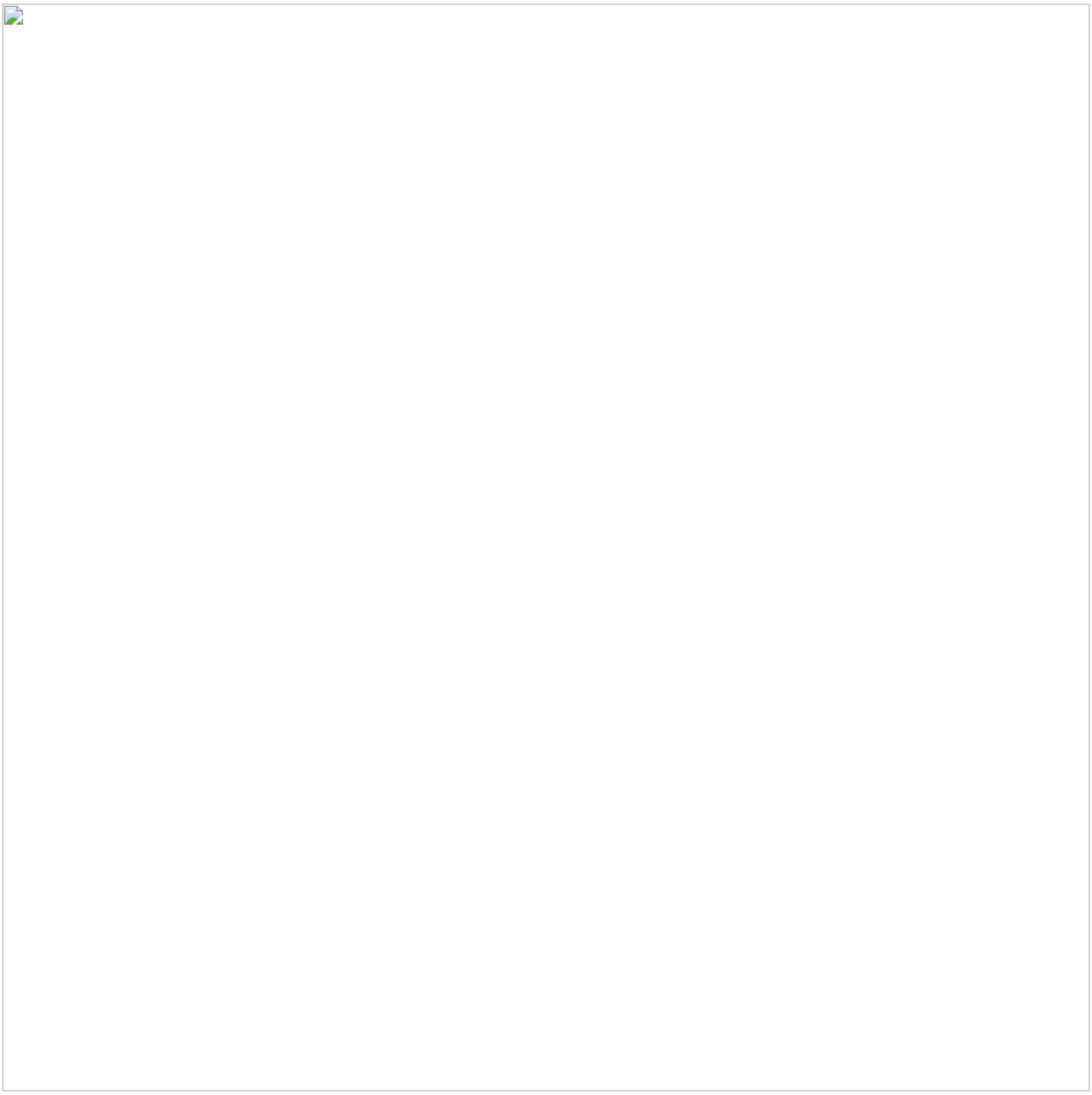
# Too trusting for its own good

**crowe.com**/cybersecurity-watch/unconstrained-delegation-too-trusting-for-its-own-good



## Unconstrained delegation grants excessive network permissions, so organizations should take steps to mitigate associated risks.

Unconstrained delegation is a configuration that attackers can potentially use to impersonate a user or service account and gain access to sensitive resources in an organization's network. To mitigate the risks associated with unconstrained delegation, organizations should take steps to fully understand such configurations, implement best practices regarding privilege, apply effective remediation steps, and replace unconstrained delegation with resource-based delegation wherever possible.

Sign up to receive the latest cybersecurity insights on identifying threats, managing risk, and strengthening your organization’s security posture.

Subscribe now

### Delegation and unconstrained delegation: What’s the difference?

Microsoft originally introduced the concept of delegation as part of Microsoft Windows Server™ 2000 to solve a straightforward problem: Sometimes services need to access resources on behalf of another user. A common example is a web server that displays information to users from a database.

One solution is to grant the account running the web server access to the entire database. However, this creates another problem because it requires the web server to check the users' permissions each time a request is made to ensure it only displays data that users making the request are allowed to access.

A second solution, called delegation, allows the account running the web server to impersonate users connected to it when accessing the database on their behalf. This way the web server can only display data to users that they would otherwise be able to retrieve from the database themselves. Therefore, the burden of checking user permissions falls to the database rather than the web server.

When the concept of delegation was first introduced, the only supported implementation method was unconstrained delegation. However, this type of delegation comes with one major caveat: Services configured for unconstrained delegation can impersonate users when accessing any other resource. For example, when a user authenticates to the web server, the server is not limited to accessing the database as that user. The web server can access any resource, including other web servers and file shares, as the user, even though it is only supposed to access the database as the user.

If unconstrained delegation sounds a little too permissive, that's because it is. Unconstrained delegation runs counter to the principle of least privilege, which dictates that services configured for delegation should only possess delegated access to resources they need to function correctly. Unconstrained delegation is a legacy Microsoft Active Directory™ configuration that attackers love to see, because it allows them to easily elevate their access from a standard user to holding the highest privilege in a Microsoft Windows™ environment.

Microsoft recognized the security issues with unconstrained delegation and later released constrained delegation and resource-based constrained delegation in Windows Server 2003 and Windows Server 2012 respectively to improve security.

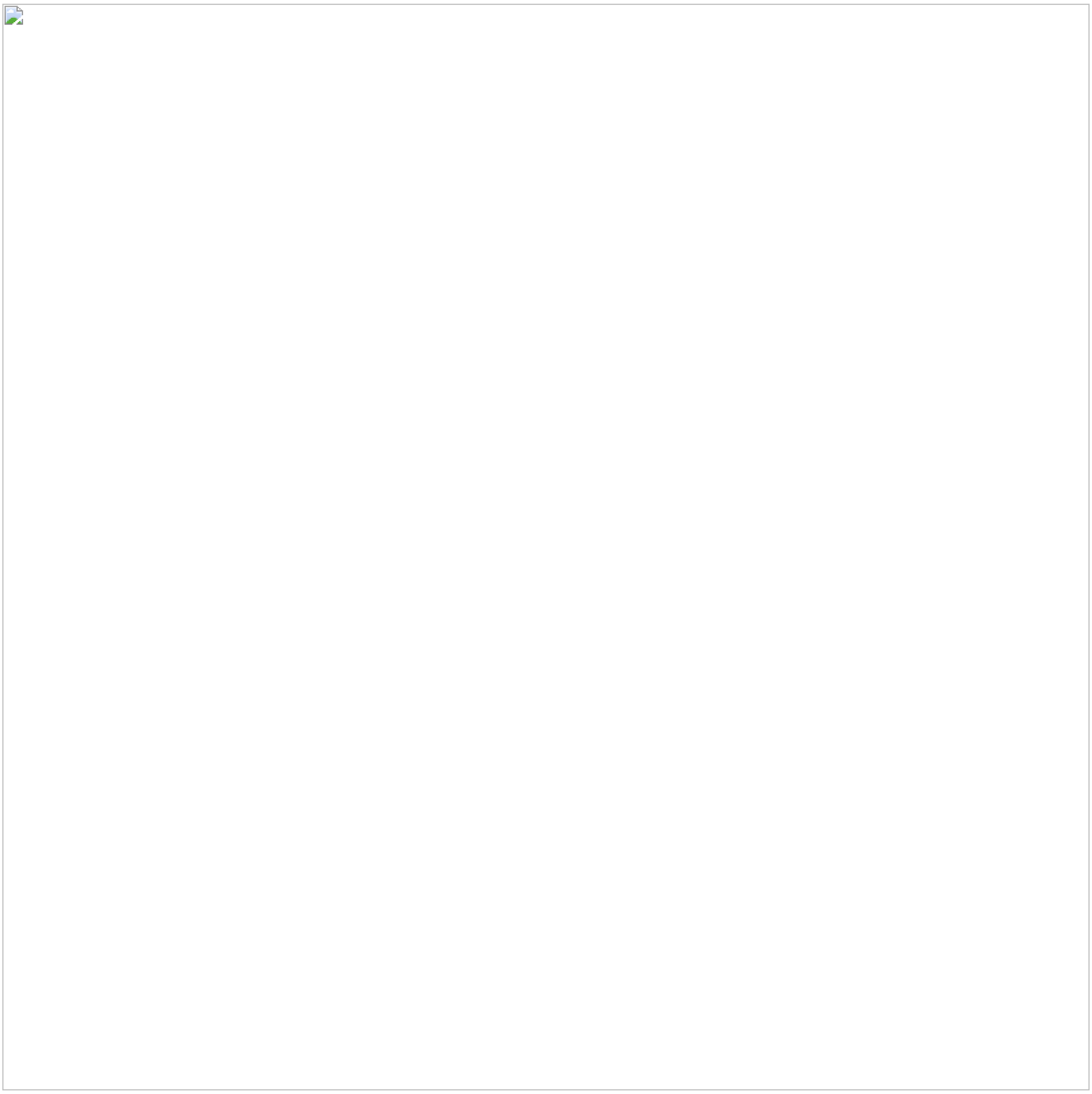
### Mechanics of unconstrained delegation

Unconstrained delegation is enabled by default and required on all domain controllers (DCs). In addition, it can be configured manually by setting the "TRUSTED_FOR_DELEGATION" flag to "true" in the userAccountControl attribute of the user running the service that will make use of delegation. The service can then delegate authentication for all accounts by default, although configuration changes can prevent delegation under specific circumstances.

The "TRUSTED_FOR_DELEGATION" flag also can be set to "true" in the userAccountControl attribute of the account that runs the web server. Unconstrained delegation can be enabled for an account by any user with the SeEnableDelegationPrivilege right. By default, only domain administrators have this right, but it can be granted to additional users.

When Kerberos authentication is used for a service without unconstrained delegation, the only information the user sends to the service is the ticket-granting service (TGS). The TGS contains the information required by the service to identify the user's identity and permissions as well as establish a secure connection. This TGS can only be used to access the service for which it was issued. Exhibit 1 shows the process for authentication and service access without unconstrained delegation.

**Exhibit 1: Authentication and access without unconstrained delegation**



Source: Crowe analysis, January 2023

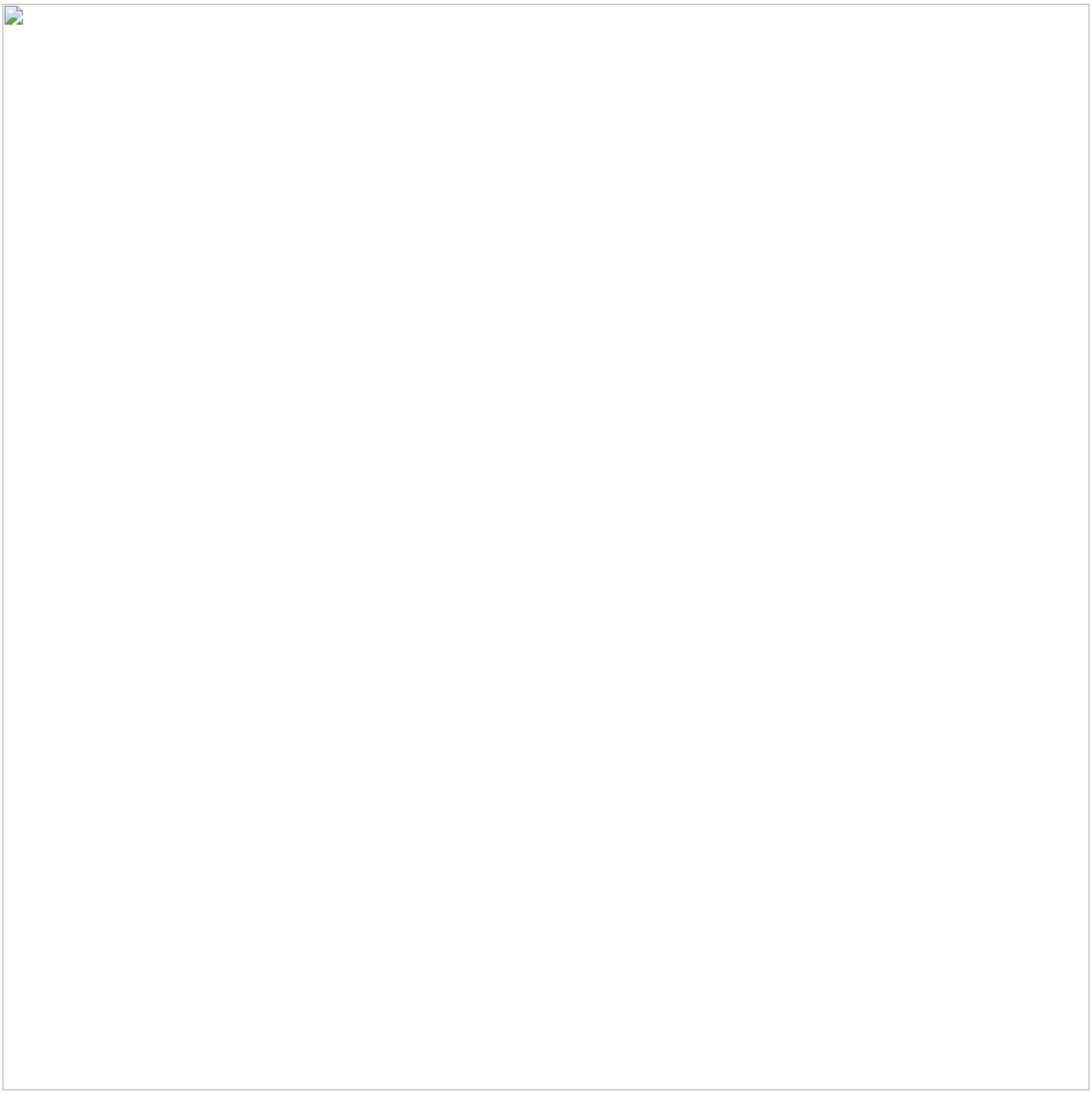
However, when unconstrained delegation is enabled for a service, the TGS sent to the service will contain an additional forwarded ticket-granting ticket (TGT). This forwarded TGT can be used by the service to request access to any resource that also uses Kerberos authentication as the user who sent the TGS. In Exhibit 1, a forwarded TGT allows the web server to access the database as the user who made the web request, as shown in Exhibit 2.

**Exhibit 2: Authentication and service access with unconstrained delegation**

Source: Crowe analysis, January 2023

However, the access provided by unconstrained delegation also allows a malicious web server to access files, remote desktop connections, and anything that belongs to the user who sent the TGS, even though the web server shouldn’t need to access any of these resources on behalf of the user. Exhibit 3 shows an example of such unauthorized access.

**Exhibit 3: Unauthorized access**



Source: Crowe analysis, January 2023

### Attacking unconstrained delegation

While several techniques exist for exploiting unconstrained delegation and variations for each of them, the following attack does not require an attacker to run tools locally, such as Rubeus or Mimikatz, on legitimate machines within the victim's network. Instead, the attack uses Impacket and Krbrelayx. All the tools used in the following attack can be run from an attacker's machine on the local network and are therefore less likely to be detected by antivirus software or endpoint detection and response solutions.

### Attack: Compromise a domain controller in the current forest

One way in which unconstrained delegation can be abused is when an attacker gains access to an account that runs a service with unconstrained delegation. An attacker can attain this access through one of many techniques for unauthenticated privilege escalation, such as abusing NetBIOS and LLMNR to collect hashed credentials and cracking them offline.

With access to a service configured for unconstrained delegation, an attacker can escalate to the domain administrator by coercing authentication from a DC, performing a pass-the-ticket attack using the forwarded TGT of the DC and recovering the Windows New Technology LAN Manager (NTLM) hash of a domain administrator stored on the DC. Following are the prerequisites, steps, and results of the attack:

**Prerequisites**

- Access to an account running a service with unconstrained delegation
- Permission to add a service principal name (SPN) record for the account, which is granted by default to computer accounts but is not granted by default to noncomputer accounts
- Permission to add a domain name system (DNS) record, which is granted by default to both user and computer accounts

**Steps**

1. (Optional) Use any compromised domain account to identify exploitable delegation relationships.
2. Compromise an account configured for unconstrained delegation.
3. Add an SPN associating the account with an additional hostname and create a DNS record that associates the attacker’s IP address with the additional hostname.
4. Coerce authentication from a DC computer account to the attacker machine.
5. Extract a forwarded TGT for the DC computer account using the password and salt, which is comprised of known data including the Kerberos realm name and hostname.
6. Perform a pass-the-ticket attack to access the NTLM hash of any domain user stored on the DC.

**Results**

By authenticating with the NTLM hash retrieved from the DC, an attacker could perform any action as a domain administrator or other domain user.

The attack described requires the account configured for unconstrained delegation to be a computer account that can add an SPN to itself or that the attacker has attained this permission through other means. Variations of this attack that only require permission to modify DNS records or the ability to poison the network are possible, but they are not described here due to their increased likelihood of disrupting the normal function of the network and authentication.

## Remediation

Attackers can exploit unconstrained delegation to escalate privileges within an Active Directory environment. However, it's not possible to disable unconstrained delegation completely. Unconstrained delegation is required on all domain controllers, and it might not be feasible to replace it with a form of constrained delegation on some legacy services.

The following remediation steps comprise a strong, but not impenetrable, defense against unconstrained delegation:

1. Replace instances of unconstrained delegation with resource-based constrained delegation wherever possible.
2. Disable configuring and modifying unconstrained delegation by creating an access control entry, which prevents everyone from editing the msDS-AllowedToActOnBehalfOfOtherIdentity attribute if unconstrained delegation is not required for any non-DC accounts.
3. Assign SeEnableDelegationPrivilege only to users that require the ability to configure delegation for services, such as domain administrators.
4. Mark accounts with elevated access, including computer accounts for domain controllers, as sensitive for delegation to prevent access for the relevant accounts from being delegated with unconstrained delegation.
5. Add sensitive accounts to the Protected Users security group to prevent access for the relevant accounts from being delegated with unconstrained delegation. Computer and service accounts should not be added to this group due to adverse effects on their functionality.
6. Reduce the machine account quota to zero whenever possible. This prevents users assigned SeEnableDelegationPrivilege from creating a computer account and configuring it from unconstrained delegation.
7. Disable Kerberos full delegation across trusts if all required uses of cross-forest unconstrained delegation can be replaced with resource-based constrained delegation.
8. Detect and block known exploits of Microsoft Remote Procedure Calls, which allow users to coerce authentication.
9. Implement detection strategies for EventIds indicative of unconstrained delegation abuse.

The preferred method of delegation in modern Active Directory environments is resource-based constrained delegation, and it should be used to replace unconstrained delegation when some form of delegation is required, whenever possible. This form of delegation addresses some of the weaknesses in unconstrained delegation by requiring services to define the accounts from which they will accept delegated access. For web servers, resource-based constrained delegation would be configured on the database server to only accept delegated access. This configuration prevents the web server, or an attacker-created computer account, from accessing any resource as another user unless the resource is specifically configured to accept delegated access from the web server. However, resource-based constrained delegation has its own security issues.

## Best practices for unconstrained delegation

Delegation is necessary in many Active Directory environments. However, unconstrained delegation is a legacy feature that violates the principle of least privilege. It allows attackers who compromise a service configured with unconstrained delegation to elevate access within a domain by impersonating highly privileged users authenticating to the service.

Vulnerable legacy configurations provide low-hanging fruit for attackers until IT administrators specifically address them, and they cannot be mitigated by diligent patching and security awareness. Remediating unconstrained delegation is essential for organizations that want to close security gaps and protect their networks.

Unconstrained delegation should be replaced with resource-based constrained delegation wherever possible. Additionally, configurations for resource-based delegation should be hardened because it is not a comprehensive protection for delegation-related attacks by default.

Microsoft, Active Directory, Windows, and Windows Server are trademarks of the Microsoft group of companies.