


Common ADCS Vulnerabilities: Logging, Exploitation, and Investigation - Part 1

 labs.lares.com/adcs-exploits-investigations-pt1

Louai Abboud

July 24, 2023

Active Directory Certificate Services (ADCS) is a Microsoft feature and server role that allows organizations to establish an on-premises Public Key Infrastructure (PKI). Threat actors have been actively documented abusing misconfigurations in ADCS to escalate privileges within a Windows domain. In June 2021, eight privilege escalation primitives - ESC1 to ESC8 - were documented by SpectreOps in a whitepaper titled "[Certified Pre-Owned: Abusing Active Directory Certificate Services](#)". Oliver Lyak published a paper the following year adding two additional privilege escalation primitives: [ESC9](#) and [ESC10](#). Finally, Security Compass, in a blog post titled "[Relaying to AD Certificate Services over RPC](#)", added ESC11. ADCS can also be abused for account and domain persistence.

Given the criticality and prevalence of these vulnerabilities, Lares engineers conduct audits of ADCS on a regular basis as part of Purple Teams, Red Teams, and Internal Penetration Testing engagements.

This blog post will dive into the most common vulnerabilities encountered by Lares engineers namely ESC1, ESC3, ESC4, and ESC6. It will be divided into two parts. Part 1] (will discuss the logging configuration required to catch and investigate these attack vectors. [Part 2](#), on the other hand, will delve into the process of:

1. Creating each vulnerability in a lab environment;
2. Exploiting it using certipy-ad; and
3. Investigating its exploitation using a combination of Certification Services logs, SACL auditing, and Splunk.

The remaining privilege escalation primitives will be addressed in future blog posts.

Lab Setup

A lab enviroment containing the following components must be set up in order to test the attacks, logging configurations, and Splunk queries discussed in [Part 1](#) and [Part 2](#) of this blog post.

1. Install the ADCS server role on a Windows server. The simplest setup requires installing the ADCS server role on a Domain Controller (DC) in Windows lab environment. To install ADCS, follow this [guide](#) by Microsoft.
2. Install [Splunk](#) on a host in the lab network and the [Splunk Universal Forwarder](#) on the ADCS Server.
3. Install [Certipy](#) on a Linux machine connected to the same subnet as the lab network (Alternatively, Certipy can be used over a SOCKS proxy). Installation instructions are found on the Certipy's README page on Github.

Required Logging

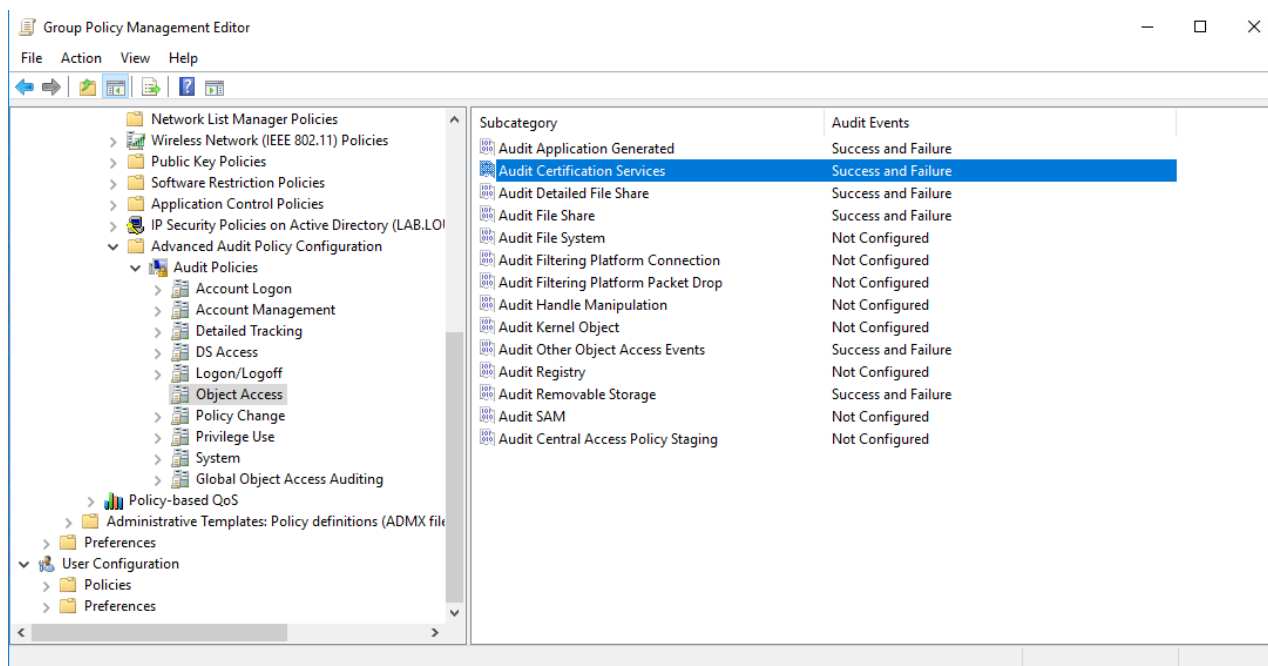
At a minimum, the following log sources must be enabled in order to investigate ADCS threats.

1. **Certification Services Logs:** This log source generates Event IDs 4868-4898 on each ADCS server. It tracks ADCS-related activities such as certificate issuance and enrollment operations and service start, stop, backup, and restore operations. According to Microsoft, event volume is relatively low to medium on ADCS servers.
2. **Directory Service Changes Logs:** This log source generates Event ID 5136 on each domain controller (DC). It can be configured to track modifications to the properties, DACL, and ownership of each certificate template. Event volume is relatively low if the audit policy is configured to track template modification only.

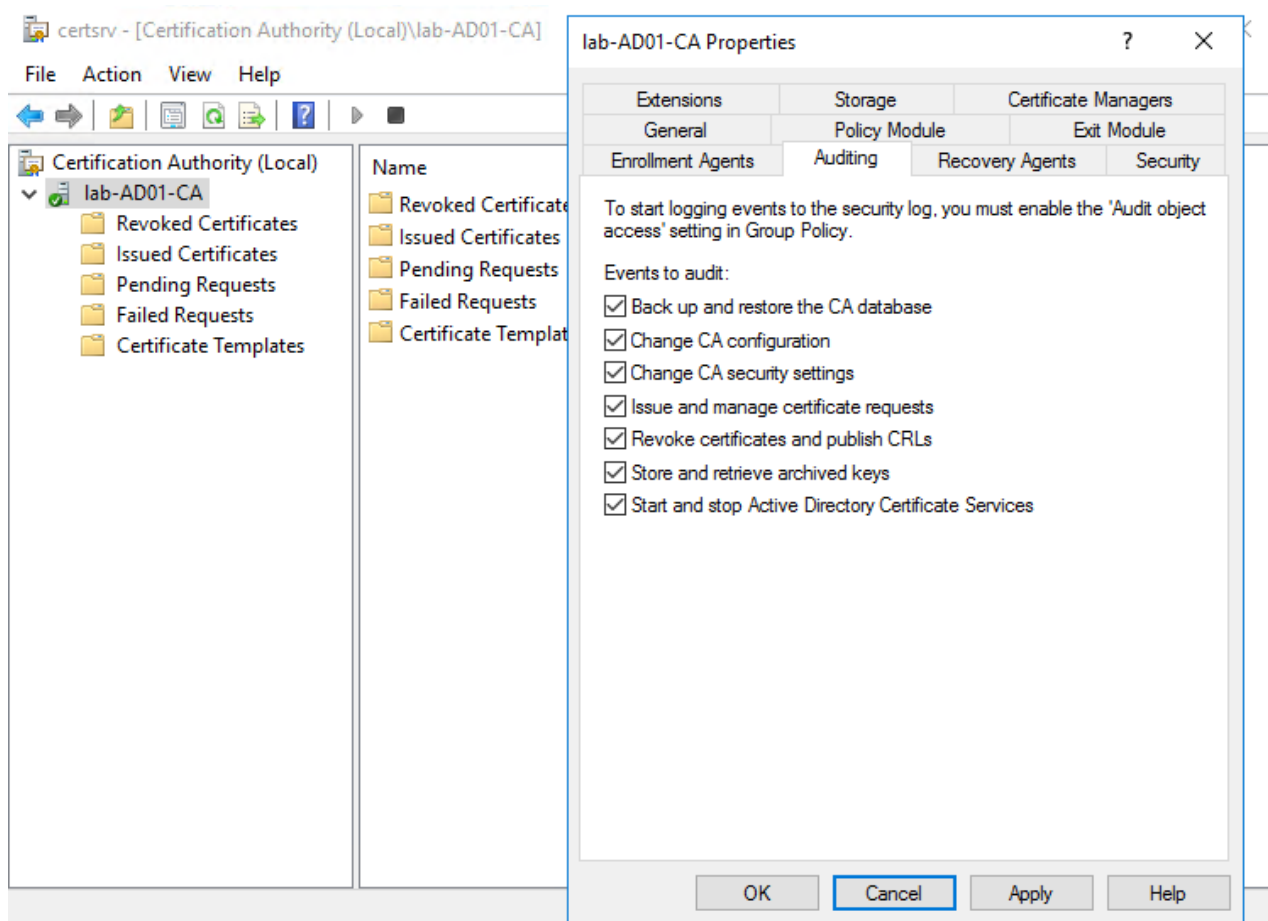
Enable Certification Services Logs

1. As part of your organization's Advanced Auditing Policy GPO or as a new GPO, enable the 'Audit Certification Services' setting under the 'Object Access' category. Monitor for success and failure. The full path to the policy setting is:

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access > Audit Certification Services



2. From Server Manager, open the 'Certification Authority' snap-in and enable auditing under the 'Auditing' tab in the CA's properties dialog.
 - Open 'Server Manager'
 - Open the 'Tools' menu
 - Open the 'Certification Authority' snap-in
 - Right-click the CA for which you want to enable auditing
 - Click 'Properties' in the drop-down menu
 - Navigate to the 'Auditing' tab
 - Enable the following events to audit

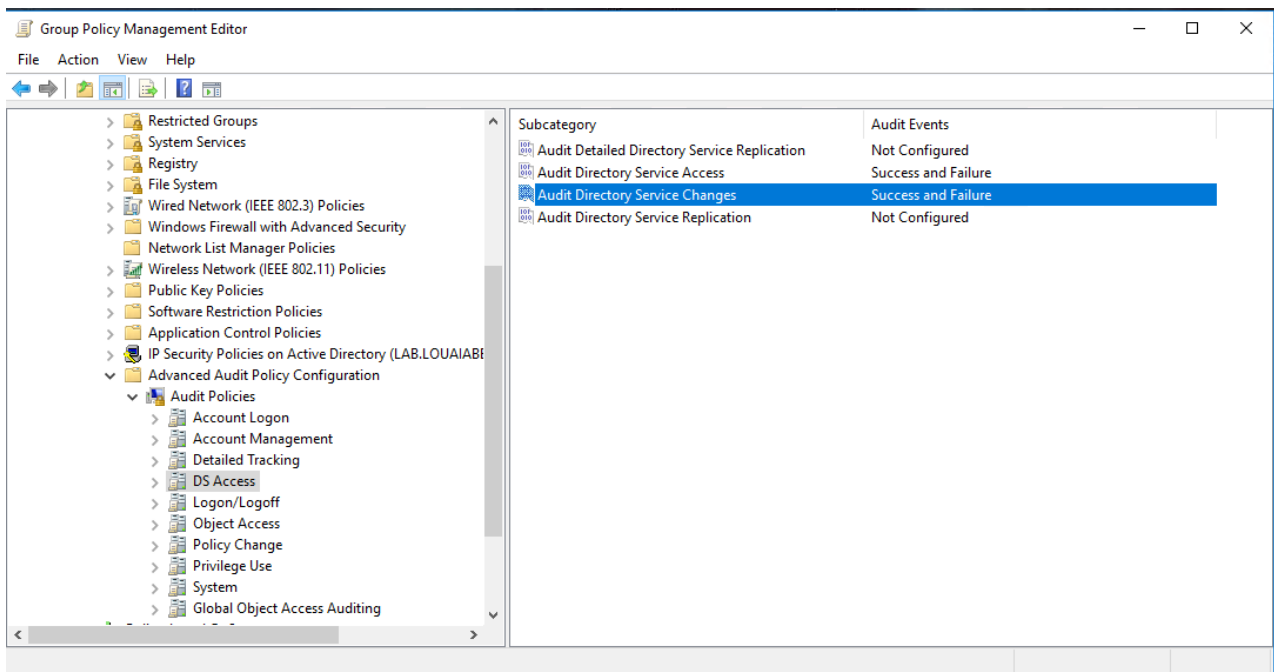


3. Once these logs are enabled, three events will be generated that are of interest:
 - **Event ID 4898:** This event is generated every time a certificate template is loaded during enrollment. It records - in detail - the properties and security descriptor of the certificate template.
 - **Event ID 4887:** This event is generated when a certificate is successfully issued to a user.
 - **Event ID 4888:** This event is generated when a certificate request is denied.

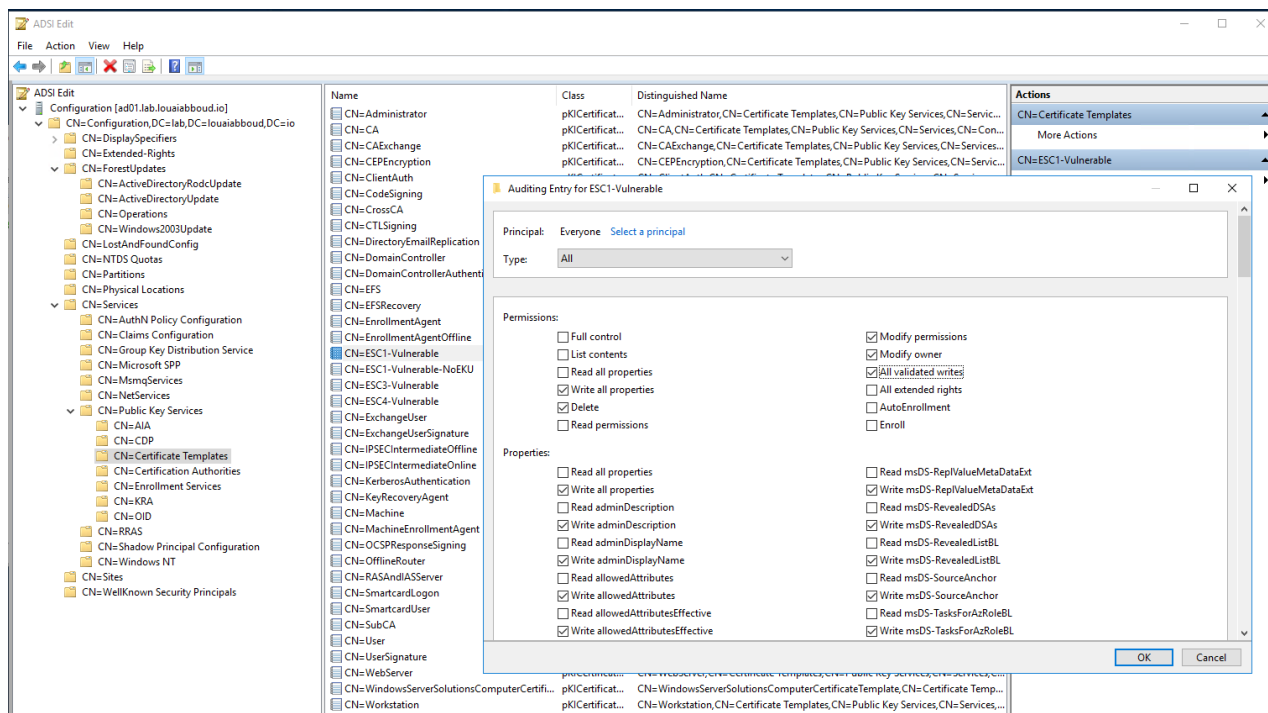
Audit Certificate Templates Modification Operations

1. As part of your organization's Advanced Auditing Policy GPO or as a new GPO, enable the 'Audit Directory Service Changes' setting under the 'DS Access' category. Monitor for success and failure. The full path to the policy setting is:

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > DS Access > Audit Directory Service Changes



2. In the ADSI Edit snap-in, enable auditing on each certificate template object for property, permission, and owner modification.
 - Open 'Server Manager'
 - Open the 'Tools' menu
 - Open the 'ADSI Edit' snap-in
 - Connect to a DC
 - Right-click the connection and click 'Settings'
 - Select the 'Configuration' Naming Context
 - Navigate to: **Configuration > Services > Public Key Services > Certificate Templates**
 - For each certificate template, enable SACL auditing. For 'Principal', select 'Everyone'. For 'Type', select 'All'.



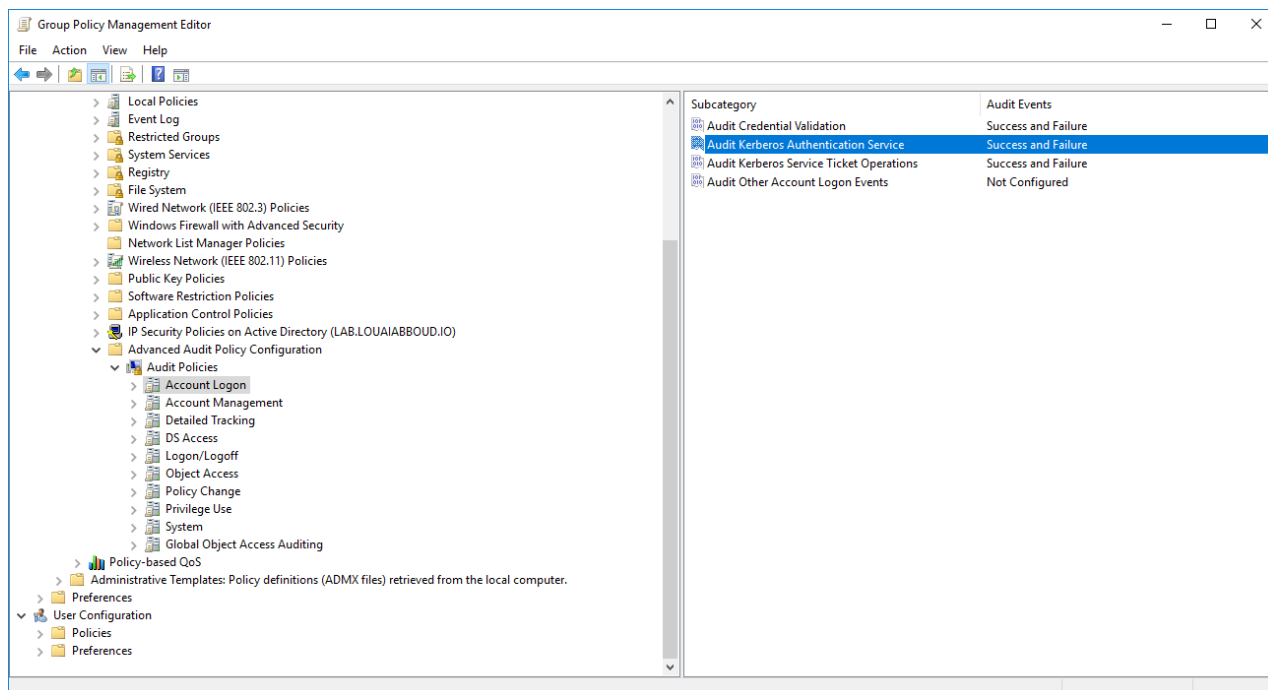
3. Once step #2 is completed, modifications to certificate templates will be logged on each DC in Event ID 5136: "A directory service object was modified."

Supplementary Log Sources

In addition to the above ADCS-centric log sources, organizations should ensure they have the following supplementary log sources enabled:

1. Process creation events either through Windows Security Event ID 4688 (with Command Line Auditing enabled via GPO) or through Sysmon Event ID 1 ("Process Creation") or through a dedicated EDR/XDR solution.
2. Kerberos Authentication Events (Windows Security Event ID 4768 and Event ID 4769). These can be enabled as part of your organization's Advanced Auditing Policy GPO or as part of a new GPO.

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Logon > Audit Directory Service Changes



Conclusion

ADCS vulnerabilities are dangerous. Ensuring proper visibility into this critical AD component is integral to a wholistic organizational security policy.

References and Resources

This blog post would not be possible without prior work by individuals that are significantly more intelligent than its author. A massive shoutout to them! And a special shoutout to Teymur Kheirhabarov and Demyan Sokolin for their talk: "Hunting Active Directory Certificate Services Abuse." Without their research into ADCS telemetry, this blog post would not have been possible.

1. [SpectreOps: Certified Pre-Owned Whitepaper](#)
2. [SpectreOps: Certificates and Pwnage and Patches! Oh My!](#)
3. [Oliver Lyak: Certipy 4.0: ESC9 & ESC10, BloodHound GUI, New Authentication and Request Methods — and more!](#)
4. [Hunting for Active Directory Certificate Services Abuse](#)
5. [Security Compass: Relaying to AD Certificate Services over RPC](#)
6. [Certipy-AD](#)