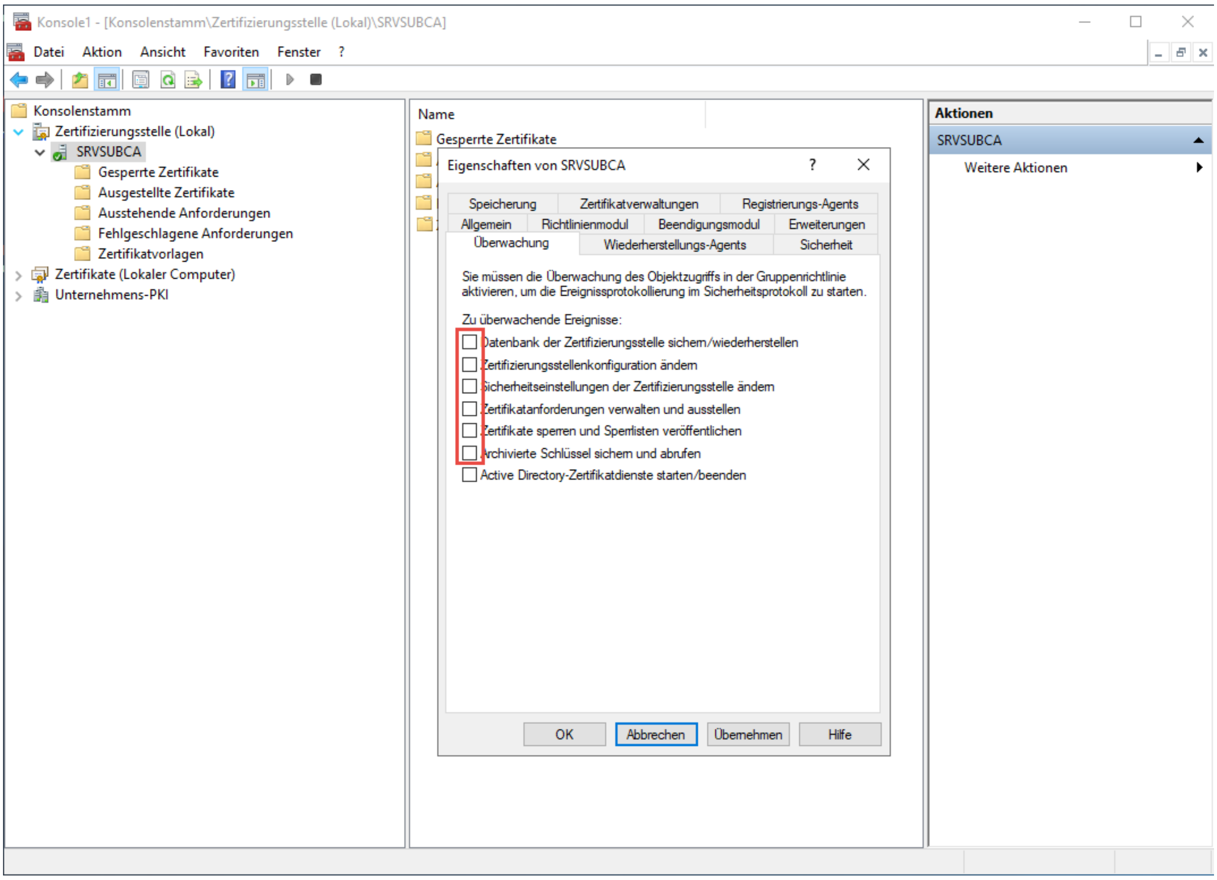
CA Überwachung

Alles was auf, in, unter einer CA (Zertifizierungsstelle) passiert muss überwacht werden.

# Manuelle Konfiguration der Überwachungsoptionen (Ereignisse) einer Zertifikatsstelle.



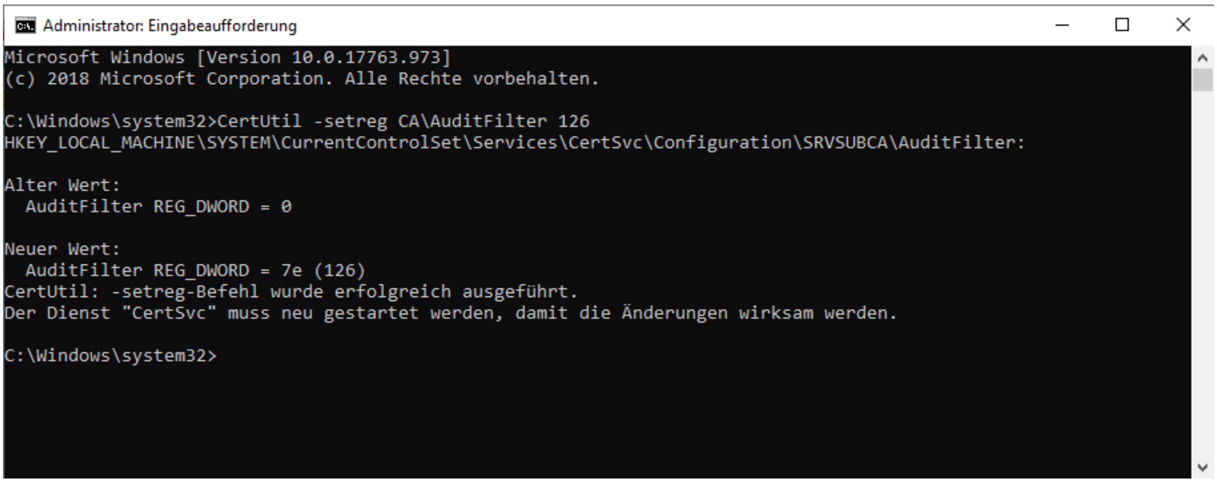
Sie müssen die Überwachung des Objektzugriffs in der Gruppenrichtlinie aktivieren, um die Ereignissprotokollierung im Sicherheitsprotokoll zu starten.

Zu überwachende Ereignisse:

- ☐ Datenbank der Zertifizierungsstelle sichern/wiederherstellen
- ☐ Zertifizierungsstellenkonfiguration ändern
- ☐ Sicherheitseinstellungen der Zertifizierungsstelle ändern
- ☐ Zertifikatanforderungen verwalten und ausstellen
- ☐ Zertifikate sperren und Sperrlisten veröffentlichen
- ☐ Archivierte Schlüssel sichern und abrufen
- ☐ Active Directory-Zertifikatdienste starten/beenden

# Überwachung von Ereignissen auf der CA mittels der CMD aktivieren anstatt dieses manuell wie oben zu tun.

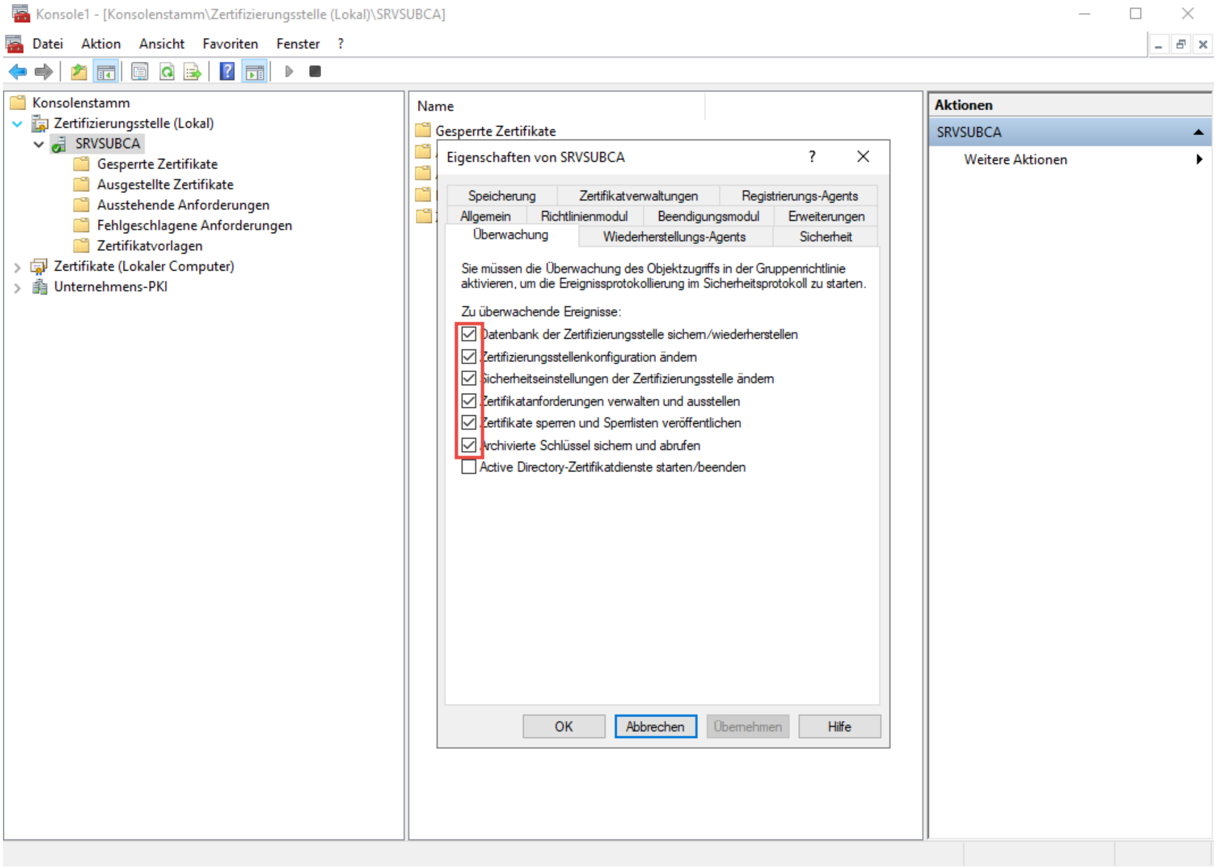
CertUtil -setreg CA\AuditFilter 126



```
Microsoft Windows [Version 10.0.17763.973]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>CertUtil -setreg CA\AuditFilter 126
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\SRVSUBCA\AuditFilter:

Alter Wert:
  AuditFilter REG_DWORD = 0

Neuer Wert:
  AuditFilter REG_DWORD = 7e (126)
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam werden.

C:\Windows\system32>
```

CA Überwachung

Die Optionen wurden erfolgreich aktiviert.



Sie müssen die Überwachung des Objektzugriffs in der Gruppenrichtlinie aktivieren, um die Ereignissprotokollierung im Sicherheitsprotokoll zu starten.

Zu überwachende Ereignisse:

☑ Datenbank der Zertifizierungsstelle sichern/wiederherstellen
☑ Zertifizierungsstellenkonfiguration ändern
☑ Sicherheitseinstellungen der Zertifizierungsstelle ändern
☑ Zertifikatanforderungen verwalten und ausstellen
☑ Zertifikate sperren und Sperrlisten veröffentlichen
☑ Archivierte Schlüssel sichern und abrufen
☐ Active Directory-Zertifikatdienste starten/beenden

Damit die oben gesetzten Optionen auch Wirkung haben, müssen die Objektzugriffe überwacht werden. Diese aktivieren wir mit dem Befehl "auditpol".

# Objektzugriffversuche-Überwachung aktivieren

Deutsches OS:

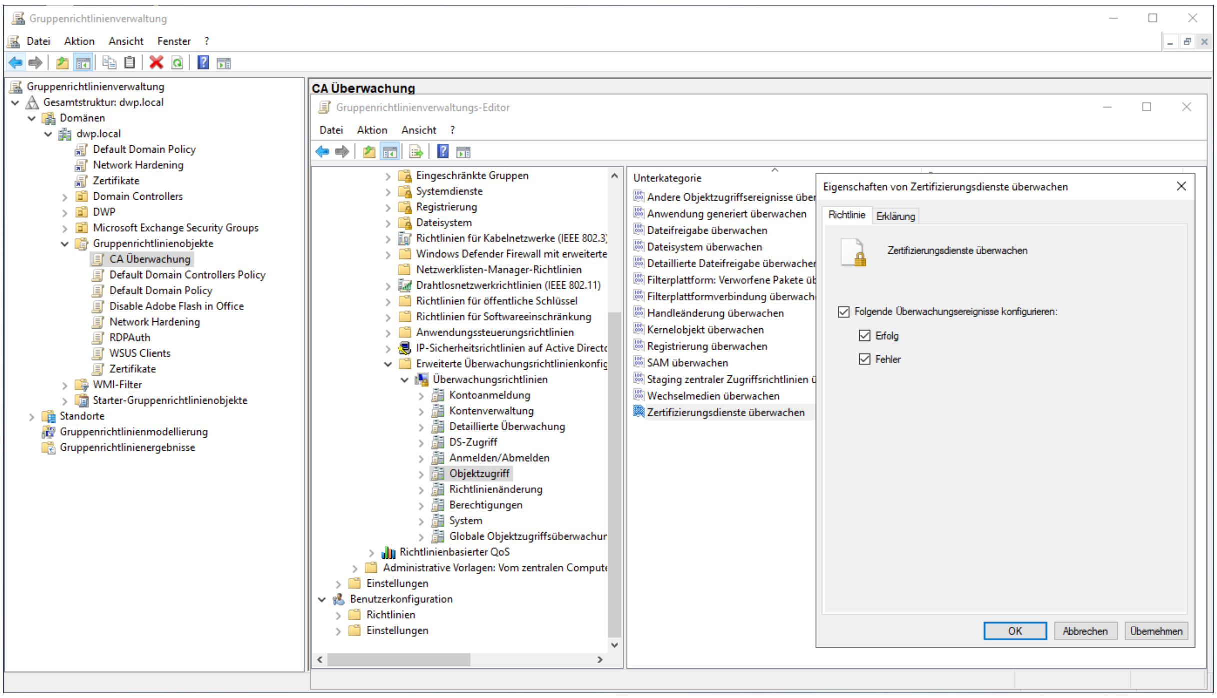
```
auditpol /set /category:"Objektzugriff" /failure:enable /success:enable
```

Englisches OS:

```
auditpol /set /category:"Object Access" /failure:enable /success:enable
```

CA Überwachung

Weiter kann über eine Gruppenrichtlinie die erweiterte Überwachung aktiviert werden.

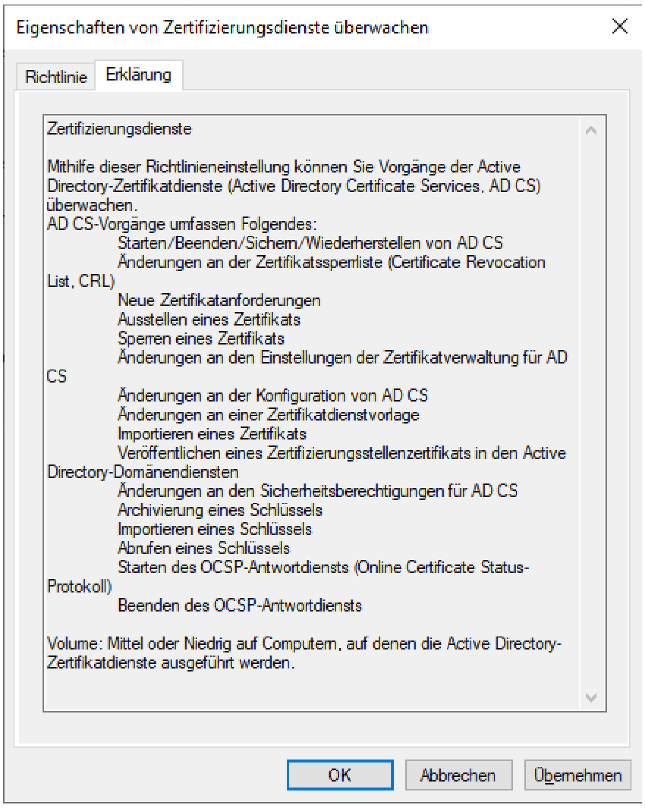

Gruppenrichtlinienverwaltung
Datei Aktion Ansicht Fenster ?
Gruppenrichtlinienverwaltung
Gesamtstruktur: dwp.local
Domänen
dwp.local
Default Domain Policy
Network Hardening
Zertifikate
Domain Controllers
DWP
Microsoft Exchange Security Groups
Gruppenrichtlinienobjekte
CA Überwachung
Default Domain Controllers Policy
Default Domain Policy
Disable Adobe Flash in Office
Network Hardening
RDPAuth
WSUS Clients
Zertifikate
WMI-Filter
Starter-Gruppenrichtlinienobjekte
Standorte
Gruppenrichtlinienmodellierung
Gruppenrichtlinienergebnisse
CA Überwachung
Gruppenrichtlinienverwaltungs-Editor
Datei Aktion Ansicht ?
Eingeschränkte Gruppen
Systemdienste
Registrierung
Dateisystem
Richtlinien für Kabelnetzwerke (IEEE 802.3)
Windows Defender Firewall mit erweiterte
Netzwerklisten-Manager-Richtlinien
Drahtlosnetzwerkrichtlinien (IEEE 802.11)
Richtlinien für öffentliche Schlüssel
Richtlinien für Softwareeinschränkung
Anwendungssteuerungsrichtlinien
IP-Sicherheitsrichtlinien auf Active Directo
Erweiterte Überwachungsrichtlinienkonfig
Überwachungsrichtlinien
Kontoanmeldung
Kontenverwaltung
Detaillierte Überwachung
DS-Zugriff
Anmelden/Abmelden
Objektzugriff
Richtlinienänderung
Berechtigungen
System
Globale Objektzugriffsüberwachur
Richtlinienbasierter QoS
Administrative Vorlagen: Vom zentralen Compute
Einstellungen
Benutzerkonfiguration
Richtlinien
Einstellungen
Unterkategorie
Andere Objektzugriffsereignisse über
Anwendung generiert überwachen
Dateifreigabe überwachen
Dateisystem überwachen
Detaillierte Dateifreigabe überwachen
Filterplattform: Verworfene Pakete üb
Filterplattformverbindung überwach
Handleänderung überwachen
Kernelobjekt überwachen
Registrierung überwachen
SAM überwachen
Staging zentraler Zugriffsrichtlinien ü
Wechselmedien überwachen
Zertifizierungsdienste überwachen
Eigenschaften von Zertifizierungsdienste überwachen
Richtlinie
Erklärung
Zertifizierungsdienste überwachen
OK
Abbrechen
Übernehmen

☑ Folgende Überwachungsereignisse konfigurieren:

☑ Erfolg

☑ Fehler

Erklärung:



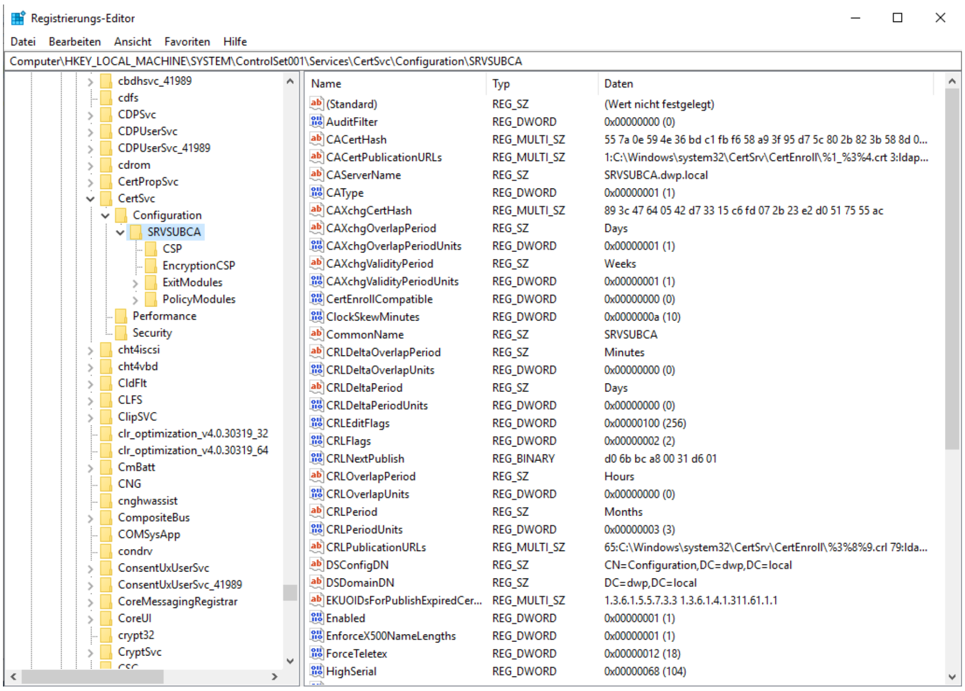
Zertifizierungsdienste

Mithilfe dieser Richtlinieneinstellung können Sie Vorgänge der Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) überwachen.
AD CS-Vorgänge umfassen Folgendes:
Starten/Beenden/Sichern/Wiederherstellen von AD CS
Änderungen an der Zertifikatssperrliste (Certificate Revocation List, CRL)
Neue Zertifikatanforderungen
Ausstellen eines Zertifikats
Sperren eines Zertifikats
Änderungen an den Einstellungen der Zertifikatverwaltung für AD CS
Änderungen an der Konfiguration von AD CS
Änderungen an einer Zertifikatdienstvorlage
Importieren eines Zertifikats
Veröffentlichen eines Zertifizierungsstellenzertifikats in den Active Directory-Domänendiensten
Änderungen an den Sicherheitsberechtigungen für AD CS
Archivierung eines Schlüssels
Importieren eines Schlüssels
Abrufen eines Schlüssels
Starten des OCSP-Antwortdiensts (Online Certificate Status-Protokoll)
Beenden des OCSP-Antwortdiensts

Volume: Mittel oder Niedrig auf Computern, auf denen die Active Directory-Zertifikatdienste ausgeführt werden.

CA Überwachung

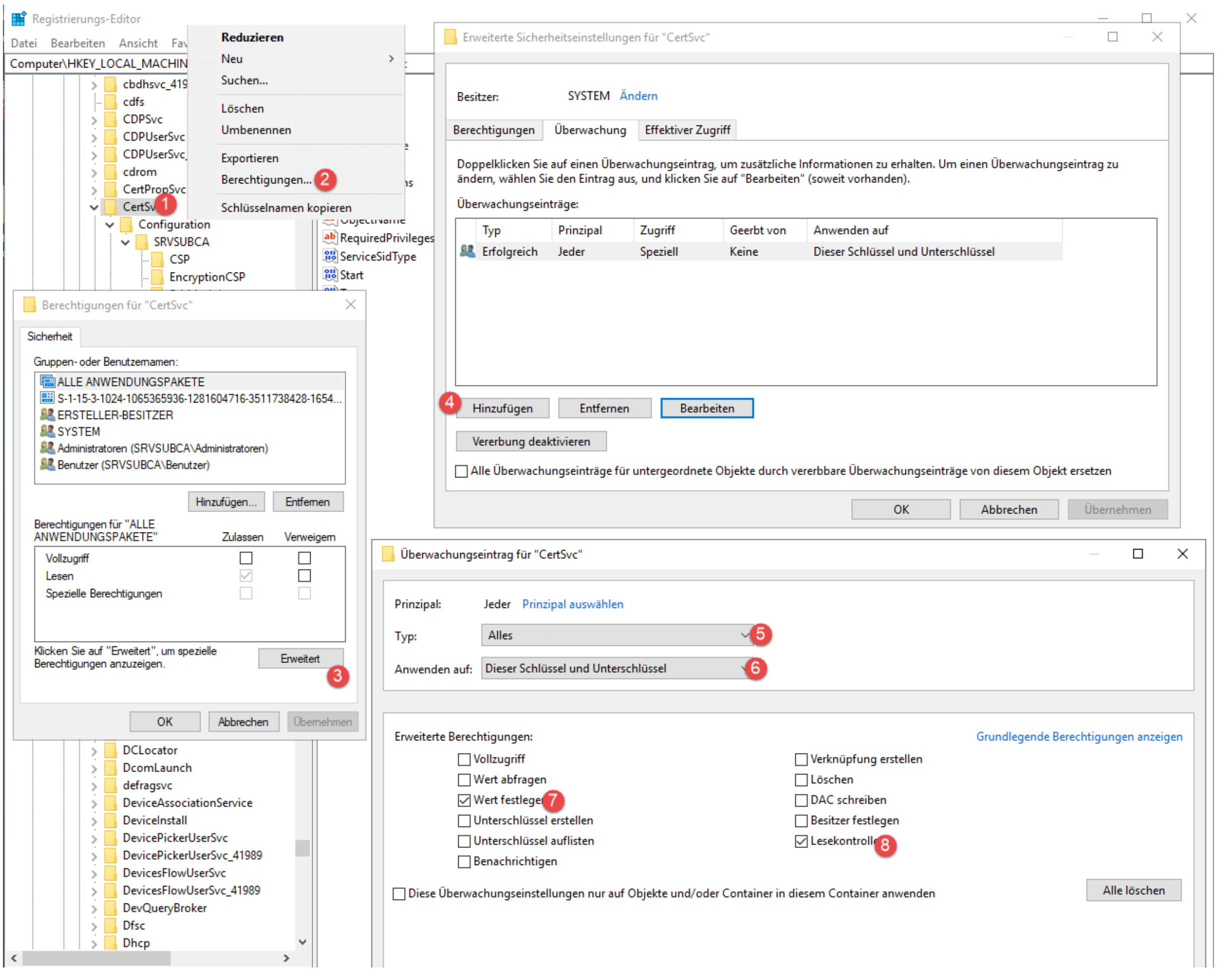
Aber die meisten Änderungen/Konfigurationen finden in der Registry statt. Diese muss zusätzlich überwacht bzw. aktiviert werden.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\CertSvc\Configuration\SRVSUBCA

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
AuditFilter	REG_DWORD	0x00000000 (0)
CACertHash	REG_MULTI_SZ	55 7a 0e 59 4e 36 bd c1 fb f6 58 a9 3f 95 d7 5c 80 2b 82 3b 58 8d 0...
CACertPublicationURLs	REG_MULTI_SZ	1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt 3:ldap...
CAServerName	REG_SZ	SRVSUBCA.dwp.local
CAType	REG_DWORD	0x00000001 (1)
CAXchgCertHash	REG_MULTI_SZ	89 3c 47 64 05 42 d7 33 15 c6 fd 07 2b 23 e2 d0 51 75 55 ac
CAXchgOverlapPeriod	REG_SZ	Days
CAXchgOverlapPeriodUnits	REG_DWORD	0x00000001 (1)
CAXchgValidityPeriod	REG_SZ	Weeks
CAXchgValidityPeriodUnits	REG_DWORD	0x00000001 (1)
CertEnrollCompatible	REG_DWORD	0x00000000 (0)
ClockSkewMinutes	REG_DWORD	0x0000000a (10)
CommonName	REG_SZ	SRVSUBCA
CRLDeltaOverlapPeriod	REG_SZ	Minutes
CRLDeltaOverlapUnits	REG_DWORD	0x00000000 (0)
CRLDeltaPeriod	REG_SZ	Days
CRLDeltaPeriodUnits	REG_DWORD	0x00000000 (0)
CRLEditFlags	REG_DWORD	0x00000100 (256)
CRLFlags	REG_DWORD	0x00000002 (2)
CRLNextPublish	REG_BINARY	d0 6b bc a8 00 31 d6 01
CRLOverlapPeriod	REG_SZ	Hours
CRLOverlapUnits	REG_DWORD	0x00000000 (0)
CRLPeriod	REG_SZ	Months
CRLPeriodUnits	REG_DWORD	0x00000003 (3)
CRLPublicationURLs	REG_MULTI_SZ	65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl 79:lda...
DSConfigDN	REG_SZ	CN=Configuration,DC=dwp,DC=local
DSDomainDN	REG_SZ	DC=dwp,DC=local
EKUOIDsForPublishExpiredCer...	REG_MULTI_SZ	1.3.6.1.5.5.7.3.3 1.3.6.1.4.1.311.61.1.1
Enabled	REG_DWORD	0x00000001 (1)
EnforceX500NameLengths	REG_DWORD	0x00000001 (1)
ForceTeletex	REG_DWORD	0x00000012 (18)
HighSerial	REG_DWORD	0x00000068 (104)

Die Eigenschaften zur Überwachung des Registry-Schlüssels **CertSRV** aktivieren wir wie folgt.



Berechtigungen für "CertSvc"

Sicherheit

Gruppen- oder Benutzernamen:

- ALLE ANWENDUNGSPAKETE
- S-1-15-3-1024-1065365936-1281604716-3511738428-1654...
- ERSTELLER-BESITZER
- SYSTEM
- Administratoren (SRVSUBCA\Administratoren)
- Benutzer (SRVSUBCA\Benutzer)

Hinzufügen... Entfernen

Berechtigungen für "ALLE ANWENDUNGSPAKETE"	Zulassen	Verweigern
Vollzugriff	□	□
Lesen	☑	□
Spezielle Berechtigungen	□	□

Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen. Erweitert

OK Abbrechen Übernehmen

Erweiterte Sicherheitseinstellungen für "CertSvc"

Besitzer: SYSTEM Ändern

Berechtigungen | Überwachung | Effektiver Zugriff

Doppelklicken Sie auf einen Überwachungseintrag, um zusätzliche Informationen zu erhalten. Um einen Überwachungseintrag zu ändern, wählen Sie den Eintrag aus, und klicken Sie auf "Bearbeiten" (soweit vorhanden).

Überwachungseinträge:

Typ	Prinzipal	Zugriff	Geerbt von	Anwenden auf
Erfolgreich	Jeder	Speziell	Keine	Dieser Schlüssel und Unterschlüssel

Hinzufügen Entfernen Bearbeiten

Vererbung deaktivieren

□ Alle Überwachungseinträge für untergeordnete Objekte durch vererbbare Überwachungseinträge von diesem Objekt ersetzen

OK Abbrechen Übernehmen

Überwachungseintrag für "CertSvc"

Prinzipal: Jeder Prinzipal auswählen

Typ: Alles

Anwenden auf: Dieser Schlüssel und Unterschlüssel

Erweiterte Berechtigungen: Grundlegende Berechtigungen anzeigen

□ Vollzugriff	□ Verknüpfung erstellen
□ Wert abfragen	□ Löschen
☑ Wert festlegen	□ DAC schreiben
□ Unterschlüssel erstellen	□ Besitzer festlegen
□ Unterschlüssel auflisten	☑ Lesekontrolle
□ Benachrichtigen	

□ Diese Überwachungseinstellungen nur auf Objekte und/oder Container in diesem Container anwenden

Alle löschen

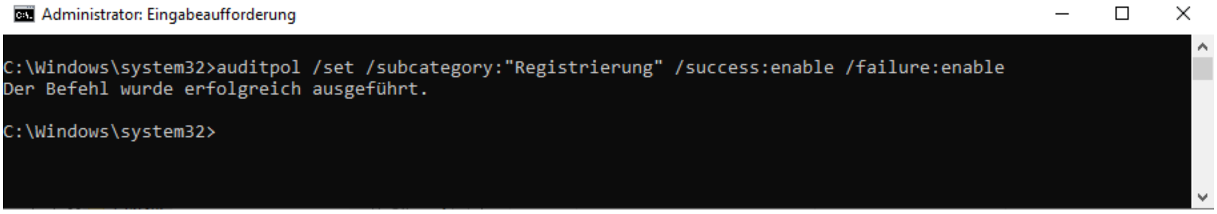
CA Überwachung

Dieser Befehl aktiviert nun die Überwachung von Registrierungsänderungen am Schlüssel CertSRV und alles was sich darunter befindet, die entweder erfolgreich ausgeführt wurden, oder ein Versuch der Änderung, die aufgrund von Berechtigungen fehlschlagen.

# Erweiterte Überwachung (Registry) aktivieren

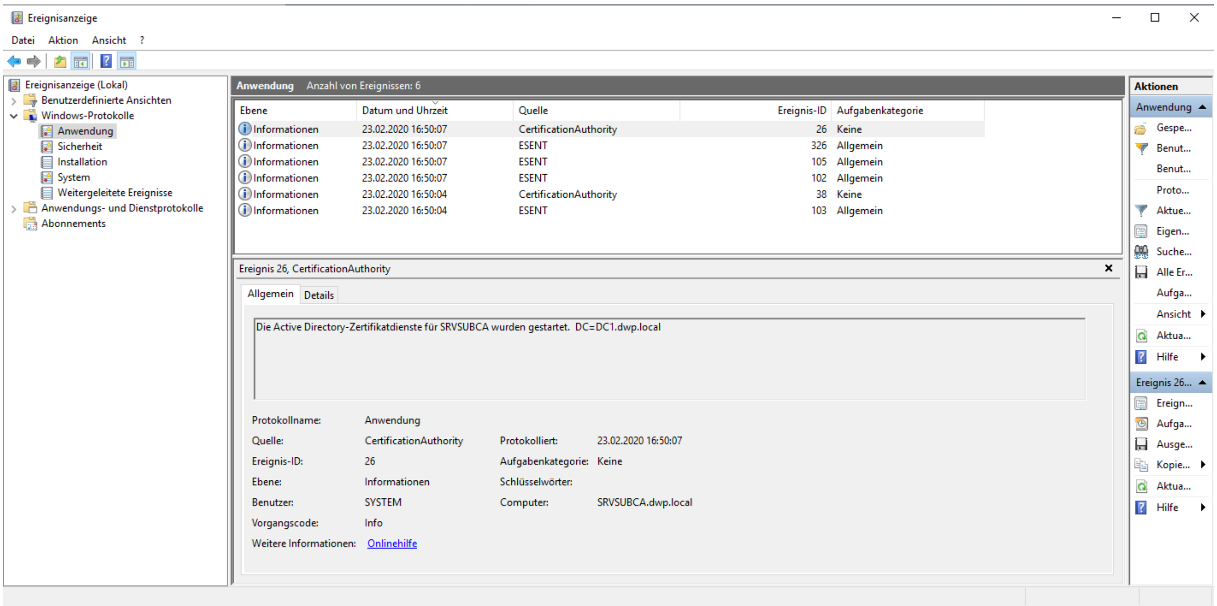
```
auditpol /set /subcategory:"Registrierung" /success:enable /failure:enable
```

```
auditpol /set /subcategory:"Registry" /success:enable /failure:enable
```



```
C:\Windows\system32>auditpol /set /subcategory:"Registrierung" /success:enable /failure:enable
Der Befehl wurde erfolgreich ausgeführt.

C:\Windows\system32>
```

Events:



Anwendung Anzahl von Ereignissen: 6

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	23.02.2020 16:50:07	CertificationAuthority	26	Keine
Informationen	23.02.2020 16:50:07	ESENT	326	Allgemein
Informationen	23.02.2020 16:50:07	ESENT	105	Allgemein
Informationen	23.02.2020 16:50:07	ESENT	102	Allgemein
Informationen	23.02.2020 16:50:04	CertificationAuthority	38	Keine
Informationen	23.02.2020 16:50:04	ESENT	103	Allgemein

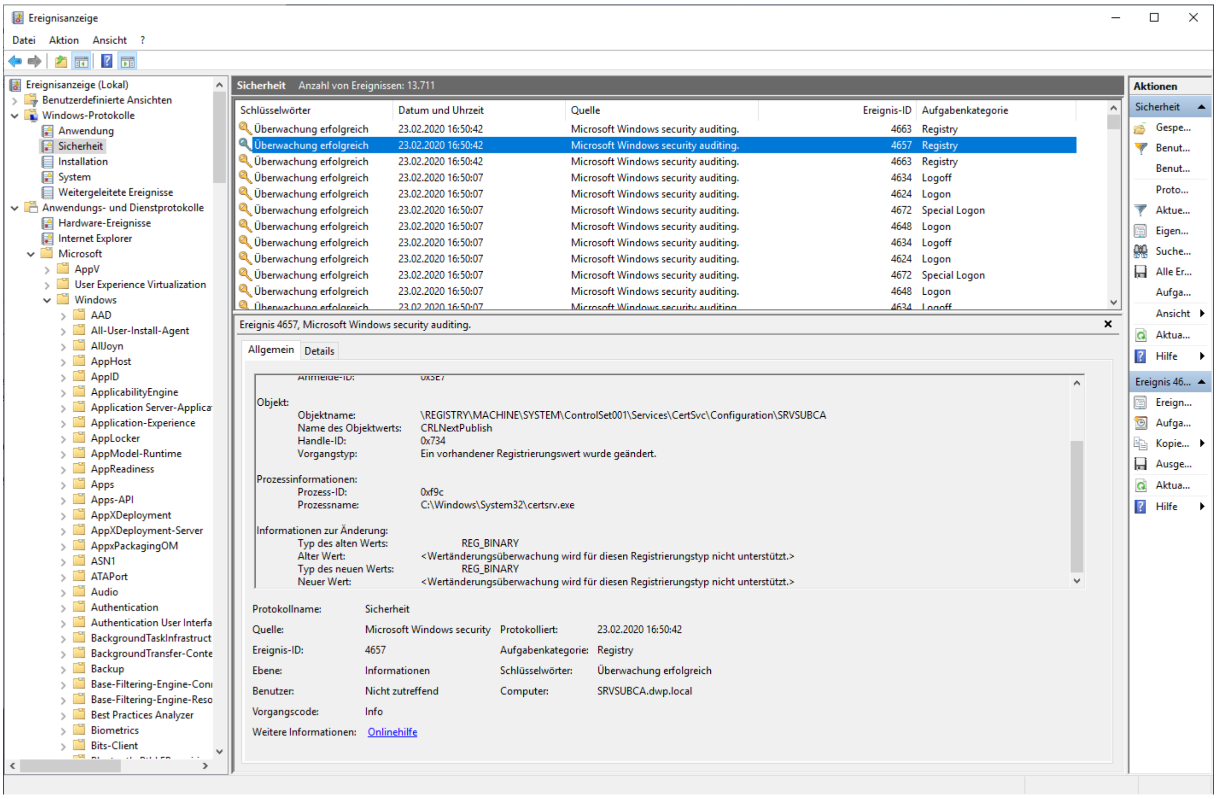
Ereignis 26, CertificationAuthority

Allgemein | Details

Die Active Directory-Zertifikatdienste für SRVSUBCA wurden gestartet. DC=DC1.dwp.local

Protokollname:	Anwendung		
Quelle:	CertificationAuthority	Protokolliert:	23.02.2020 16:50:07
Ereignis-ID:	26	Aufgabenkategorie:	Keine
Ebene:	Informationen	Schlüsselwörter:	
Benutzer:	SYSTEM	Computer:	SRVSUBCA.dwp.local
Vorgangscode:	Info		
Weitere Informationen:	Onlinehilfe		

CA Überwachung



Sicherheit Anzahl von Ereignissen: 13.711

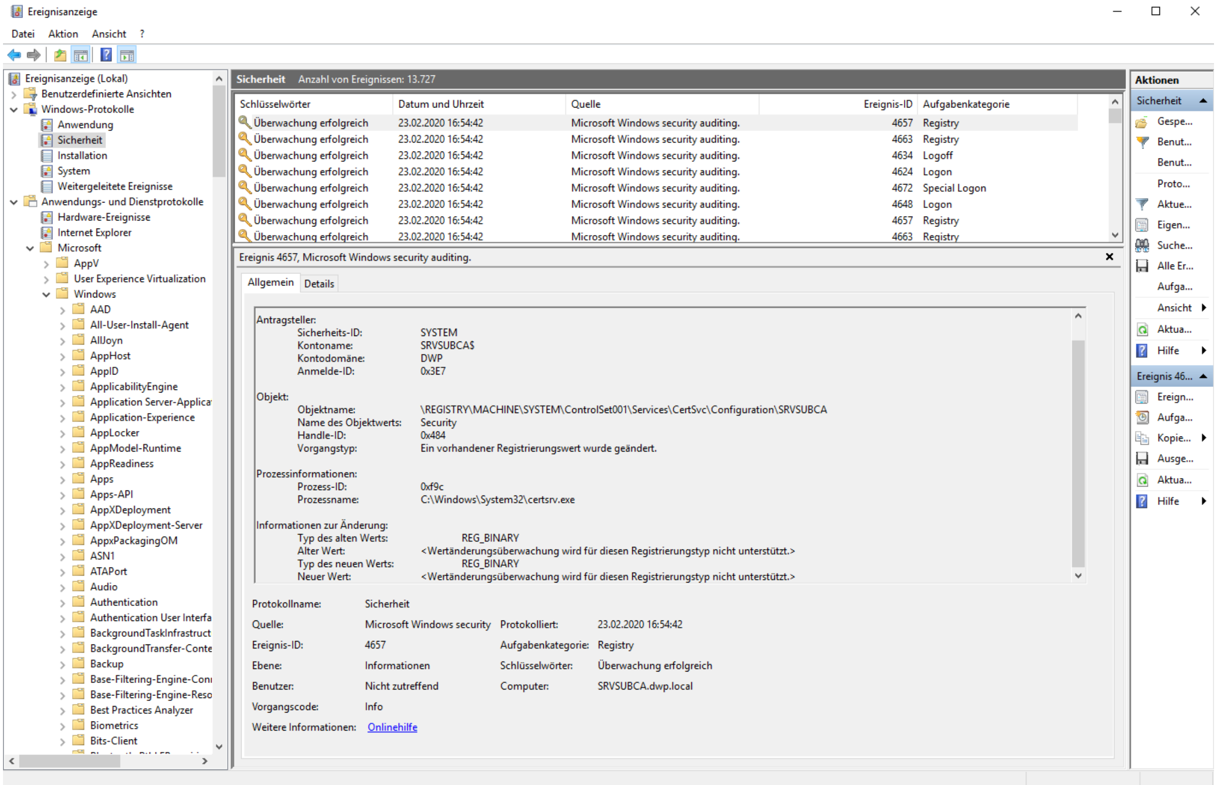
Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erfolgreich	23.02.2020 16:50:42	Microsoft Windows security auditing.	4663	Registry
Überwachung erfolgreich	23.02.2020 16:50:42	Microsoft Windows security auditing.	4657	Registry
Überwachung erfolgreich	23.02.2020 16:50:42	Microsoft Windows security auditing.	4663	Registry
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4634	Logoff
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4624	Logon
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4672	Special Logon
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4648	Logon
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4634	Logoff
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4624	Logon
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4672	Special Logon
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4648	Logon
Überwachung erfolgreich	23.02.2020 16:50:07	Microsoft Windows security auditing.	4634	Logoff

Ereignis 4657, Microsoft Windows security auditing.

Allgemein | Details

```
        Anmelde-ID:              0x3E7

Objekt:
        Objektname:              \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\CertSvc\Configuration\SRVSUBCA
        Name des Objektwerts:    CRLNextPublish
        Handle-ID:               0x734
        Vorgangstyp:             Ein vorhandener Registrierungswert wurde geändert.

Prozessinformationen:
        Prozess-ID:              0xf9c
        Prozessname:             C:\Windows\System32\certsrv.exe

Informationen zur Änderung:
        Typ des alten Werts:             REG_BINARY
        Alter Wert:              <Wertänderungsüberwachung wird für diesen Registrierungstyp nicht unterstützt.>
        Typ des neuen Werts:             REG_BINARY
        Neuer Wert:              <Wertänderungsüberwachung wird für diesen Registrierungstyp nicht unterstützt.>
```

Protokollname:	Sicherheit		
Quelle:	Microsoft Windows security	Protokolliert:	23.02.2020 16:50:42
Ereignis-ID:	4657	Aufgabenkategorie:	Registry
Ebene:	Informationen	Schlüsselwörter:	Überwachung erfolgreich
Benutzer:	Nicht zutreffend	Computer:	SRVSUBCA.dwp.local
Vorgangscode:	Info		
Weitere Informationen:	Onlinehilfe		



Sicherheit Anzahl von Ereignissen: 13.727

Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4657	Registry
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4663	Registry
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4634	Logoff
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4624	Logon
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4672	Special Logon
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4648	Logon
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4657	Registry
Überwachung erfolgreich	23.02.2020 16:54:42	Microsoft Windows security auditing.	4663	Registry

Ereignis 4657, Microsoft Windows security auditing.

Allgemein | Details

```
Antragsteller:
        Sicherheits-ID:          SYSTEM
        Kontoname:               SRVSUBCA$
        Kontodomäne:             DWP
        Anmelde-ID:              0x3E7

Objekt:
        Objektname:              \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\CertSvc\Configuration\SRVSUBCA
        Name des Objektwerts:    Security
        Handle-ID:               0x484
        Vorgangstyp:             Ein vorhandener Registrierungswert wurde geändert.

Prozessinformationen:
        Prozess-ID:              0xf9c
        Prozessname:             C:\Windows\System32\certsrv.exe

Informationen zur Änderung:
        Typ des alten Werts:             REG_BINARY
        Alter Wert:              <Wertänderungsüberwachung wird für diesen Registrierungstyp nicht unterstützt.>
        Typ des neuen Werts:             REG_BINARY
        Neuer Wert:              <Wertänderungsüberwachung wird für diesen Registrierungstyp nicht unterstützt.>
```

Protokollname:	Sicherheit		
Quelle:	Microsoft Windows security	Protokolliert:	23.02.2020 16:54:42
Ereignis-ID:	4657	Aufgabenkategorie:	Registry
Ebene:	Informationen	Schlüsselwörter:	Überwachung erfolgreich
Benutzer:	Nicht zutreffend	Computer:	SRVSUBCA.dwp.local
Vorgangscode:	Info		
Weitere Informationen:	Onlinehilfe		

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786422(v%3Dws.11)

Microsoft Windows® Security Auditing

Current Windows Event ID	Potential Criticality	Event Summary	Audit Filter Required	Description
4868	Low	The certificate manager denied a pending certificate request. Request ID: %1	Issue and manage certificate requests	
4869	Low	Certificate Services received a resubmitted certificate request. Request ID: %1	Issue and manage certificate requests	
4870	Low	Certificate Services revoked a certificate. Serial Number: %1 Reason: %2	Revoke certificates and publish CRLs	
4871	Low	Certificate Services received a request to publish the certificate revocation list (CRL). Next Update: %1 Publish Base: %2 Publish Delta: %3	Revoke certificates and publish CRLs	
4872	Low	Certificate Services published the certificate revocation list (CRL). Base CRL: %1 CRL Number: %2 Key Container: %3 Next Publish: %4 Publish URLs: %5	Revoke certificates and publish CRL	
4873	Medium	A certificate request extension changed. Request ID: %1 Name: %2 Type: %3 Flags: %4 Data: %5	Issue and manage certificate requests	If this functionality is not used by the CA, it may indicate tampering with a request
4874	Medium	One or more certificate request attributes changed. Request ID: %1 Attributes: %2	Issue and manage certificate requests	If this functionality is not used by the CA, it may indicate tampering with a request
4875	Low	Certificate Services received a request to shut down.	Start and stop Active Directory® Certificate Services	This event is triggered when the **certutil –shutdown** command is issued to the CA

Current Windows Event ID	Potential Criticality	Event Summary	Audit Filter Required	Description
4876	Low	Certificate Services backup started. Backup Type: %1	Back up and restore the CA database	
4877	Low	Certificate Services backup completed.	Back up and restore the CA database	
4878	Low	Certificate Services restore started.	Back up and restore the CA database	
4879	Low	Certificate Services restore completed.	Back up and restore the CA database	
4880	Low	Certificate Services started. Certificate Database Hash: %1 Private Key Usage Count: %2 CA Certificate Hash: %3 CA Public Key Hash: %4	Start and stop Active Directory® Certificate Services	
4881	Low	Certificate Services stopped. Certificate Database Hash: %1 Private Key Usage Count: %2 CA Certificate Hash: %3 CA Public Key Hash: %4	Start and stop Active Directory® Certificate Services	
4882	High	The security permissions for Certificate Services changed. %1	Change CA security settings	May indicate an attacker granting permissions for other accounts to enroll.
4883	Medium	Certificate Services retrieved an archived key. Request ID: %1	Store and retrieve archived keys	
4884	Low	Certificate Services imported a certificate into its database. Certificate: %1 Request ID: %2	Issue and manage certificate requests	
4885	High	The audit filter for Certificate Services changed. Filter: %1	Change CA security settings	May indicate an attacker disabling monitoring in an attempt to cover their

Current Windows Event ID	Potential Criticality	Event Summary	Audit Filter Required	Description
				tracks prior to certificate activities.
4886	Low	Certificate Services received a certificate request. Request ID: %1 Requester: %2 Attributes: %3	Issue and manage certificate requests	
4887	Medium	Certificate Services approved a certificate request and issued a certificate. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Issue and manage certificate requests	Issuance of certificates that contain usages that allow the owner to perform privileged operations (Enrollment Agent, Code Signing etc.) or certificates issued to VIP users should be monitored.
4888	Medium	Certificate Services denied a certificate request. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Issue and manage certificate requests	
4889	Low	Certificate Services set the status of a certificate request to pending. Request ID: %1 Requester: %2 Attributes: %3 Disposition: %4 SKI: %5 Subject: %6	Issue and manage certificate requests	
4890	High	The certificate manager settings for Certificate Services changed. Enable: %1 %2	Change CA security settings	May indicate tampering with permissions with what users are able to enroll on behalf of other users, commonly used to issue smart card certificates.
4891	Medium	A configuration entry changed in Certificate Services. Node: %1 Entry: %2 Value: %3	Change CA configuration	Can be used to monitor for changes to Policy/Exit modules on the CA or configuration of CDP/AIA extensions.
4892	Medium	A property of Certificate Services changed. Property:	Change CA configuration	Can be used to track changes to Key Recovery Agent configuration

Current Windows Event ID	Potential Criticality	Event Summary	Audit Filter Required	Description
		%1 Index: %2 Type: %3 Value: %4		
4893	Low	Certificate Services archived a key. Request ID: %1 Requester: %2 KRA Hashes: %3	Store and retrieve archived keys	
4894	Low	Certificate Services imported and archived a key. Request ID: %1	Store and retrieve archived keys	
4895	Low	Certificate Services published the CA certificate to Active Directory® Domain Services. Certificate Hash: %1 Valid From: %2 Valid To: %3		
4896	High	One or more rows have been deleted from the certificate database. Table ID: %1 Filter: %2 Rows Deleted: %3	Issue and manage certificate requests	May indicate an attacker covering their tracks after issuing certificates.
4897	Medium	Role separation enabled: %1	Change CA security settings	If role separation is used, this can be used to trigger an alert if the expected configuration changes.
4898	Medium	Certificate Services loaded a template. %1 v%2 (Schema V%3) %4 %5 Template Information: Template Content: %7 Security Descriptor: %8 Additional Information: Domain Controller: %6	Change CA security settings	Alert if templates that are not expected on a CA are loaded.
4899	Medium	A Certificate Services template was updated. %1 v%2 (Schema V%3) %4 %5 Template Change Information: Old Template Content: %8 New Template Content: %7 Additional	Change CA security settings	

Current Windows Event ID	Potential Criticality	Event Summary	Audit Filter Required	Description
		Information: Domain Controller: %6		
4900	Medium	Certificate Services template security was updated. %1 v%2 (Schema V%3) %4 %5 Template Change Information: Old Template Content: %9 New Template Content: %7 Old Security Descriptor: %10 New Security Descriptor: %8 Additional Information: Domain Controller: %6	Change CA security settings	

Microsoft-Windows-CertificationAuthority

Current Windows Event ID	Potential Criticality	Message
3	Low	Request failed
5	Low	Active Directory Certificate Services could not find required registry information. Services may need to be reinstalled.
6	Low	Active Directory Certificate Services issued a certificate for request %1 for %2.
7	Low	Active Directory Certificate Services denied request %1 because %2. The reques
8	Low	Active Directory Certificate Services left request %1 pending in the queue for %2
9	Low	The Active Directory Certificate Services did not start: Unable to load an externa
10	Low	Active Directory Certificate Services were unable to build a new certificate or cer
15	High	Active Directory Certificate Services did not start: Version does not match certif.d
16	Low	Active Directory Certificate Services did not start: Unable to initialize OLE: %1.
17	Low	Active Directory Certificate Services did not start: Unable to initialize the databas
19	Low	Active Directory Certificate Services did not start: The Subject Name Template st HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configurat An example of a valid string is: CommonName OrganizationalUnit Organization L
20	Low	Active Directory Certificate Services did not start: The Certificate Date Validity Pe HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configurat Valid strings are "Seconds", "Minutes", "Hours", "Days", "Weeks", "Months" and "

Current Windows Event ID	Potential Criticality	Message
21	Low	Active Directory Certificate Services could not process request %1 due to an erro
22	Low	Active Directory Certificate Services could not process request %1 due to an erro Additional information: %4
23	Low	Active Directory Certificate Services could not process request %1 due to an erro The certificate would contain an encoded length that is potentially incompatible w Submit a new request using different length input data for the following field: %
25	Low	Active Directory Certificate Services revoked the certificate for request %1 for %
26	Low	Active Directory Certificate Services for %1 was started.%2%3
27	Low	Active Directory Certificate Services did not start: Hierarchical setup is incomplet obtain a certificate for this Certificate Server, and use the CA administration tool complete the installation.
28	Low	Active Directory Certificate Services did not start: The Certificate Revocation List registry value HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cert Valid strings are "Seconds", "Minutes", "Hours", "Days", "Weeks", "Months" and "
29	Low	Active Directory Certificate Services issued a new Certificate Revocation List for
33	Low	Active Directory Certificate Services did not start: Could not create the Certificate %2.
34	Low	Active Directory Certificate Services did not start: Could not initialize RPC for %1
35	Low	Active Directory Certificate Services did not start: Could not initialize OLE for %1
38	Low	Active Directory Certificate Services for %1 was stopped.
39	Low	Active Directory Certificate Services did not start: The CA DCOM class for %1 co services administration tool to change the CA logon context.
40	Low	Active Directory Certificate Services did not start: Could not initialize DCOM class
41	Low	Active Directory Certificate Services did not start: Could not initialize DCOM Secu
42	Low	Could not build a certificate chain for CA certificate %3 for %1. %2.
43	Low	The "%1" Policy Module "%2" method caused an exception at address %4. The e
44	Low	The "%1" Policy Module "%2" method returned an error. %5 The returned status
45	Low	The "%1" Exit Module "%2" method caused an exception at address %4. The exc
46	Low	The "%1" Exit Module "%2" method returned an error. %5 The returned status c

Current Windows Event ID	Potential Criticality	Message
48	Low	Revocation status for a certificate in the chain for CA certificate %3 for %1 could currently unavailable. %2.
49	Low	A certificate in the chain for CA certificate %3 for %1 could not be verified becau describing how to check the revocation status. %2.
51	Low	A certificate in the chain for CA certificate %3 for %1 has been revoked. %2.
52	Low	Active Directory Certificate Services issued a certificate for request %1 for %2. A
53	Low	Active Directory Certificate Services denied request %1 because %2. The reques information: %4
54	Low	Active Directory Certificate Services left request %1 pending in the queue for %2
55	Medium	Active Directory Certificate Services unrevoked the certificate for request %1 for
56	Low	Active Directory Certificate Services denied request %1. The request was for %2
57	Low	Active Directory Certificate Services denied request %1. The request was for %2
58	Low	A certificate in the chain for CA certificate %3 for %1 has expired. %2.
59	Low	Active Directory Certificate Services did not start: Could not connect to the Activ
60	High	Active Directory Certificate Services refused to process an extremely long reques denial-of-service attack. If the request was rejected in error, modify the MaxInco parameter via certutil -setreg CA\MaxIncomingMessageSize <bytes>. Unless ver will not be logged again for 20 minutes.
62	Low	Active Directory Certificate Services had problems loading valid CRL publication v publication to its default settings.
63	Low	Active Directory Certificate Services did not start: %1 %2.
64	Low	Active Directory Certificate Services cannot publish enrollment access changes to
65	Low	Active Directory Certificate Services could not publish a Base CRL for key %1 to t %3.%5%6
66	Low	Active Directory Certificate Services could not publish a Delta CRL for key %1 to %3.%5%6
67	Low	Active Directory Certificate Services made %1 attempts to publish a CRL and will next CRL is generated.
68	Low	Active Directory Certificate Services successfully published Base CRL(s).
69	Low	Active Directory Certificate Services successfully published Delta CRL(s).

Current Windows Event ID	Potential Criticality	Message
70	Low	Active Directory Certificate Services successfully published Base and Delta CRL(s
71	Low	Active Directory Certificate Services successfully published Base CRL(s) to server
72	Low	Active Directory Certificate Services successfully published Delta CRL(s) to serve
73	Low	Active Directory Certificate Services successfully published Base and Delta CRL(s
74	Low	Active Directory Certificate Services could not publish a Base CRL for key %1 to t %4: %2. %3.%5%6
75	Low	Active Directory Certificate Services could not publish a Delta CRL for key %1 to %4: %2. %3.%5%6
76	Low	The "%1" Policy Module logged the following information: %2
77	Low	The "%1" Policy Module logged the following warning: %2
78	Low	The "%1" Policy Module logged the following error: %2
79	Low	Active Directory Certificate Services could not publish a Certificate for request % %3.%5%6
80	Low	Active Directory Certificate Services could not publish a Certificate for request % server %4: %2. %3.%5%6
81	Low	Active Directory Certificate Services key archival is only supported on Advanced S
82	Low	Active Directory Certificate Services could only verify %1 of %2 key recovery cer key archival. Requests to archive private keys will not be accepted.
83	Low	Active Directory Certificate Services encountered an error loading key recovery c private keys will not be accepted. %1
84	Low	Active Directory Certificate Services will not use key recovery certificate %1 beca as a Key Recovery Agent. %2 %3
85	Low	Active Directory Certificate Services ignored key recovery certificate %1 because
86	Low	Active Directory Certificate Services could not use the provider specified in the re
87	Low	Active Directory Certificate Services could not use the default provider for encryp
88	Low	Active Directory Certificate Services switched to the default provider for encryptio
90	Low	%1: Active Directory Certificate Services detected an exception at address %2. F
91	Low	Could not connect to the Active Directory. Active Directory Certificate Services w Active Directory access.

Current Windows Event ID	Potential Criticality	Message
92	Low	Active Directory Certificate Services could not update security permissions. %1
93	Low	The certificate (#%1) of Active Directory Certificate Services %2 does not exist i CN=NTAuthCertificates,CN=Public Key Services,CN=Services in the Active Direct directory replication may not be completed.
94	Low	Active Directory Certificate Services %1 can not open the certificate store at CN= Services,CN=Services in the Active Directory's configuration container.
95	High	Security permissions are corrupted or missing. The Active Directory Certificate S
96	Low	Active Directory Certificate Services could not create an encryption certificate. %
97	Low	Active Directory Certificate Services %1 will reduce the maximum lifetime of the because the CA certificate lifetime is shorter than the registry validity period. Co or reducing the registry validity period.
98	Low	Active Directory Certificate Services encountered errors validating configured key archive private keys will no longer be accepted.
99	Low	Active Directory Certificate Services could not create cross certificate %1 to certi %3.
100	Low	Active Directory Certificate Services did not start: Could not load or verify the cu
101	Low	Active Directory Certificate Services created CA cross certificate %2 for %1.
102	Low	Active Directory Certificate Services could not create cross certificate %1 to certi extension is inconsistent. %3. %4.
103	Low	Active Directory Certificate Services added the root certificate of certificate chain Root Certification Authorities Enterprise store on the CA computer. This store wil Authorities container in Active Directory the next time Group Policy is applied. To published correctly in Active Directory, run the following command: certutil -view quotation marks when you run this command). If the Root CA certificate is not p on the Root CA computer to export the certificate to a file, and then run the follo Active Directory: Certutil -dspublish %certificatefilename% Root.
104	Low	Active Directory Certificate Services published certificate %1 to %2.
105	Low	Active Directory Certificate Services deleted invalid certificate %1 from %2.
106	Low	Active Directory Certificate Services cannot add certificate %1 to %2. %3. %4.
107	Low	Active Directory Certificate Services cannot delete invalid certificate %1 from %2
108	Low	Active Directory Certificate Services could not delete a Certificate for request %1 %3.%5%6

Current Windows Event ID	Potential Criticality	Message
109	Low	Active Directory Certificate Services could not delete a Certificate for request %1 server %4: %2. %3.%5%6
110	Low	Active Directory Certificate Services could not initialize the performance counters
111	Low	Active Directory Certificate Services upgrade failed because the upgrade path co
112	Low	Active Directory Certificate Services upgrade failed because information required %1
113	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not cr shared folder with proper permissions. %1
114	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not cr
115	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not up
116	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not cr
117	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not cr
118	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not up
119	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not re
120	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not re
121	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not in
122	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not up
123	Low	A portion of the Active Directory Certificate Services upgrade failed: Could not up
124	Low	Active Directory Certificate Services upgrade succeeded. Active Directory Certific upgraded successfully.
125	Low	Active Directory Certificate Services upgrade failed. Active Directory Certificate S upgraded. %1
126	Low	Current information about advanced features supported by this CA is not availab and restart Certificate Services in order to update this information. %1
127	Low	Key recovery certificate %1 is about to expire soon and will not be used upon ex administrator to renew this certificate. %2 %3
128	Low	An Authority Key Identifier was passed as part of the certificate request %1. This enable specifying a CA key for certificate signing, run: "certutil -setreg ca\UseDe restart the service.

Current Windows Event ID	Potential Criticality	Message
129	Low	An invalid OID has been detected in the EnabledEKUForDefinedCACert configurat "certutil -getreg ca\EnabledEKUForDefinedCACert" to identify the invalid OID anc ("1.3.6.1.5.5.7.3.9") will be used.
130	Low	Active Directory Certificate Services could not create a certificate revocation list. that need to check the revocation status of certificates issued by this CA to fail. Y revocation list manually by running the following command: "certutil -CRL". If th Certificate Services.
131	Low	An invalid OID has been detected in the EKUOIDsForPublishExpiredCertInCRL co "certutil -getreg ca\EKUOIDsForPublishExpiredCertInCRL" to identify the invalid (("1.3.6.1.5.5.7.3.3" and "1.3.6.1.4.1.311.61.1.1") will be used.
132	Low	The CA was unable to perform a decryption operation. This error can occur when such as Advanced Encryption Standard (AES) is used and the CA has not been co Generation (CNG) key storage provider. If this error occurred during certificate e Template to ensure that advanced encryption for key archival is not enabled.
133	Low	The CA failed to encode a server extension required to validate a certificate or ce The CA will not issue any certificates or CRLs that do not contain this extension. snap-in to remove any Unicode characters in the URLs for the AIA, CDP, and IDP

Registry Values to Monitor

The following events are recommendations for advanced monitoring of registry changes that affect the security of a CA. While many of these same alerts are generated when enabling auditing on the CA, there are cases where values can be changed and no alert is generated. In those cases, registry auditing can be enabled and the following events can be monitored for.

In the table below, "Event ID" is the current Microsoft Windows® event ID for versions of Microsoft Windows® currently in mainstream support. "Text to Alert On" is the text to search for within the event body when an alert is generated. "Potential Criticality" identifies whether the event should be considered of low, medium or high criticality in detecting attacks. The event summary contains a brief description of the event.

Event ID	Text to Alert On	Potential Criticality	Event Summary
4657	"AuditFilter"	High	The audit filter controls which Microsoft Wind logged. Changing the audit filter may indicate logging prior to performing a certificate opera configured when the CA is created and not ch
4657	"EKUOIDsForPublishExpiredCertInCRL"	High	This value controls what types of certificates certificate expires. An attacker could remove Code Signing) that would allow a previously r was signed with to validate successfully agai publication.This value is not changed during

Event ID	Text to Alert On	Potential Criticality	Event Summary
4657	“EditFlags”	Medium	Alert if the new value enables EDITF_ATTRIB be identified by taking the value found in the a bitwise “AND” operation with 262144 (the c the EDITF_ATTRIBUTESUBJECTALTNAME2 va any certificate request to contain arbitrary alt
4657	"KRACertHash"	Medium	This will happen rarely in normal operations a a valid KRA certificate could assign it to a CA that are subsequently archived on the CA.
4657	"RoleSeparationEnabled"	Medium	Role separation allows for a CA to tightly con enforce that all users can only have one role Issuer, administrator, Auditor). A local admin separation, which may allow an account who an operation to be eligible for those rights.
4657	"Security"	High	This alert is raised when the permissions on t permissions control which users and groups a issue certificates, manage the CA settings an given CA. Modification could allow an attacke account for enrollment.This is a similar alert t
4657	"ExitModules","Active"	High	Indicates a change to the default exit module modules allow additional actions to be perfor occurs (issuance, revocation, CRL publishing, modules occur very infrequently in normal op tampering with the CA.
4657	"PolicyModules","Active"	High	Indicates a change to the active policy modul module control certificate issuance and is cha operations.