left side, or the blank area on the right side, And highlight "New" then click "User”.<br>• In the next dialog, we can set the user's First name, Last name, and various other pieces of information, including their log-on name, and domain to which we want to add them.<br>• After clicking "Next" you are presented with the password-settings screen.<br>• In the next dialog, we get a summary of the user to be created. Click "Finish" and the user has been created.<br>Verify that the user is active in the Active Directory. |
| New Error Message: | Suspect Windows accounts encountered processing OS objects<br>• User with groupSID - [SID group] is not present in the active directory/Account table.<br>• User with username - [ username ] and groupSID - [SID group] is not present in the active directory /Account table. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server’s file permissions and registry permissions. So, users and groups exist and are accessible.<br>To get users and group account LookupAccountSid is executed which is a windows API and, since the account exists and is accessible, it returns the name for the specified SID.<br>So in normal functioning, it is not null. So the negative case is not reproduced.<br>Source: https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-lookupaccountsida |

# SID Group

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - unable to determine the location of the SID |
| Cause: | The location of the given groupSID is not found as this groupSID is not part of either the Well-Known account group, Domain server group role, or a Local server group. |
| Solution: | Add a group to the active directory using the given steps :<br>• Go to Start.<br>• Select “Administrative Tools”.<br>• Select “Active Directory Users and Computers”.<br>• Either right-click the "Group" folder on the left side, or the blank area on the right side, And highlight "New" then click “Group”.<br>• In the next dialog, we can set the group’s name and various other pieces of information, including their log-on name, and domain to which we want to add them.<br>Verify that the group is active in the Active Directory. |

| | |
|---|---|
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• GroupSID [SID group] is missing from Active Directory. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. If the user or group account is not valid then the account location is returned as unknown. So in normal functioning, the account location will not be unknown therefore the negative case is not reproduced. |

## Group accounts

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - group account object creation failed for |
| Cause: | Local account creation for group account object failed. |
| Solution: | Check if the directory entry obtained from WInNT path is valid and has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• The creation of a local account for the group account failed. |
| Reason for not getting negative findings: | A local account is created for the specified server name, SID Group, and Directory Entry Group. A negative case will arise when the group directory entry is empty or null which will not happen in a normal functioning environment as it is made using the server name and group name. So in the normal functioning environment, the account creation will not fail therefore the negative case will not be reproduced. |

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - enumeration of the group failed for |
| Cause: | Local account creation for group account object failed. |
| Solution: | Check if the directory entry obtained from WInNT path is valid and has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing the OS objects.<br>• Retrieval of the directory members and their paths of the group directory corresponding to the groupSID failed. |
| Reason for not getting negative findings: | In a normal functioning environment, we get members and their paths of the group directory. It may fail during the run time due to some flaws in the environment. Then this error gets logged. It is a custom error and not a standard windows error. We couldn't reproduce this error in a normal functioning environment. |

## Directory Entry

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |

| | |
|---|---|
| Type of exception: | ERROR - group directory entry not found for |
| Cause: | Directory Entry for the given WinNT path not available. |
| Solution: | Please check if the directory exists at the given path. If the directory exists, please check if the user has permission to access the directory. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Directory entry [Directory name] for the given groupSID [SID group] WinNT path is not valid. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. If the directory entry for the SID is not found it returns null. But in a normal functioning environment, the directory entry will not be null for the given SID and therefore the negative case is not reproduced. |

## Domain Controller

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to get domain object for |
| Cause: | Failed to get the name of the domain controller for the specified domain. If Domain is AD, failed to get DNS name for the domain. The domain name was to be returned as either a flat name or a DNS name. |
| Solution: | • Check if the format of the specified Domain Name is invalid.<br>• Check if the Flags parameter does not contain conflicting or superfluous flags.<br>• Check if the memory allocation failure has not occurred.<br>• Check if the domain controller is available for the specified domain or the domain does exist. |
| New Error Message: | Suspect Windows accounts encountered processing OS objects Failed to retrieve the name of the domain controller for the specified domain: [domain name]. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Since the server name and domain name will also be available in normal functionality, so the domain controller details will be accessible therefore the negative case is not reproduced. |

## SID Group Directory

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - domain group account object creation failed for |
| Cause: | This can mean directory entry for the given groupSID is not present or valid. |
| Solution: | Check if the directory path is valid or the user has required permissions to access the directory path. |
| New Error Message: | Suspect Windows accounts encountered processing OS objects. Active Directory entry [directory entry name] for the given groupSID [SID group] is not valid/does not exist. |

| | |
|---|---|
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Since the directory entry name for the users or group is not null or empty or the object class is not unknown for the users or groups in normal functionality therefore the negative case is not reproduced. |

## Group Members

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - domain group enumeration failed for |
| Cause: | Retrieving of the directory members and their paths, of the group directory corresponding to the groupSID has failed. |
| Solution: | Add a group to the active directory using the given steps :<br>• Go to Start.<br>• Select "Administrative Tools".<br>• Select "Active Directory Users and Computers".<br>• Select the server from the left side.<br>• A list of groups and users will appear on the screen.<br>• Select a particular group.<br>• In the dialog opened there will be a tab to see members of the group.<br>Verify if the retrieved group members and their paths are valid entries in the server. |
| New Error Message: | Suspect Windows accounts encountered processing OS objects.<br>Retrieval of the active directory members and their paths of the group directory corresponding to the groupSID [SID group] failed. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Since the directory entry name for the users or group is not null or empty and domain details are available for the users or groups in normal functionality therefore the negative case is not reproduced. |

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - group directory entry not found for |
| Cause: | Directory entry for the given groupSID WinNT path is not valid. |
| Solution: | Check if the specified directory entry path is valid or has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Directory entry[directory entry name] for the given groupSID [SID group] WinNT path is not valid. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. If the directory entry for the SID is not found it returns null. But in a normal functioning environment, the directory entry will not be null for the given SID and therefore the negative case is not reproduced. |

## LDAP Path

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - no elements in the LDAP path |
| Cause: | No elements present in the given path. |
| Solution: | Check if the specified path is valid or has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Given [ldap path] does not contain any elements. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Server Name and group names are available for the users and groups to get the LDAP path. Therefore the path will be generated and it will have elements in normal functionality therefore the negative case is not reproduced. |

## Path Elements

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - not a valid number of elements in the path |
| Cause: | This is logged when there are not enough elements in the path to extract the domain from the path. |
| Solution: | Check if the specified path is valid or has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• The given path [ specific path ] does not contain a valid number of elements. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Server Name and group names are available for the users and groups to get the LDAP path. Therefore the path will be generated and it will have a valid number of elements in normal functionality therefore the negative case is not reproduced. |

## Local Directory

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - Failed to get the local directory entry |
| Cause: | The local directory entry is not found. |
| Solution: | Check if the local Directory entry is valid or has read/write permissions. |

| | |
|---|---|
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Local directory entry not found. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Members of these groups are also accessible and local directory path. So in normal functionality, the local directory entry for each member of the group will be available so the negative case is not reproduced. |

## Group Object Account

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - account object creation failed |
| Cause: | This error is logged when the group object account is tried to be created locally. |
| Solution: | Check if the local Directory entry supplied to this method is valid or has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Please check that the user [ specific user ] has the required permissions for the local directory [local directory name]. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. Since the directory entry name for the users or group is not null or empty or the object class is not unknown for the users or groups in normal functionality, therefore the negative case is not reproduced. |

## Domain

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to get a domain, DN: |
| Cause: | Failed to get Domain for specified object path. |
| Solution: | Check if the specified path is valid or has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Failed to get Domain for specified object path [specific object path]. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. `Domain information for each user or group is fetched using the server name and the user or group members therefore the domain information is available in normal functionality, so the negative case is not reproduced. |

## Directory

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - FSP group directory entry not found for |
| Cause: | Directory entry not found for provided Foreign Security Principal sid or fspsid. |
| Solution: | Check if the specified path is valid or has read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Active directory entry not found for provided Foreign Security Principal sid/fspsid [specific sid\fspsid]. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path in normal functionality so active directory entry will be found for fspsid therefore in normal functionality the negative case is not reproduced. |

## SAM account

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to get SAM account name for the SID: |
| Cause: | Failed to get SAM account name for the SID |
| Solution: | Check if the Active DirectoryEntry from which the sid was obtained is valid or has read/write permission. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Active Directory entry from which SID [specific SID] was obtained is not valid or does not have required permissions. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class that will not be unknown in normal functionality, it will be amongst user, group, computer, or inetOrgPerson. So in normal functionality, the object class won't be unknown therefore the negative case is not reproduced. |

## SID Objective Category

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to get object category for the SID: |
| Cause: | Failed to get an object category for the SID. |
| Solution: | Check if the DirectoryEntry from which the sid was obtained is valid or has read/write permission. |

| | |
|---|---|
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Active Directory entry from which SID [specific SID] was obtained is not valid or does not have required permissions. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class that will not be unknown in normal functionality, it will be amongst user, group, computer, or inetOrgPerson. So in normal functionality, the object class won't be unknown therefore the negative case is not reproduced. |

## Directory Group Type

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to get group type |
| Cause: | Failed to group type of the Directory Entry with Object class as a group. |
| Solution: | Check if the DirectoryEntry obtained is valid or has read/write permission. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Active Directory entry obtained is not valid or does not have the required permissions. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class, if the object class is group and directory entry has more than one group type or the group type is not an integer which will not happen in normal functionality. So in normal functionality, the negative case is not reproduced. |

## ADSI path

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to get adsi path |
| Cause: | Failed to get adsi path from the given directory entry object |
| Solution: | Check if the DirectoryEntry obtained is valid or has read/write permission. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects<br>• Active Directory entry obtained is not valid or does not have the required permissions. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path. The directory path will not be null or empty in normal functionality. So in normal functionality, the negative case is not reproduced. |

## Directory Entry

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - exception raised when querying dir entry object |
| Cause: | The exception to handle any other exception occurred while creating an account. |
| Solution: | Check if the DirectoryEntry obtained is valid or has read/write permission. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects<br>• Active Directory entry obtained is not valid or does not have the required permissions. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For every user or group, there will be a directory path and the path has an object class, if the object class is group and directory entry has more than one group type or the group type is not an integer which will not happen in normal functionality. So in normal functionality, the negative case is not reproduced. |

## WinNT path

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to get dom dir entry |
| Cause: | Failed to get domain directory entry for given WinNT path. |
| Solution: | Check if the WinNT path obtained is valid. If the path is valid, check if the account has elevated privileges and account used to get domain directory details have read/write permissions. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Failed to get domain directory entry for given WinNT path. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For each user or group, there are domain details and for each domain, there is a directory path created. In normal functionality, the domain directory path will be created since it will not be null or empty therefore the negative case is not reproduced. |

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR - failed to parse the member DN |
| Cause: | Error in parsing given WinNT Path. |
| Solution: | Check if the WinNT path obtained is valid. If the path is valid, check if the account has elevated privileges and account used to get domain directory details have read/write permissions. |

| | |
|---|---|
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Error in parsing the given WinNT path [specific WinNT path]. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. For each user or group, there are domain details and for each domain, there is a directory path created. In normal functionality, the domain directory path has the domain name which can be extracted successfully so it will not be null or empty therefore the negative case is not reproduced. |

## Group members

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR: Failed to load <path> group members |
| Cause: | No Group members retrieved for the given groupSID. |
| Solution: | Check if the given SID is a valid group SID. If not, one try changing the scope of the account through :<br>• Programs.<br>• Administrative Tools.<br>• Active Directory Users and Computers. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• No group members retrieved for the groupSID - [specific SID group]. |
| Reason for not getting negative findings: | This error should come when a group with the respective groupSID does not have a member. According to code, an error will be reproduced when a member's object is null. members' object is never null even if there is no member. If there is no member, then members object will have count as 0. Since the check is if the members object is null, so this is not reproduced. |

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | ERROR: failed to read <path> AD group object |
| Cause: | Group members cannot be retrieved for the given groupSID. |
| Solution: | Check if the given SID is a valid group SID. If not, one try changing the scope of the account through :<br>• Programs.<br>• Administrative Tools.<br>• Active Directory Users and Computers. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• No group members retrieved for the groupSID - [specific SID group]. |

| | |
|---|---|
| Reason for not getting negative findings: | This error should come when the group is null. Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. So, in a normal functioning environment, the group is not null. Therefore, the error is not reproduced. |

## SID and SAM path

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2]<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI] |
| Type of exception: | Failed to create an account for File Access Rights. |
| Cause: | Failed to create group account access rights for the given sid and sam path. |
| Solution: | Check if the given SID is a valid group SID. If not, one try changing the scope of the account through:<br>• Programs.<br>• Administrative Tools.<br>• Active Directory Users and Computers.<br>• Check if the given path is valid and has read/write permission. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Failed to create an account for File Access Rights. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. To get users and group account LookupAccountSid is executed which is a windows API and an account are created for files that have permissions for the file and is accessible, it returns file details for the specified SID. So in the normal functioning account will be created for file access rights therefore negative case is not reproduced. |

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | Failed to create an account for File Audit Rights. |
| Cause: | Failed to create group account audit rights for the given sid and sam path. |
| Solution: | Check if the given SID is a valid group SID. If not, one try changing the scope of the account through:<br>• Programs.<br>• Administrative Tools.<br>• Active Directory Users and Computers.<br>• Check if the given path is valid and has read/write permission. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects.<br>• Failed to create an account for File Audit Rights. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. To get users and group account LookupAccountSid is executed which is a windows API and an account are created for files that have permissions for the file and is accessible, it returns file details for the specified SID. So in the normal functioning account will be created for file access rights therefore negative case is not reproduced. |

| | |
|---|---|
| Corresponds to warning on UI / Exception in Logs: | • Suspect Windows accounts encountered processing OS objects [UI] [Old message replaced by the message below in 3.2].<br>• We could not load/read data while processing OS objects. Please check the Activity logs of the server for possible solutions to avoid this. [UI]. |
| Type of exception: | Failed to create an account for File Audit Settings. |
| Cause: | Failed to create group account audit settings for the given sid and sam path. |
| Solution: | Check if the given SID is a valid group SID. If not, one try changing the scope of the account through:<br>• Programs.<br>• Administrative Tools.<br>• Active Directory Users and Computers.<br>• Check if the given path is valid and has read/write permission. |
| New Error Message: | • Suspect Windows accounts encountered processing OS objects<br>• Failed to create an account for File Audit Settings. |
| Reason for not getting negative findings: | Users and group accounts are fetched using SQL Server's file permissions and registry permissions. So, users and groups exist and are accessible. To get users and group account LookupAccountSid is executed which is a windows API and an account are created for files that have permissions for the file and is accessible, it returns file details for the specified SID. So in the normal functioning account will be created for file access rights therefore negative case is not reproduced. |