Kerberos Constrained Delegation Overview

- Article
- 07/29/2021
- 12 contributors
- Applies to:

✅ Windows Server 2025, ✅ Windows Server 2022, ✅ Windows Server 2019, ✅ Windows Server 2016, ✅ Windows 11, ✅ Windows 10

Feedback

In this article

This overview topic for the IT professional describes new capabilities for Kerberos constrained delegation in Windows Server 2012 R2 and Windows Server 2012.

Feature description

Kerberos constrained delegation was introduced in Windows Server 2003 to provide a safer form of delegation that could be used by services. When it is configured, constrained delegation restricts the services to which the specified server can act on the behalf of a user. This requires domain administrator privileges to configure a domain account for a service and is restricts the account to a single domain. In today's enterprise, front-end services are not designed to be limited to integration with only services in their domain.

In earlier operating systems where the domain administrator configured the service, the service administrator had no useful way to know which front-end services delegated to the resource services they owned. And any front-end service that could delegate to a resource service represented a potential attack point. If a server that hosted a front-end service was compromised, and it was configured to delegate to resource services, the resource services could also be compromised.

In Windows Server 2012 R2 and Windows Server 2012 , ability to configure constrained delegation for the service has been transferred from the domain administrator to the service administrator. In this way, the back-end service administrator can allow or deny front-end services.

For detailed information about constrained delegation as introduced in Windows Server 2003, see Kerberos Protocol Transition and Constrained Delegation.

The Windows Server 2012 R2 and Windows Server 2012 implementation of the Kerberos protocol includes extensions specifically for constrained delegation. Service for User to Proxy (S4U2Proxy) allows a service to use its Kerberos service ticket for a user to obtain a service ticket from the Key Distribution Center (KDC) to a back-end service. These extensions allow constrained delegation to be configured on the back-end service's account, which can be in another domain. For more information about these extensions, see [MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol Specification in the MSDN Library.

Practical applications

Constrained delegation gives service administrators the ability to specify and enforce application trust boundaries by limiting the scope where application services can act on a user's behalf. Service administrators can configure which front-end service accounts can delegate to their back-end services.

By supporting constrained delegation across domains in Windows Server 2012 R2 and Windows Server 2012 , front-end services such as Microsoft Internet Security and Acceleration (ISA) Server, Microsoft Forefront Threat Management Gateway, Microsoft Exchange Outlook Web Access (OWA), and Microsoft SharePoint Server can be configured to use constrained delegation to authenticate to servers in other domains. This provides support for across domains service solutions by using an existing Kerberos infrastructure. Kerberos constrained delegation can be managed by domain administrators or service administrators.

Resource-based constrained delegation across domains

Kerberos constrained delegation can be used to provide constrained delegation when the front-end service and the resource services are not in the same domain. Service administrators are able to configure the new delegation by specifying the

domain accounts of the front-end services which can impersonate users on the account objects of the resource services.

What value does this change add?

By supporting constrained delegation across domains, services can be configured to use constrained delegation to authenticate to servers in other domains rather than using unconstrained delegation. This provides authentication support for across domain service solutions by using an existing Kerberos infrastructure without needing to trust front-end services to delegate to any service.

This also shifts the decision of whether a server should trust the source of a delegated identity from the delegating-from domain administrator to the resource owner.

What works differently?

A change in the underlying protocol allows constrained delegation across domains. The Windows Server 2012 R2 and Windows Server 2012 implementation of the Kerberos protocol includes extensions to Service for User to Proxy (S4U2Proxy) protocol. This is a set of extensions to the Kerberos protocol that allows a service to use its Kerberos service ticket for a user to obtain a service ticket from the Key Distribution Center (KDC) to a back-end service.

For implementation information about these extensions, see [MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol Specification in MSDN.

For more information about the basic message sequence for Kerberos delegation with a forwarded ticket-granting ticket (TGT) as compared to Service for User (S4U) extensions, see section 1.3.3 Protocol Overview in the [MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol Specification.

Security Implications of Resource-based Constrained Delegation

Resource-based constrained delegation puts control of delegation in the hands of the administrator owning the resource being accessed. It depends on attributes of the resource service rather than the service being trusted to delegate. As a result, resource-based constrained delegation cannot use the Trusted-to-Authenticate-

for-Delegation bit that previously controlled protocol transition. The KDC always allows protocol transition when performing resource-based constrained delegation as though the bit were set.

Because the KDC does not limit protocol transition, two new well-known SIDs were introduced to give this control to the resource administrator. These SIDs identify whether protocol transition has occurred, and can be used with standard access control lists to grant or limit access as needed.

Expand table

SID	Description
AUTHENTICATION_AUTHORITY_ASSERTED_IDENTITY S-1-18-1	A SID that means the client's identity is asserted by an authentication authority based on proof of possession of client credentials.
SERVICE_ASSERTED_IDENTITY S-1-18-2	A SID that means the client's identity is asserted by a service.

A backend service can use standard ACL expressions to determine how the user was authenticated.

How do you configure Resource-based Constrained Delegation?

To configure a resource service to allow a front-end service access on the behalf of users, use Windows PowerShell cmdlets.

- To retrieve a list of principals, use the **Get-ADComputer**, **Get-ADServiceAccount**, and **Get-ADUser** cmdlets with the **Properties PrincipalsAllowedToDelegateToAccount** parameter.
- To configure the resource service, use the **New-ADComputer**, **New-ADServiceAccount**, **New-ADUser**, **Set-ADComputer**, **Set-ADServiceAccount**, and **Set-ADUser** cmdlets with the **PrincipalsAllowedToDelegateToAccount** parameter.

Software requirements

Resource-based constrained delegation can only be configured on a domain controller running Windows Server 2012 R2 and Windows Server 2012, but can be applied within a mixed-mode forest.

You must apply the following hotfix to all domain controllers running Windows Server 2012 in user account domains on the referral path between the front-end and back-end domains that are running operating systems earlier than Windows Server: Resource-based constrained delegation KDC_ERR_POLICY failure in environments that have Windows Server 2008 R2-based domain controllers (https://support.microsoft.com/en-gb/help/2665790/resource-based-constrained-delegation-kdc-err-policy-failure-in-enviro).