# Resource SID Compression in Windows Server 2012 may cause Authorization problems on devices that do not support Resource SID compression

https://support.microsoft.com/ru-ru/kb/2774190

**Symptoms**

When accessing file shares hosted on devices that do not support Resource SID compression, after deploying Windows Server 2012 domain controllers, the following symptoms may be observed.

Connections to mapped network drives using the format \\servername\sharename\subfolder fail with Access Denied

Note: Connecting to the same path by using the IP address will always work.

Access to resources that are controlled by membership of Resource group will fail.

**Cause**

This problem occurs under the following conditions:

- Kerberos is used to authenticate the user's session to the device
- The kerberos ticket used in the session setup was issued by a KDC running Windows Server 2012
- The target device does not understand Resource SID Compression, which is a new feature for Kerberos in Windows Server 2012
- Resource SID compression is not understood by Windows XP and Windows 2003 operating systems.
- Resource SID compression may not be understood by some NAS device (Network Access Storage Devices).

**Resolution**

There are two ways to resolve a Kerberos Resource SID Compression interoperability issue

## Resolution 1: (preferred)

The preferred resolution to resource SID compression interoperability is to turn on the disable Resource Group Compression bit (0x80000) in msDS-SupportedEncryptionTypes attribute of the object in Active Directory that is the principal representing the security context of the target service/Device.

Note:This method is not supported when the target Device is Windows XP or Windows 2003.

To produce the correct value, you need to

1. Retrieve the current value in msDS-SupportedEncryptionTypes attribute of the security principal.
2. Perform a bit-wise OR on the current value with 0x80000 to calculate the new value.
3. Store the new value on the msDS-SupportedEncryptionTypes attribute of the security principal.

Alternatively, you can use the following Windows PowerShell script to disable resource SID compression on the given security principal

DisableKerbGroupCompression.ps1

```
#
# Script to Disable Kerberos Group SID Compression
#
param( $principalName)
$newValue = 0
# Get the AD principal and value
$obj = get-adobject -Filter {(cn -like $principalName)} -Properties *
if($obj -eq $null)
{
  Write-Host "Cannot find $principalName in the directory"
  break
}
$newValue = $value = $obj."msDS-SupportedEncryptionTypes"
$msgBefore =$msgAfter = "Resource group compression status on principal {0}: " -f
$principalName
if( ($value -band 0x0080000) -eq 0)
  {$msgBefore += "Enabled"}
else
  {$msgBefore += "Disabled"}
Write-Host $msgBefore
```

```
if( ($value -band 0x00080000) -eq 0) #enable the disable bit
  {$newValue = $value -bor 0x00080000}
if($newValue -ne $value) #update if values are different
{
  Set-ADObject $obj -Replace @{"msDS-SupportedEncryptionTypes"=$newValue}
  if( ($newvalue -band 0x0080000) -eq 0)
    {$msgAfter += "Enabled"}
  else
    {$msgAfter += "Disabled"}
  Write-Host $msgAfter
}
else
{ Write-Host "Resource group compression did not change."}
```

**Syntax**

**DisableKerbGroupCompression.ps1** ***objectName***

## Resolution 2:

This resolution should be used only when resolution one cannot be used.

This resolution disables resource SID compression on an individual Windows Server 2012 domain controller (KDC). You must apply this setting to each Windows Server 2012 domain controller to ensure the domain controllers do not issue tickets that use resource group SID compression.

Resource SID compression is on by default; however, you can disable it. You disable resource SID compression on a Windows Server 2012 KDC using the **DisableResourceGroupsFields** registry value under the **HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kdc\Parameters** registry key. This registry value has a DWORD registry value type. You completely disable resource SID compression when you set the registry value to 1. The KDC reads this configuration when building a service ticket. With the bit enabled, the KDC does not use resource SID compression when building the service ticket.

**More Information**

## KDC Resource SID Compression

Kerberos authentication inserts security identifiers (SIDs) of the security principal, SID history, all the groups to which the user is a member including universal groups and groups from the resource domain. Security principals with too many group memberships greatly affect the size of the authentication data. Sometimes the authentication data is larger than the allocated size reported by Kerberos to applications. This can causes authentication failure in some applications. SIDs from the resource domain share the same domain portion of the SID, these SIDs can be compressed by only providing the resource domain SID once for all SIDs in the resource domain.

Windows Server 2012 KDCs help reduce the size of the PAC by taking advantage of resource SID compression. By default, a Windows Server 2012 KDC will always compress resource SIDs. To compress resource SIDs, the KDC stores SID of the resource domain to which the target resource is a member. Then, it inserts only the RID portion of each resource SID into the **ResourceGroupIds** portion of the authentication data.

Resource SID Compression reduces the size of each stored instance of a resource SID because the domain SID is stored once rather than with each instance. Without resource SID Compression, the KDC inserts all the SIDs added by the resource domain in the **Extra-SID** portion of the PAC structure, which is a list of SIDs. [MS-KILE]

**Interoperability**

Some Kerberos implementations may not understand resource group compression and therefore are not compatible. In these scenarios, you may need to disable resource group compression to allow the Windows Server 2012 KDC to interoperate with the third-party Kerberos implementation.

Note This is a "FAST PUBLISH" article created directly from within the Microsoft support organization. The information contained herein is provided as-is in response to emerging issues. As a result of the speed in making it available, the materials may include typographical errors and may be revised at any time without notice. See Terms of Use for other considerations.

For more information read this - **SID Compression**

http://social.technet.microsoft.com/wiki/contents/articles/24370.sid-compression.aspx