

<https://www.sqldbachamps.com>

<https://github.com/PMSQLDBA/PraveenMadupu>

Telegram Group → SQLDBACloud-DevOps <https://t.me/+r2OYsT2qRZJkYWVI>

Praveen Madupu
Mb: +91 98661 30093
Database Administrator

TSQL Script to find All DB's Orphan Users Report:

1. **Orphan users without any corresponding SQL Server login** (no matching SID).
2. **Orphan users with a corresponding login but a mismatched SID** (login exists but SIDs don't match).

```
CREATE TABLE #OrphUsers
(
    DatabaseName NVARCHAR(50),
    OrphanedUserName NVARCHAR(100),
    UserType NVARCHAR(50),
    OrphanType NVARCHAR(50) -- 'No Login' or 'SID Mismatch'
);
EXEC sp_MSforeachdb '
IF DB_ID("?") NOT IN (1,2,3,4) -- Skip system DBs: master=1, tempdb=2, model=3, msdb=4
BEGIN
    -- 1. Orphan users without any corresponding login
    INSERT INTO #OrphUsers
    SELECT
        "?" AS DatabaseName,
        dp.name AS OrphanedUserName,
        dp.type_desc AS UserType,
        "No Login" AS OrphanType
    FROM [?].sys.database_principals dp
    LEFT JOIN sys.server_principals sp
        ON dp.name = sp.name
    WHERE sp.name IS NULL
        AND dp.type IN ("S", "U", "G")
        AND dp.name NOT IN ("sys", "INFORMATION_SCHEMA", "guest");

    -- 2. Orphan users with corresponding login but mismatched SID
    INSERT INTO #OrphUsers
    SELECT
        "?" AS DatabaseName,
        dp.name AS OrphanedUserName,
        dp.type_desc AS UserType,
        "SID Mismatch" AS OrphanType
    FROM [?].sys.database_principals dp
    INNER JOIN sys.server_principals sp
        ON dp.name = sp.name
    WHERE dp.sid <> sp.sid
        AND dp.type IN ("S", "U", "G")
        AND dp.name NOT IN ("sys", "INFORMATION_SCHEMA", "guest");
END
';
-- Final Report
SELECT *
FROM #OrphUsers
where OrphanedUserName NOT in ('dbo')
ORDER BY DatabaseName, OrphanType, OrphanedUserName;

DROP TABLE #OrphUsers;
```

Alternate Script:

```

CREATE TABLE #OrphUsers
(
    DatabaseName NVARCHAR(50),
    OrphanedUserName NVARCHAR(100),
    UserType NVARCHAR(50),
    OrphanType NVARCHAR(50) -- 'No Login' or 'SID Mismatch'
);

DECLARE @DBName NVARCHAR(255);
DECLARE @SQL NVARCHAR(MAX);

DECLARE db_cursor CURSOR FOR
SELECT name
FROM sys.databases
WHERE database_id > 4 -- skip system DBs: master=1, tempdb=2, model=3, msdb=4
AND state_desc = 'ONLINE'; -- only online databases

OPEN db_cursor;
FETCH NEXT FROM db_cursor INTO @DBName;

WHILE @@FETCH_STATUS = 0
BEGIN
    BEGIN TRY
        SET @SQL = N'
-- 1. Orphan users without any corresponding login
INSERT INTO #OrphUsers
SELECT
    ''' + @DBName + ''' AS DatabaseName,
    dp.name AS OrphanedUserName,
    dp.type_desc AS UserType,
    "No Login" AS OrphanType
FROM [' + @DBName + '].sys.database_principals dp
LEFT JOIN sys.server_principals sp
    ON dp.name = sp.name
WHERE sp.name IS NULL
AND dp.type IN ("S","U","G")
AND dp.name NOT IN ("sys", "INFORMATION_SCHEMA", "guest");

-- 2. Orphan users with corresponding login but mismatched SID
INSERT INTO #OrphUsers
SELECT
    ''' + @DBName + ''' AS DatabaseName,
    dp.name AS OrphanedUserName,
    dp.type_desc AS UserType,
    "SID Mismatch" AS OrphanType
FROM [' + @DBName + '].sys.database_principals dp
INNER JOIN sys.server_principals sp
    ON dp.name = sp.name
WHERE dp.sid <> sp.sid
AND dp.type IN ("S","U","G")
AND dp.name NOT IN ("sys", "INFORMATION_SCHEMA", "guest");
';

        EXEC sp_executesql @SQL;
    END TRY
    BEGIN CATCH
        PRINT 'Could not query database: ' + @DBName;
    END CATCH;

    FETCH NEXT FROM db_cursor INTO @DBName;
END

```

```
CLOSE db_cursor;  
DEALLOCATE db_cursor;  
  
-- Final report  
SELECT *  
FROM #OrphUsers  
where OrphanedUserName not in ('dbo')  
ORDER BY DatabaseName, OrphanType, OrphanedUserName;  
  
DROP TABLE #OrphUsers;
```

Sample output:

	DatabaseName	OrphanedUserName	UserType	OrphanType
1	Adworks	Anirudh	SQL_USER	No Login
2	Adworks	Karthik	SQL_USER	SID Mismatch
3	AuditDBA	Anirudh	SQL_USER	No Login
4	AuditDBA	Karthik	SQL_USER	SID Mismatch

<https://www.sqldbachamps.com/>

<https://www.sqldbachamps.com/>