# Lab: SID

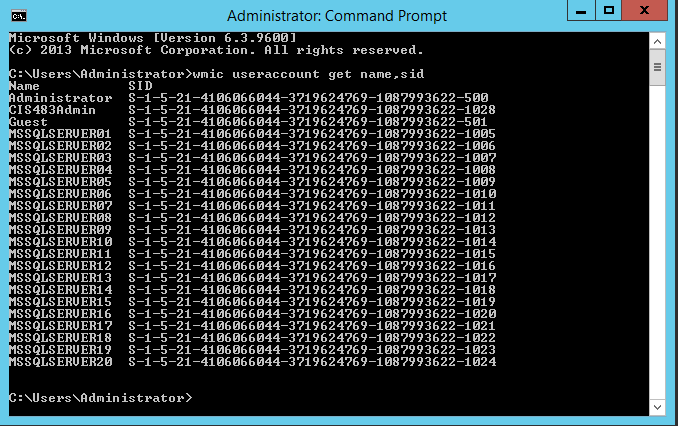
|  |
| --- |
| * This is an in-class lab, and worth 10 points. * The due date and time is tonight. * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab\_SQLi\_ImG.docx). |

# Preparation

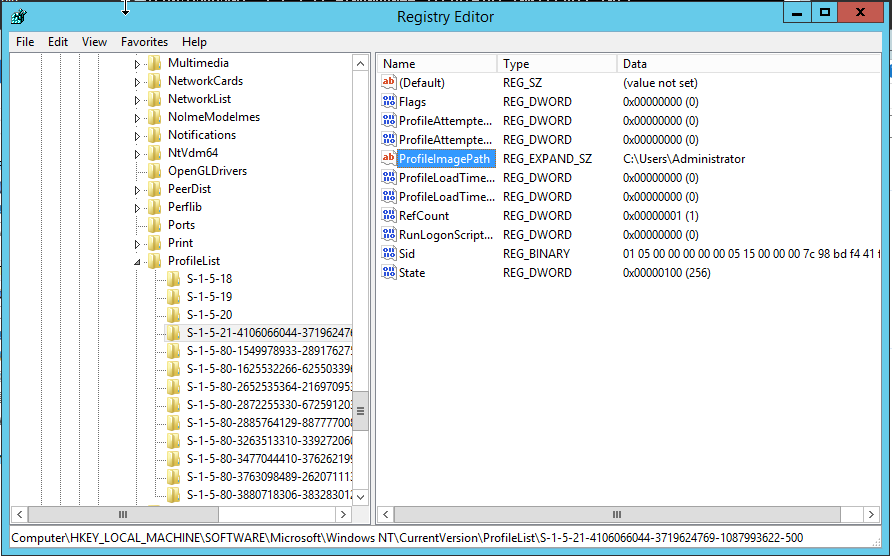
* Read the following articles to understand how security identifiers (SIDs) work.
* <https://msdn.microsoft.com/en-us/library/cc246018.aspx>
* https://technet.microsoft.com/en-us/library/cc778824(v=ws.10).aspx
* Use the Proxmox server. Login to the server and download this file from there to be able to copy the code below.

# Task 1: Getting SID, SAT in Windows

* Use the following website for this task.
  + <https://www.lifewire.com/how-to-find-a-users-security-identifier-sid-in-windows-2625149>
* Login to Windows Server 2012.
  + Obtain the SID of the current login with **WMIC** command. Attach a screenshot for this.



* + Obtain the SID of the current login in the Registry. Attach a screenshot for this.



# Task 2: Getting SID in SQL Server

* Login to SQL Server using Windows Authentication.
* Run the following.

SELECT \*

FROM sys.server\_principals

* Get the SID of the account you used for SQL Server login.
* A. SID: \_\_\_0x0105000000000005150000007C98BDF441F8B4DD1677D940F4010000\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* Execute the following script to convert the SID of the account into the string SID.
* First, create the function.

CREATE FUNCTION fn\_SIDToString

(

@BinSID AS VARBINARY(100)

)

RETURNS VARCHAR(100)

AS BEGIN

IF LEN(@BinSID) % 4 <> 0 RETURN(NULL)

DECLARE @StringSID VARCHAR(100)

DECLARE @i AS INT

DECLARE @j AS INT

SELECT @StringSID = 'S-'

+ CONVERT(VARCHAR, CONVERT(INT, CONVERT(VARBINARY, SUBSTRING(@BinSID, 1, 1))))

SELECT @StringSID = @StringSID + '-'

+ CONVERT(VARCHAR, CONVERT(INT, CONVERT(VARBINARY, SUBSTRING(@BinSID, 3, 6))))

SET @j = 9

SET @i = LEN(@BinSID)

WHILE @j < @i

BEGIN

DECLARE @val BINARY(4)

SELECT @val = SUBSTRING(@BinSID, @j, 4)

SELECT @StringSID = @StringSID + '-'

+ CONVERT(VARCHAR, CONVERT(BIGINT, CONVERT(VARBINARY, REVERSE(CONVERT(VARBINARY, @val)))))

SET @j = @j + 4

END

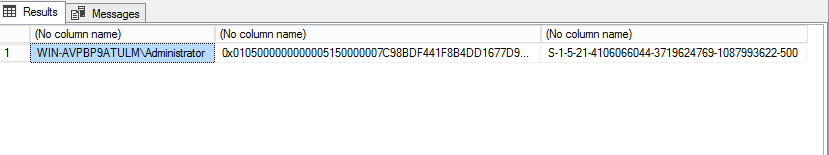
RETURN ( @StringSID )

END

* Next, run the function to get the SIDs.

SELECT SUSER\_NAME(), SUSER\_SID(), dbo.fn\_SIDToString(SUSER\_SID())

* B. Show that the SID from SQL Server for the admin login and the SID from Windows Server are the same.



* Let us create logins. Run the following script.

CREATE LOGIN SIDTest WITH PASSWORD = 'Pa$$w0rd'

GO

* Get the SID of this login.

SELECT sid

FROM sys.server\_principals

WHERE name = 'SIDTest'

GO

* C. SID: \_\_\_0x3B5674B42D76EC4FAF99FB3AA796AA52\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* Drop this login.

DROP LOGIN SIDTest

GO

* Recreate this login and identify its SID.

CREATE LOGIN SIDTest WITH PASSWORD = ' Pa$$w0rd'

GO

SELECT sid

FROM sys.server\_principals

WHERE name = 'SIDTest'

GO

* D. SID: \_\_\_\_\_\_0xA6F72F70CA748D4F8715147FA15D114E\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* E. Are the SIDs of login SIDTest the same? Describe the reason why they are (not) the same?

\_\_No.\_Because SIDs are unique and made when a new account is created and is randomly generated\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

* After this, drop the login you have created.

# Task 3: Learn PowerShell Scripting

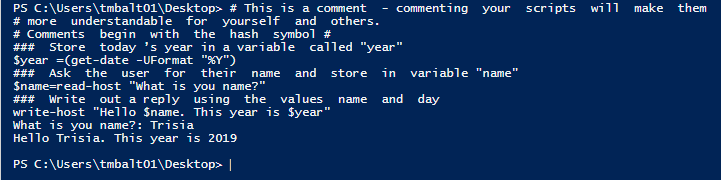
* For this, use **Windows 10**. Search for “**PowerShell**.” And select **Windows PowerShell ISE**.
* Check out the execution policy by typing: **Get-ExecutionPolicy**. Remember this setting.

Restricted

* You can change it by typing the following commands: **Set-ExecutionPolicy unrestricted**, or

**Set-ExecutionPolicy restricted**.

* First, review the “**Getting Started With Microsoft PowerShell.pdf**.” Next, complete **9.1 Exercise**. Run your script and report the output in a screenshot. When you run the script, you should specify the full file path.



* Set the execution policy back to the original one if you have changed.