**EFFECTIVEUSERNAME:**

The Effectiveusername property is used, it uses the windows [S4U windows API](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fwindows%2Fdesktop%2Fapi%2Fntsecapi%2Fnf-ntsecapi-lsalogonuser&data=02%7C01%7CAkshita.Srivastava%40microsoft.com%7Ca1e69ed49dbb46653b5708d76e8a8b3a%7C72f988bf86f141af91ab2d7cd011db47%7C0%7C0%7C637099413663677555&sdata=AkMeWpF5OvVkHdAK7jjdE0sEmBruHrhsr9zQzRwlEac%3D&reserved=0)(KERB\_S4U\_LOGON). S4U logon allows an application such as SSAS to obtain a token to a domain user with just the user's User Principal Name (UPN).

**REQUIREMENT:**

**1. Privilege and permission requirement:**

The caller needs to have SeTcbPrivilege to generate SecurityImpersonation level token.

**2. Trust:**

**A. Domain Trust:**

Normally, when the two **domains have established with trust** ( trust type is External with no transitive). The Kerb\_s4u\_logon should work for remote domain users' UPN when caller (SSAS is in domain1) and users are from cross domain (domain2). Please see below screenshot for detail.

**LAB SCENARIO INFO:**

**Domain1**

SSAS machine: DCSQL1

**Domain2**

Domain2\D2

[D2@domain2.net](mailto:username@domain2.net)

The Kerb\_s4u\_logon can work  for remote domain users’ UPN across domain. For example, SSAS service account (exists in domain1 ) can generate securityImpersonation level token for User UPN in domain2  (i.e. [D2@domain2.net](mailto:D2@domain2.net) ). This is under the assumption of all proper permission, AD permission and SPN in place.

However, the Kerb\_s4u\_logon cannot work for remote domain users' UPN **with SUFFIX** across domain. For example, if domain2 user has an UPN with suffix (i.e. [D2@abc2.net](mailto:D2@abc2.net)), it will fail.

Active Directory Domains and Trusts 
d Trust 
pot-nainl,iiet Preperti" 
General Trusts Managed By 
Domains trusted by this domain (outgoing trustsh 
Domain Name 
Clomain2 net 
Trust Type Transitive 
aternal 
Domains that trust this domain Oncoming trusts) 
Ions 
properties 
Remove 
Domain Name 
Domain 2 net 
New Trust. 
Trust Type 
Ed em al 
Tran stive 
NO 
Apply

In domain2 active directory level, the username account is  ENABLED with suffix name such as [username@abc2.net](mailto:username@abc2.net) , then the s4u will fails when the caller (SSAS) is from different AD.

For example, in below screenshot, the user called D2 is marked to use @Domain2.net (instead of the suffix called abc2.net) in the Active Directory Users and Computers of Domain2.

Remote control 
General Address 
user logon name: 
D2 Properti 
Dial*n 
Remote Desktop Services Profile 
Account profile Telephones 
@Oomain2net 
@Oomain2net 
COM* 
Organization 
user logon name bre-Wtndows 2000) 
@abc2nat 
DOMAIN2\ 
C] Unlock account 
Account options 
C] User must change password at logon 
C] User cannot change password 
C] Passvwnd never expires 
C] Store password using reversible encryption 
Account expires 
O 
Wadnasday. November 28. 2018 
App f y

**B. FOREST TRUST**

The (SSAS) Effectiveusername function actually uses the windows api [S4U windows API](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fwindows%2Fdesktop%2Fapi%2Fntsecapi%2Fnf-ntsecapi-lsalogonuser&data=02%7C01%7CAkshita.Srivastava%40microsoft.com%7Ca1e69ed49dbb46653b5708d76e8a8b3a%7C72f988bf86f141af91ab2d7cd011db47%7C0%7C0%7C637099413663677555&sdata=AkMeWpF5OvVkHdAK7jjdE0sEmBruHrhsr9zQzRwlEac%3D&reserved=0). In this case, the Kerb\_s4u\_logon can still fail when trying to obtain token on user’s UPN from remote domain **with suffix.** It raises the windows error #1326.

If the involving domains have **Forest trust**, it can be fixed by setting the **suffix routing on the trust properties.**

For example, in our lab, we have the following **Domain1.net and Domain2.net setup with Forest trust.**

The user (D2) is from Domain2.net but has marked with suffix **abc2.net**, instead of Domain2.net.

2 0 」 d saOlAJes doptse•O OLLBH 
一 廿 djd 20 
「 OZ smopu 一 , 2 」 aweu u050 一 」 n 
一0」W」OOAY)UJ@H 
2E2L1 u050 一 」 n 
IZNIYNOO

In the Active Directory Domains and Trust-- Domain1 properties, you can go to the **BOTH “outgoing” and “incoming**” trust to ensure the **“Name Suffix Routing”** are enabled for the suffix. In the lab, it is  abc2.net.

Afterward, the S4u logon from SSAS (in domain1) can obtain users from domain1 when using the UPN with suffix, such as “;effectiveusername=D2@abc2.net”.

File Action View Help 
Active Directory Domains and Trust Name 
Domai 
Manage 
Raise Domain Functional Level... 
Properties 
Help 
JÄCtive'D1réåOry Domains rusts 
domai n D NS 
More Actions

IDömäin1 .net Properties 
General Trusts Managed By 
Domains ousted by this domain (outgoing trusts): 
Domain Name 
Domain 2 net 
Trust Type Transitive 
Domains that trust this domain Oncoming trusts): 
Domain2,net Prpperties 
General Name SLffx Routing Authentication 
f outing enabled for a particular name Sl_ffm. all authentication requests 
using that SLfftx are routed to the specified forest 
The specified forest contains multiple name suffixes To change the muting 
status of a suffix. select the suffix. and then click Enable or Disable 
Name sLffixas in the Domain2net forest 
• Domain2net 
Domain Name 
Domain 2 net 
New Trust 
Tust Type Transitive

**C. AD permission:**

The caller must be a member of the Pre-Windows 2000 Compatible Access or have read access to the group memberships of the client.

Membership in the Windows Authorization

Access group guarantees read access to group membership of the client.

In the Active Directory Users and Computers --" Builtin":

File Action View Help 
Active Directory Users and Com 
Saved Queries 
Builtin 
Domain Controllers 
ForeignSecurityPrincipaI! 
Managed Service Accout 
Users 
Name 
Access Control Assistance Operators 
t Operators 
Adm 
inistrators 
Backup Operators 
Certificate Service DCOM Access 
Cryptographic Operators 
Distributed COM Users 
Event Log Readers 
Hyper-V Administrators 
IIS IUSRS 
Incoming Forest Trust Builders 
Network Configuration Operators 
Performance Log Users 
Pre-Windows 2DDO Compatible Access 
r I n pera ors 
ROS Endpoint Servers 
ROS Management Servers 
ROS Remote Access Servers 
Remote Desktop Users 
Remote Management Users 
Replicator 
Server Operators 
Terminal Server License Servers 
Users 
Windows Authorization Access Group 
Type 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Security Group... 
Description 
Members of this group can remotely query authorization attributes and permissi 
Members can administer domain user and group accounts 
Administrators have complete and unrestricted access to the computer/domain 
Backup Operators can override security restrictions for the sole purpose of backi 
Members of this group are allowed to connect to Certification Authorities in the 
Members are authorized to perform cryptographic operations. 
Members are allowed to launch, activate and use Distributed COM objects on th 
Members of this group can read event logs from local machine 
Guests have the same access as members of the Users group by default, except 
Members of this group have complete and unrestricted access to all features of 
Built-in group used by Internet Information Services. 
Members of this group can create incoming, one-way trusts to this forest 
Members in this group can have some administrative privileges to manage conf 
Members of this group may schedule logging of performance counters, enable 
Members of this group can access performance counter data locally and remote 
A backward compatibility group which allows read access on all users and 
Members can administer printers installed on domain controllers 
Servers in this group run virtual machines and host sessions where users Remote 
Servers in this group can perform routine administrative actions on servers runni 
Servers in this group enable users of RemoteApp programs and personal virtual 
Members in this group are granted the right to logon remotely 
Members of this group can access WMI resources cn.'er management protocols ( 
Supports file replication in a domain 
Members can administer domain servers 
Members of this group can update user accounts in Active Directory with inform 
Users are prevented from making accidental or intentional system wide change: 
Members of this group have access to the computed tokenGroupsGIobaIAndUn

**3. Windows AD SPN:**

SPN for the Analysis Service. Please refer to [https://docs.microsoft.com/en-us/sql/analysis-services/instances/spn-registration-for-an-analysis-services-instance?view=sql-server-2017](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fsql%2Fanalysis-services%2Finstances%2Fspn-registration-for-an-analysis-services-instance%3Fview%3Dsql-server-2017&data=02%7C01%7CAkshita.Srivastava%40microsoft.com%7Ca1e69ed49dbb46653b5708d76e8a8b3a%7C72f988bf86f141af91ab2d7cd011db47%7C0%7C0%7C637099413663677555&sdata=ob9VMtrnMw72Qo63Ho0PT10Mn%2BSIa0b%2B2XsOcKuy16c%3D&reserved=0)

Enable the delegation on the DC1SQL object (the SSAS machine).

Properties 
General Operating System Member Of Delegation location Managed ay 
Delegation is a security-sensitive operation which allows services to act on 
behaf of another user 
C) Do not trust this computer for delegation 
O 
Trust this computer for delegation to any service (Kerberos only) 
• lust t is computer or agation to sp 
services on 
@ use Kerberos only 
O 
use any authentication protocol 
Services to which this account can present delegated credentials 
Service Type user or Comput ar 
MSOLAPSvc3 DCISQL 
MSOLAPSvc3 DCISGLDomain1net 
e] apanded 
Dialdn