

<u>Inhalt</u>

Zielsetzung	2
Ist-Situation	2
Soll-Situation	2
Migrationsszenario	2
Vorbereitung	3
Berechtigungen	3
Review	3
Aufbau der neuen VM (mit Windows Update Problem)	7
Aufbau der neuen VM (Neuinstallation)	16
CleanUp PKI	19
Anpassungen an der PKI	23
Backup PKI	31
Migration	33
Austausch des Servers	33
Rolleninstallation	35
Problem mit 802.1x	37
Migration der ADCS	38
Anpassung und Überarbeitung der Sperrlistenverteilung	48
Grundkonfiguration und Ausstellung eines neuen Zertifizierungsstellen-Zertifikates	52
TroubleShooting – Korrektur des LDAP-Sperrlistenverteilungspunktes	57
Fortsetzung der Grundkonfiguration	62
Bereitstellung des Online Responders	63
Bereitstellung von CEPCES	74
Testphase	81
Aktivierung der PKI	88
Nacharbeiten	89
Konfiguration der Datensicherung	89
Monitoring	90
Updates	91
Bereinigungen	92
Problem Smartcard Logon	93
Problem Snort	97
Zusammenfassung	99

<u>Zielsetzung</u>

Ist-Situation

Ich betreibe in meiner Windows Server Infrastruktur eine eigene PKI. Diese wird durch den Server WS-CA1 bereitgestellt und läuft aktuell auf einem Windows Server 2016 Server Core. Es handelt sich dabei um eine Active Directory integrierte Root-Zertifizierungsstelle. Damals hatte ich keine Anforderung für eine mehrstufige PKI mit Offline-Root-CA.

Verschiedene Zertifikatvorlagen werden von meinen Systemen bei der automatischen Ausstellung von Zertifikaten genutzt. Die Zertifikate werden dabei nicht traditionell, sondern über **CEP-CES** ausgestellt (**C**ertificate Enrollment **P**olicy Service & **C**ertificate Enrollment Web **S**ervice). Diese beiden zusätzlichen Services auf meiner Zertifizierungsstelle ermöglichen die Anfrage und die Ausstellung von Zertifikaten über **HTTPS** statt **RPC-DCOM**, was eine Platzierung der Zertifizierungsstelle hinter einer Firewall deutlich vereinfacht.

Das Zertifizierungsstellen-Zertifikat läuft in den nächsten 12 Monaten aus.

Soll-Situation

Ich habe verschiedene Anforderungen für die Migration definiert:

- Das Betriebssystem soll auf Windows Server 2019 umgestellt werden.
- CEP-CES soll weiter genutzt werden.
- Zusätzlich soll ein Online Responder eine Echtzeitsperrprüfung ermöglichen.
- Das Sperrsystem soll später auch über das Internet erreichbar sein.
- Sperrlisten sollen nicht mehr über LDAP oder http erreichbar sein. Ich möchte nur noch über OCSP (Online Responder) verwenden.
- Eine Bereinigung der bisher ausgestellten Zertifikate ist durchaus sinnvoll.
- Das Zertifizierungsstellen-Zertifikat muss erneuert werden. Dabei können auch die neuen Certificate Revocation List Distribution Points veröffentlicht werden, denn diese werden in alle neuen Zertifikate integriert.
- Der Server Core hat mir mehr Probleme verursacht als Nutzen gebracht. Daher soll der neue Server mit der grafischen Oberfläche bereitgestellt werden.

Migrationsszenario

Durch die Besonderheit des erforderlichen neuen Zertifizierungsstellen-Zertifikats muss die Migration über mehrere Schritte geführt werden:

- **Cleanup**: Zuerst werde ich die Bereinigung und die Erneuerung des Zertifizierungsstellen-Zertifikats auf der alten Windows CA durchführen.
- Migration: Dann werde ich mittels Wipe & Load den Service auf das neue Betriebssystem verschieben. So kann ich den Namen des Betriebssystems weiterführen und die IPv4-Adresse wiederverwenden und erspare mir verschiedene Anpassungen in Richtlinien und Firewall-Regeln.
- Erweiterung: Zuletzt erweitere ich die PKI mit einem Online Responder.

Generell kann man an dieser Stelle auch über eine parallele, neue Zertifizierungsstelle sinnieren. Diese könnte frisch aufgesetzt und nach Wunsch konfiguriert zuerst ausgiebig getestet werden. Anschließend könnte man alle bisher ausgestellten und noch gültigen Zertifikate auf allen Systemen mit der neuen CA erneut ausstellen. Wenn keine Zertifikate der alten CA mehr in Verwendung sind, dann könnte diese einfach abgeschaltet werden. Durch das bereits ablaufende Zertifizierungsstellen-Zertifikat ist die Restlaufzeit einiger ausgestellter Zertifikate bereits reduziert (Eine Zertifizierungsstelle kann keine Zertifikate über ihre eigene Gültigkeit hinaus signieren). Die vielen Windows Systeme könnten bequem durch Gruppenrichtlinien automatisiert migriert werden. Aber in meinem Fall sind auch fast alle Nicht-Windows-Systeme mit Zertifikaten versorgt: Das sind z.B. alle Netzwerkgeräte. Und da würde mir eine Umstellung der Zertifikate mehr Arbeit bereiten als eine Bereinigung und Migration der alten CA.

Daher bleibe ich beim Wipe & Load.

Vorbereitung

Berechtigungen

Für den Zugriff auf meine PKI bzw. den Review sind mehrere Gruppenmitgliedschaften erforderlich. Diese delegiere ich mit meinem PAM-Script für 24 Stunden an meine Admin-Kennung:

🛥 PAM-Admin(GUI - verbunden mit	t WS-DC1.ws	its (Version V2.00)							- 0]	×
Zeitraum: Ziel-DC:	24 Stunden	~		21	allen DC replizieren Die automatische AD-F	Replikation ist	t akt	tiv.				
Security-Tiers:		Admins:			mögliche Gruppen:		a	aktive Mitgliedschaften:				
ale		stephan-T	1	X	GG-Admin-AD-GPO	x		C701-1-1	·			x
Terd - Domain Adv Terd - Strenz Admir Terd - Client Admir Terd - Service Adr	niedztałon odrzeton nietzko nin				UG-Admin-AD-Jan GG-Admin-AD-Jan GG-Admin-Backup GG-Admin-Backup GG-Admin-DNS GG-Admin-DNS GG-Admin-Stageton GG-Admin-Stageton GG-Admin-Stage-Sarever GG-Admin-MK GG-Admin-MK-Storage GG-Admin-MK-Storage GG-Admin-MK-Storage GG-Admin-MK-Storage GG-Admin-MK-Storage GG-Admin-MK-Storage GG-Admin-MK-Storage GG-Admin-MK-Storage GG-Admin-MK-Admin GG-Admin-MK-Admin GG-Admin-MK-Admin GG-Admin-MK-Admin GG-Admin-MK-Admin GG-Admin-MK-Admin GG-SEC-Sarever-File-Admine GG-SEC-Sarever-File-Admine GG-SEC-Sarever-Rib-Admine GG-SEC-Sarever-Rib-Admine GG-SEC-Sarever-Rib-Admine GG-SEC-Sarever-Rib-Admine GG-SEC-Sarever-Rib-Admine GG-SEC-Sarever-Rib-Admine GG-SEC-Sarever-Rib-Admine Cg-SEC-Sarever-Rib-Admine SG-SEC-Sarever-Rib-Admine			Giblgeet Gr attisch Pr 2020-11-29 09:31:33 Gr 2020-11-29 09:31:33 Gr 2020-11-29 09:31:33 Gr 2020-11-29 09:31:33 Gr	inpe Gr-Admin-Mperi-Gorage Gr-Admin-PKI GSEC-Server-HyperV-Admins GSEC-Server-Standard-Admins			
bereit - Wähle ein	e Gruppe zur Bearbe	itung der Mitg	liedschaft aus.		hinzufügen		ł	entfernen entfern	rne alle			

Die Gruppe "GG-Admin-PKI" ist in eine Gruppe "LD-Admin-PKI" verschachtelt, welcher ich die administrativen Rechte in meiner PKI delegiert habe.

<u>Review</u>

So ausgestattet verbinde ich mich mit meiner Admin-Kennung auf meinen Admin-Server. Dort hatte ich mir eine Management-Konsole für den Remotezugriff auf die PKI-Services erstellt – der Server WS-CA hat ja als Server Core keine grafische Oberfläche.

Beginnen wir mit den Zertifikatvorlagen. Ich denke, die Namensgebung sagt genug aus:

■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ Datei Aktion Ansicht Favoriten Fenster ? ■ # # ■ With Statistication Controller-V2 Smattard-Anmeldung Clientauthentif ■ With Statistication Ferritikate ■ WS-ITS-CodeSignatur-V2 Codesignatur ■ Ausstehende Anforderungen ■ Fehlgeschlagene Anforderungen ■ # ##################################	🚪 PKI - [Konsolenstamm\Zertifizierungsstelle (WS-CA1.ws.its)\WS-ITS-Zertifizierungsstelle-CA1\Zertifikatvorlagen] - 🛛									
 Konsolenstamm Zetrificatvorlagen (WS-DC1.ws.it), WS-ITS-SmartCard-V2 WS-ITS-Certificaterungstelle-CA1 Gesperte Zetrifikate Aussgestelle Zetrifikate Aussgestelle Zetrifikate Mare Beabsichtigter Zweck WS-ITS-CodeSignatur WS-ITS-Computer-V2 KDC-Authentifizierung Serverauthentifizierung WS-ITS-Benutzer-V2 Serverauthentifizierung WS-ITS-Benutzer-V2 Clientauthentifizierung WS-ITS-Benutzer-V2 Clientauthentifizierung WS-ITS-Benutzer-V2 Serverauthentifizierung Serverauthentif	🚟 Datei Aktion Ansicht Favoriten Fen	ister ?			_ 8 ×					
 Konsolenstamm Zertifikatvorlagen (WS-DC1.ws.its) WS-ITS-Zertifizierungsstelle-CA1 Gesperte Zertifikate Ausstehende Anforderungen Fehigeschlagen e Anforderungen Tertifikatorlagen WS-ITS-Benutzer-V2 Serverauthentifizierung WS-ITS-Benutzer-V2 Clientauthentifizierung WS-ITS-Benutzer-V2 Clientauthentifizierung WS-ITS-Benutzer-V2 VS-ITS-Benutzer-V2 Gesperte Zertifikate Mustehende Anforderungen Tehigeschlagen Ausstehende Anforderungen Tehigeschlagen MS-ITS-Benutzer-V2 VS-ITS-Benutzer-V2 	🗢 🔿 🙍 🖬 🙆 🖬									
	 Konsolenstamm Zertifikatvorlagen (WS-DC1.ws.its) Zertifikierungsstelle (WS-CA1.ws.its) Zertifikierungsstelle (WS-CA1.ws.its) Gesperte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Fehlgeschlagene Anforderungen Zertifikatvorlagen Juternehmens-PKI Online-Responder: 	Name WS-ITS-SmartCard-V2 WS-ITS-DomainController-V2 WS-ITS-CodeSignatur-V2 WS-ITS-Webserver-V2 WS-ITS-Computer-V2 WS-ITS-Benutzer-V2	Beabsichtigter Zweck Smartcard-Anmeldung, Clientauthentif KDC-Authentifizierung, Smartcard-An Codesignatur Serverauthentifizierung Clientauthentifizierung Clientauthentifizierung							

Das Zertifizierungsstellen-Zertifikat wurde bereits einmal erneuert. Das aktuelle ist jetzt weniger als 12 Monate gültig:

PKI - [Konsolenstamm\Zertifizier	ungsstelle (WS-CA1.)	ws.its)\WS-ITS-Zertifizien	ungsstelle-CA1\Zertifikatv	orlagen]	– 🗆 X
🚟 Datei Aktion Ansicht Favr	ritan Eanstar ?				_ & ×
🗢 🔿 🙍 📰 🧔 📑 🛛 🛙	Eigenschaften von V	/S-ITS-Zertifizierungsstel	le-CA1 ? X		,
 Konsolenstamm Zertifikatvorlagen (WS-DC1.» Zertifizierungsstelle (WS-CA1 WS-ITS-Zertifizierungsstelle (WS-CA1 Gesperte Zertifizierungssteller Zertifikat Ausgestelltet Zertifikat Ausgehende Anforde 	Speicherung Überwachung Allgemein Richt Zertifizierungsstell Name: Zertifizierungsstell	Zertifikatverwaltungen Wiederherstellungs-A linienmodul Beendigun WS-ITS-Zertifizierungs enzertifikate:	Registrierungs-Agents gents Sicherheit gsmodul Erweiterungen stelle-CA1	veck Idung erung, ierung erung	Zertifikat
 Fehlgeschlagene Anfreit Zertifikatvorlagen Junternehmens-PKI Sonine-Responder: 	Zertifikat Nr.0 (ab Zertifikat Nr. 1	gelaufen)		erung	Dieses Stammizertrünkt erschemt auf dem Remotecomputer verfrauenswürdig zu sein. Verifizieren Sie das Stammzertrifikat auf dem Remotecomputer, um sicher zu stellen, dass das Stammzertrifikat dort gültig ist.
	- Kryptografieeinste Anbieter: Hashalgorithmus:	lungen Microsoft Software Key SHA256	Zentifikat anzeigen Storage Provider		Ausgestellt von: WS-ITS-Zertifizierungsstelle-CA1 Gültig ab 15. 10. 2016 bis 15. 10. 2021 Ausstellerenklärung
	0	K Abbrechen	Obernehmen Hilfe		ок —

Zertifikate müssen auch gesperrt werden können, wenn sie z.B. kompromittiert wurden. Dafür müssen aber im Vorfeld Sperrlistenverteilungspunkte definiert werden. Ich habe damals den Webserver, der auf der Windows CA für CEPCES erforderlich ist, auch für die Veröffentlichung der CRL (**C**ertificate **R**evocation **L**ist) verwendet. Den Zugriff auf die Web-Ressource hatte ich an einen CNAME crl.ws.its gebunden. So hätte ich jederzeit eine Verschiebung auf einen anderen Webserver vornehmen können. Zusätzlich habe ich im Active Directory die Sperrliste veröffentlicht:

Datei Aktion Ansicht Favrähler Einstein von WS-ITS-Zertifizierungsstelle-CA1 ? ×]	- 8 ×
Konsolenstamm Speicherung Zertifikatvorlagen (WS-DC1, V Zertifikatvorlagen (WS-DC1, V Wederhenstellungs-Agents Sicherheit Augemein Richtliniermodul Beendigungsmodu Erweiterungen Erweiterungen Gesperrte Zertifikat Speinsten-Verteilungspunkt Imagemeinstellungs-Agents Ausgestellte Zertifikat Speinsten-Verteilungspunkt Imagemeinstellungs-Agents Phelgeschlagener Anfr Zertifikatvorlagen Imagemeinstellungsverteilte and von denen Benutzer eine Zertifikatspentiste Imagemeinstellungsverteilte Zertifikat Geben Sie Standorte an, von denen Benutzer eine Zertifikatspentiste Imagemeinstellungsverteilte Zertifikat Geben Sie Standorte an, von denen Benutzer eine Zertifikatspentiste Imagemeinstellungsverteilte Zertifikatspentiste Imagemeinstellungsverteilte and von denen Benutzer eine Zertifikatspentiste Imagemeinstellungsverteilte Zertifikatspentiste Imagemeinstellungsverteilte and von denen Benutzer eine Zertifikatspentiste Imagemeinstellungsverteilte Zertifikatspentiste Imagemeinstellungsverteilte and von denen Benutzer eine Zertifikatspentiste Imagemeinstellungsverteilte Zertifikatspentiste Imagemeinsten zertifikatspentiste Imagemeinstellungsverteilte Zertifikatspentiste Imagemeinsten zertifikatspentiste Imagemeinstellungsverteilte Zertifikatspentiste Imagemeinsten einbez	veck Idung, Clientauthentif erung, Smartcard-An erung erung erung	

Der Pfad c:\admin... in den Verteilungspunkten ist das Backend-Verzeichnis des lokalen Webservers. Hier legt die CA die Sperrliste ab. Über den mittleren Eintrag wird dann der Zugriff über http definiert.

In den Stelleninformationen schaut es weniger angepasst aus. Diese arbeiten mit den Default-Settings:



\overline PKI - [Konsolenstamm\Zertifizie	erungsstelle (WS-CA1.ws.its)\WS-ITS-Zertifizier	ungsstelle-CA1\Zertifikatvo	rlagen]	- 🗆 ×
搹 Datei Aktion Ansicht Fav	/ ?			- 8 ×
🗢 🄿 🙍 📅 🔯 🔒 👔 🛛	Eigenschaften von WS-ITS-Zertifizierungsstel	lle-CA1 ? X		
 Konsolenstamm Zertifikatvorlagen (WS-DC1.x Zertifikatvorlagen (WS-DC1.x Zertifikatrongsstelle (WS-CA.x) Gesperte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Gethjeschlagene Anford Zertifikatvorlagen Unternehmens-PKI Online-Responder: 	Speicherung Zertifikatverwaltungen Oberwachung Wiederherstellungs-A Allgemein Richtlinienmodul Beendigun Erweterung auswählen: Zugriff auf Stelleninformationen Geben Sie Standorte an, von denen Benutzer e Zertifizierungsstelle erhalten können. Galym 20. Nor-CA Truncaterd Name >. Chet Ernoll V-Server Klapp://-O.Ne-CA Truncaterd Name >. Chet Ernoll V-Server file //-ServerDNSName >/Cert Ernoll /-Server K	Registrierungs-Agents sgents Sicherheit gramodul Erweiterungen ein Zertfikat dieser sorefDISVences - Colvence In Pubble Key Swrices CH-S DNSName> - Colvame> - Cer NSName> - Colvame> - Cer NSName> - Colvame> - Cer > 2ufügen Entfemen	veck Idung, Clientauthentif erung, Smartcard-An erung erung erung	
	In AIA-Erweiterung des ausgestellten Zertifik In Online Certificate Status-Protokoll (OCSP) OK Abbrechen	ats einbeziehen -Erweiterungen einbeziehen Obernehmen Hilfe		

Ein wichtiger Punkt bei der Planung der Migration ist das Vorhandensein von archivierten, privaten Schlüsseln. Diese können Teil eines Recovery-Szenarios sein und machen immer dann Sinn, wenn Benutzer die ausgestellten Zertifikate für Datenverschlüsselungen verwenden (können). Verliert der Benutzer nach einer Verschlüsselung sein Zertifikat mit dem Private Key, dann kann er seine Daten selber nicht mehr entschlüsseln! In meiner CA habe ich darauf geachtet, dass die ausgestellten Zertifikat-Vorlagen keine Verschlüsselung ermöglichen. Daher hatte ich für die Archivierung auch keine Notwendigkeit:

PKI - [Konsolenstamm\Zertifizier	rungsstelle (WS-CA1.ws	.its)\WS-ITS-Zertifizierungss	telle-CA1\Zertifikatvo	vrlagen]	×
	Eigenschaften von WS	-ITS-Zertifizierungsstelle-CA	1 ? X		
 Konsolenstamm Zertifikatvorlagen (WS-DC1.v Zertifizierungsstelle (WS-C41.v WS-ITS-Zertifizierungsste Gesperrte Zertifikate Ausgestellte Zertifikat Ausgestellte Zertifikat Fehlgeschlagen en Anforde Fehlgeschlagen en Anforde Zertifikatvorlagen 	Speicherung Algemein Richtlin Überwachung Folgenden Vorgang du Schlüsselarchivierung Schlüssel archivier Anzahl der zu verv	Zertfikatverwaltungen F ienmodul Beendigungsmor Wiederherstellungs-Agents urchführen, wenn die Zertfikata enthält: hivieren en endenden Wiederherstellungs-	Registrierungs-Agents dul Erweiterungen Sicherheit nforderung Agents:	veck Idung, Clientauthentif erung, Smartcard-An erung erung erung	
 A Unternehmens-PKI P Online-Responder: 	Antragsteller	Aussteller Ablaufdat	n Ansicht		
	OK	Abbrechen Obern	ehmen Hilfe		

Hinweis: Wenn die alte CA über archivierte Schlüssel verfügt, dann ist eine Side-by-Side-Migration – also der Aufbau einer neuen CA und das Ablösen der alten CA – wesentlich schwieriger. Denn selbst wenn alle Benutzer neue Zertifikate erhalten haben und diese für Verschlüsselungen verwenden können: Es kann immer noch Daten geben, die mit den alten Zertifikaten verschlüsselt wurden. Und für eine Entschlüsselung benötigen die Benutzer demnach auch die alten Zertifikate!

Mit PKIVIEW prüfe ich den Zustand der Verteilungspunkte. Hier ist alles ok:

WS IT-Solutions

WSHowTo – Migration einer Windows PKI (WS-CA1) 2020-11-28 Migration auf Windows Server 2019

🚟 PKI - [Konsolenstamm\Unternehmens-PKI\W	/S-ITS-Zertifizierungsstelle-CA1 (V1	.1)]		- [-	×
🚟 Datei Aktion Ansicht Favoriten Fens	ter ?					. 8 ×
🗢 🔿 📶 🍳 🗟 🖬						
 Konsolenstamm Zertifikatvorlagen (WS-DC1.ws.its) WS-UTS-Zertifizierungsstelle (WS-CA1.ws.its) WS-ITS-Zertifizierungsstelle-CA1 Gesperte Zertifikate Ausgetellte Zertifikate Ausgetellte Zertifikate Fehlgeschlagene Anforderungen Fehlgeschlagene Anforderungen WINTEN-Ertifizierungsstelle-CA1 (V1: Online-Responder: WS-WAC.ws.its 	Name Zertifizierungsstellenzertifikat JAIA-Speicheront #1 AIA-Speicheront #2 E Speicheront für Sperrilsten E DeltaCRL-Speicheront #1 E DeltaCRL-Speicheront #2 E Speicherort für Sperrilsten	Status OK OK OK OK OK OK	Ablaufdatum 15.10.2021 18:15 15.10.2021 18:15 04.12.2020 04:36 29.11.2020 04:37 04.12.2020 04:37 04.12.2020 04:36	Ort Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1,CN=AIA,CN=Pu http://ws-ca1.ws.its/CertEnroll/WS-CA1.ws.its_WS-ITS-Zertifizi Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1(1),CN=WS-CA1, Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1(1),CN=WS-CA1, http://crl.ws.its/crld/WS-ITS-Zertifizierungsstelle-CA1(1)crl http://crl.ws.its/crld/WS-ITS-Zertifizierungsstelle-CA1(1).crl		

Das Verzeichnis c:\admin... enthält die Sperrlisten-Dateien:

📕 🖓 📑 = PKI							- 0	×
Datei Start Freigeben Ansicht								~ 🕐
An Schnellzugriff Kopieren Einfügen anheften	sschneiden ad kopieren rknöpfung einfügen			Neuer Ordner			Alles auswählen Nichts auswählen	
Zwischenablage		Organisieren		Neu	Offnen		Auswanien	
$\leftarrow \rightarrow \land \uparrow \square$ Netzwerk \rightarrow ws-ca1 \rightarrow cS	Admin	> PKI			~ 0	"PK	" durchsuchen	2
✓	Nam	ne A	Ände	rungsdatum	Тур	Größe		
✓		web.config	02.01	.2020 16:14	CONFIG-Datei		1 KB	
✓	×: \	WS-ITS-Zertifizierungsstelle-CA1(1).crl	26.11.2020 16:27		Zertifikatssperrliste		2 KB	
🗸 📙 Admin	WS-ITS-Zertifizierungsstelle-CA1(1)+.crl			.2020 16:27	Zertifikatssperrliste		1 KB	
	×:	WS-ITS-Zertifizierungsstelle-CA1.crl	26.11	.2020 16:27	Zertifikatssperrliste		1 KB	
> PSTranscript	×: \	WS-ITS-Zertifizierungsstelle-CA1+.crl	27.11	.2020 16:27	Zertifikatssperrliste		1 KB	
> Benutzer								
> 🔜 inetpub								
Logs								
> PerfLogs								
> 🔄 Program Files (x86)								
> Programme								
> Windows								
> 📮 CertEnroll								
> 📴 Systemsteuerung								
Papierkorb								
5 Elemente								

Der Server wird als VM auf einem meiner Hyper-V-Server ausgeführt. Die Systemanforderungen sind überschaubar:



Hyper-V-Manager								– 🗆 X
Datei Aktion Ansicht	?							
🗢 🔿 🖄 🖬 🚺								
Hyper-V-Manager WS-HV1	Virtuelle Computer							
WS-HV2	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status		Konfiguratio
	WS-ACAD	Wird ausgeführt	0 %	2048 MB	5.20:57:42			8.0
	WS-CA1	Wird ausgeführt	0 %	1234 MB	10.05:45:13			8.0
	WS-CL6	Wird ausgeführt	0 %	1188 MB	9.06:12:52			9.0
	WS-CL8	Wird ausgeführt	0 %	1302 MB	10.06:20:47			9.0
	🗧 WS-DC2	Wird ausgeführt	4 %	4912 MB	9.03:21:06			9.0
	🗧 WS-DPM	Wird ausgeführt	0 %	4096 MB	4.05:13:50			9.0
	WS-FS2	Wird ausgeführt	0 %	1398 MB	2.05:11:30			9.0
	🗄 WS-MON	Wird ausgeführt	0 %	3868 MB	4.05:47:42			8.0
	WS-MX2	Wird ausgeführt	11 %	16384 MB	4.05:21:16			9.0
	WS-PFS1b	Wird ausgeführt	0 %	5120 MB	26.20:37:12			8.0
	WS-RDS2	Wird ausgeführt	0 %	3576 MB	10.05:30:29			8.0
	WS-Steuer-alt	Aus						8.0
	WS-WAC	Wird ausgeführt	0 %	2048 MB	10.05:03:49			9.0
	Prüfpunkte							$\overline{\bullet}$
	WS-CA1							
	Erstellt: Konfigur	1: ationsversion: 8	9.10.2016 17:46:50 0	D		Grupj Takt:	piert: Nein OK (Anwendungen	fehlerfrei)
	ion: 2							
	ung: #	CLUSTER-INVARI	ANT#:{c89fe344-2319-43	0a-a485-cebbc9194	85a}			
	Zusammenfassung Arbeitssp	eicher Netzwerk	Replikation					
WS-HV2: Ein virtueller Compu	iter ausgewählt.							

Die System-Festplatte ist recht klein geblieben:

	Enstellungen für Worlden auf Worl	184				^
🔜 📝 🔜 🖛 WS-CA1						- 🗆 X
Datei Start Freigeben Ansicht						~ 🕐
← → × ↑ 🔒 > Dieser PC > Tier-Silver (W:)) > Hyper-V > WS-CA1				~ Č	"WS-CA1" d ,0
> 👳 Freigaben (M:)	Name ^	Änderungsdatum	Тур	Größe		
✓	HDD0.vhdx	28.11.2020 09:41	Festplatten-Image	27.889.664		
✓ Hyper-V						
VI WS-CA1						
Planned Virtual Machines						
Snapshots						
UndoLog Configuration						
> Virtual Machines						
> KWS-CL8						
> KWS-DC2						
> KWS-DPM						
> 🔜 WS-FS2						
> 🔜 WS-MON						
> 🔜 WS-MX2						
> KWS-PFS1b						
> KWS-RDS2						
> KS-WAC						
Y 👝 Tier-Silver (W:)						
Base						
V Hyper-V						
WS-CA1						
> WS-CL6						
> 👝 Tier-Bronze (X:)						
1 Element						

Es gibt keine geplanten Aufgaben.

Aufbau der neuen VM (mit Windows Update Problem)

Auf meinem Hyper-V-Server ist noch ausreichend Platz für die neue VM:



Ich kopiere mir ein Basefile mit Windows Server 2019 in das alte Verzeichnis:

WS IT-Solutions

📕 🛃 🥃 🗸 Virtual Hard Disks								- 🗆	×
Datei Start Freigeben Ansicht									~ 🕐
← → × ↑ 📙 > Dieser PC > Tier-Silver	W:) > Hyper-V > WS-	CA1 > Virtual Hard Disks					√ Ö	"Virtual Har	P
WS-DPM	^ Name	^	Änderungsdatum	Тур		Größe			
WS-FS2									
WS-MON			Die	er Ordner ist l	leer.				
WS-MX2									
WS-PFS1b									
WS-RDS2									
WS-WAC									
Tier-Silver (W:)		4% abgeschlossen		_		×			
Base		Ein Element wird von Bas	e nach Virtual Hard [isks kopiert					
Hyper-V		4% abgeschlossen			п	×			
WS-CA1									
Virtual Hard Disks				Geschwindig	keit: 114 I	MB/s			
WS-CL6									
Tier-Bronze (X:)									
Bibliotheken		Name: Win2019-2005.vho Restdauer: Ungefähr 2 M	dx inuten und 45 Sekun	den					
Metzwerk		Verbleibende Elemente: 1	(17,2 GB)						
ws-hv1									
Base		(Weniger Details							
Hyper-V									
Systemsteuerung									
Papierkorb									
0 Elemente	•							E	

Dann erstelle ich eine neue VM mit dem gleichen Bezeichner im gleichen Verzeichnis:

Hyper-V-Manager		- 🗆 X
Datei Aktion Ansicht ?	🖳 Assistent für neue virtuelle Computer	×
← ♠ ▲ Image: Imag	 Assistent für neue virtuelle Computer Name und Pfad angeben Vorbemerkungen Name und Pfad angeben Generation angeben Speicher zuweisen Installationsoptionen Zusammenfassung Wituelle Computer in Speicher oft sind einen neue Ordner, oder verwenden Sis tanden Ordner gespeichert, der für diesen Speicher oft speicher Wetuelke Computer in site kainen Ordner auswahlen, wird der virtuelle Computer in Standardordner gespeichert, der für diesen Server konfiguriert ist. Wituellen Computer an einem anderen Speicherort speicher Wituelen Computer sinen neuer Ordner, oder verwenden Sis tanden Ordner gespeichert, der für diesen Server konfiguriert ist. Wituelen Computer an einem anderen Speicherort speicher Wetuelen Computers und benötigen daher möglicherweise sehr viel Speicherplatz. Wetuelen Computers und benötigen daher möglicherweise sehr viel Speicherplatz. 	gen astung. 8.0 9.0 9.0 9.0 9.0 3ie einen 8.0 8.0 8.0 suchen 8.0 se 9.0 9.0 9.0 9.0 9.0 9.0 9.0 8.0 8.0 8.0 8.0 9.0 9.0
Zusammerfassung	rbeitsspeicher Netzwerk Replikation	



Hyper-V-Manager				- 🗆 X
Datei Aktion Ansicht ?		Sistent für neue virtuelle	Computer 2	×
Hyper-V-Manager WS-HV1 WS-HV2 Na	rtuelle Computer ame WS-ACAD WS-CL6 WS-CL8 WS-DC2 WS-DM WS-FS2 WS-MNN WS-FS2 WS-MNN WS-FS1b WS-FS1b	Abschließen of Vorbemerkungen Name und Pfad angeben Generation angeben Speicher zuweisen Netzwerk konfigurieren Virtuelle Festplatte verbinden Zusammenfassung	Der Assistenten für neue virtuelle Computer Der Assistent für neue virtuelle Computer wurde erfolgreich abgeschlossen. Der folgende virtuelle Beschreibung: Wame: WS-CA1 Generation: Generation 2 Arbeitsspeicher: 2.048 MB Netzweit: LAI-100 Festplatte: Keine	Konfiguratio 8.0 9.0 9.0 9.0 9.0 9.0 9.0 9.0 8.0 8.0 8.0 8.0 8.0
Pri WS	WS-Steuer-ait WS-WAC üfpunkte S-CA1		Klicken Sie auf 'Fertig stellen', um den virtuellen Computer zu erstellen und den Assistenten zu beenden.	8.0 9.0 ••••••••••••••••••••••••••••••••••••
Zu	usammenfassung /	Arbeitsspeicher Netzwerk Replika	< Zurück Weiter > Fertig stellen Abbrechen]

Damit ich nicht durcheinanderkomme, benenne ich den neuen Server um:

Hyper-V-Manager							- 0	×
Datei Aktion Ansicht ?								
🗢 🔿 🖄 🖬 🚺								
Hyper-V-Manager WS-HV1	Virtuelle Computer							
WS-HV2	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio	^
	WS-ACAD	Wird ausgeführt	0 %	2048 MB	5.21:03:24		8.0	
	WS-CA1	Wird ausgeführt	6 %	1082 MB	10.05:50:52		8.0	
	WS-CA1-neu	Aus					9.0	
	WS-CL6	Wird ausgeführt	0 %	1124 MB	9.06:18:33		9.0	
	WS-CL8	Wird ausgeführt	0 %	1302 MB	10.06:26:28		9.0	
	WS-DC2	Wird ausgeführt	2 %	4638 MB	9.03:26:48		9.0	
	WS-DPM	Wird ausgeführt	0 %	4096 MB	4.05:19:31		9.0	
	WS-FS2	Wird ausgeführt	0 %	1358 MB	2.05:17:11		9.0	
	WS-MON	Wird ausgeführt	8 %	3586 MB	4.05:53:24		8.0	
	WS-MX2	Wird ausgeführt	9 %	16384 MB	4.05:26:58		9.0	
	WS-PFS1b	Wird ausgeführt	0 %	5120 MB	26.20:42:53		8.0	
	WS-RDS2	Wird ausgeführt	0 %	3410 MB	10.05:36:10		8.0	
	WS-Steuer-alt	Aus					8.0	~
	WS-WAC	Wird ausgeführt	0 %	1922 MR	10.05/09/31		9.0	-
	Prüfpunkte							
	WS-CA1							
	Erstellt:	28	.11.2020 09:46:14	ł		Gruppiert: Nein		
	Konfigurat	tionsversion: 9.0)					
	Generatio	n: 2						
	Anmerkun	i g: Ke	ine					
	Zusammanfassura Atheiteenei	icher Netzwerk	Replikation					
	Zusammeniassung Aibeitssper	GINGI INGLZWEIK	riopiirtation					

WS-HV2: Ein virtueller Computer ausgewählt.

Jetzt passe ich noch einige Eigenschaften an und integriere die eben kopierte VHDX:





Nach dem Anpassen der Startreihenfolge kann es losgehen. Aber das System startet nicht:



Hyper-V-Manager				-		\times
Datei Aktion Ansicht	?					
🗢 🄿 🖄 🖬 🚺						
Hyper-V-Manager WS-HV1	Virtuelle Computer		🕎 "WS-CA1-neu" auf "WS-HV2" - Verbindung mit virtuellen Computern — 🗌	×		
WS-HV2	Name	Phase	Datei Aktion Medien Zwischenablage Ansicht ?		atio	^
	WS-ACAD WS-CA1 WS-CA1-neu WS-CL6 WS-CL8 WS-D2 WS-DPM WS-MX2 WS-MX2 WS-PFS1b WS-RDS2	Wrd ausgefür Aus Wrd ausgefür Wrd ausgefür Wrd ausgefür Wrd ausgefür Wrd ausgefür Wrd ausgefür Wrd ausgefür Wrd ausgefür Wrd ausgefür	Der virtuelle Computer "WS-CA1-neu" ist ausgeschaltet.			
	WS-Steuer-ait	Aus Wird ausgefült	Status von "WS-CA1-neu" zu ändern			~
	Prüfpunkte		Der Status von "WS-CA1-neu" zu andern.			\odot
	WS-CA1-neu Erstellt: Konfigur Generat Anmerka Zusammenfassung Arbetssp	ationsversion: ion: ung: veicher Netzwerk	Verden. Der Vorgang kann nicht ausgeführt werden, während das Objekt verwendet wird. Schließen Status: Aus 🔇 Fehler beim Starten			

Ich hatte versehentlich die alte VHDX mit dem Windows Server 2016 zugewiesen. Aber die wird ja vom alten Server verwendet. Also passe ich den Pfad an:

Hyper-V-Manager					
Datei Aktion Ansicht ?		Einstellungen für "WS-CA1-neu" auf "WS	-HV2"		×
🗢 🔿 🙍 📰 🛛 🖬		WS-CA1-neu \checkmark	3 ♦ ♦		
WS-HV2	Virtuelle Computer Name Ph WS-ACAD WW WS-ACAD WW WS-CA1 WW WS-CA1 WW WS-CA1 WW WS-CA2 WW WS-CA2 WW WS-CA2 WW WS-CA2 WW WS-SC2	★ Hardware Firmware Yor Postplatte* starten Sicherheit 2040 MB Image: Postplatte* startwert 2040 MB Image: Postplatte* startwert 2040 MB Image: Postplatte Postplatte Postplatte Postplatte Postplatte Image: Postplatte <t< th=""><th>Festplate Festplate Festplate Sie können auswählen, wie die virbuelle Festp werden soll. Ist auf dem Datenträger ein Beit Computer nach dem Ändern der Zuordnung n werden. Ontroller: SCSI-Controller Meden Ene virbuele Festplatte kann durch Bearbe Konverber, erweitert, zusammegneführt, werden. Geben Sie den vollständigen Pfad W:Hyper-VWS-CA1(Virbuel Hard Dia Physiche Festplatte: W:Hyper-VWS-CA1(Virbuel Hard Dia Physiche Festplatte: V:Hyper-VWS-CA1(Virbuel Hard Dia Physiche Festplatte: Sie sich, dass der Datenträger of physicher Festplatten die Daten Computers. Klicken Sie zum Entfernen der virbuelen Festp</th><th>Aatte dem virtuellen Computer zugeordnet riebssystem installiert, kann der virtuelle söglicherweise nicht mehr gestartet Speicherort: (wird verwendet) iten der zugehörigen Datei komprimiert, erneut verbunden oder verkleinert der Datei an. siyHDD0.vhdx en Überprüfen Durchsuchen siyHDD0.vhdx en Überprüfen Durchsuchen siyHDD0.vhdx en Überprüfen Durchsuchen siyHDD0.vhdx en Überprüfen Durchsuchen Entfernen</th><th></th></t<>	Festplate Festplate Festplate Sie können auswählen, wie die virbuelle Festp werden soll. Ist auf dem Datenträger ein Beit Computer nach dem Ändern der Zuordnung n werden. Ontroller: SCSI-Controller Meden Ene virbuele Festplatte kann durch Bearbe Konverber, erweitert, zusammegneführt, werden. Geben Sie den vollständigen Pfad W:Hyper-VWS-CA1(Virbuel Hard Dia Physiche Festplatte: W:Hyper-VWS-CA1(Virbuel Hard Dia Physiche Festplatte: V:Hyper-VWS-CA1(Virbuel Hard Dia Physiche Festplatte: Sie sich, dass der Datenträger of physicher Festplatten die Daten Computers. Klicken Sie zum Entfernen der virbuelen Festp	Aatte dem virtuellen Computer zugeordnet riebssystem installiert, kann der virtuelle söglicherweise nicht mehr gestartet Speicherort: (wird verwendet) iten der zugehörigen Datei komprimiert, erneut verbunden oder verkleinert der Datei an. siyHDD0.vhdx en Überprüfen Durchsuchen siyHDD0.vhdx en Überprüfen Durchsuchen siyHDD0.vhdx en Überprüfen Durchsuchen siyHDD0.vhdx en Überprüfen Durchsuchen Entfernen	
			OK	Abbrechen Anwenden	_

Jetzt startet das System. Weiter geht es im Out-Of-Box-Experience-Mode:

Hallo		
Lassen Sie uns zunächst einige grundlegende Dir	ige klären.	
Was ist Ihr Heimatland/Ihre Heimatregion?		
Deutschland	~	
Was ist Ihre bevorzugte App-Sprache?		
Deutsch (Deutschland)	~	
Welches Tastaturlayout möchten Sie verwender	?	
Deutsch	~	

Den neuen Server klemme ich fix ins Client-VLAN:

Hindware hinzufügen Firmware Von Datei fasten Schenheit Schenheit Schenheit ZoHein Start' staktiviert Arbeitsgeicher ZoHein Start' staktiviert Arbeitsgeicher ZoHein Markenheit El Prozessor	Wetzwerkarte Konfiguieren Sie die Netzwerkarte, oder entfernen Sie sie. Virbueler Skutch: LAN-110_DMZ VI-N1D VLAN-1D Virbueler LANs aktivieren Mithlife der VLAN-1D wird das virbuele LAN angegeben, das von diesem virbuelen
A Whole Processorem Soci-Controler Soci-Controler H= SetUsate Hotov.hdx Wereverklante LAM-110,0HZ Verwaltung Name Wo-C41 reu Metgradosalenste Ale Denste verfußate Produktion Specificent für die Smart Paging-D Verbige-VPVS-C41 Societerent für die Smart Paging-D Verbigs-VPVS-C41 Societerstehen Specificent für die Smart Paging-D Verbigs-VPVS-C41 Societerstehen Verbigs-VPVS-C41 Societerstehen Verbigs-VPVS-C41 Societerstehen Societerstehen Verbigs-VPVS-C41 Societerstehene Verbigs-VPVS-C41 Societerstehene Verbigs-VPVS-C41 Societerstehene Verbigs-VPVS-C41 Societerstehene Verbigs-VPVS-C41 Societerstehene Verbigs-VPVS-C41 Societerstehene Verbigs-VPVS-VPVS-VPVS-VPVS-VPVS-VPVS-VPVS-VPV	Computer für die gesamte Netzwerkkante verwerkaate sondoreten verwerkaate
Autometische Stoppeldon Herunterfahren	entfernen. Entfernen

Hier kann er nach Updates im Internet suchen:





Danach wird der Neustart erforderlich:



Ich bin aber etwas irritiert: Das Betriebssystem hatte ich aus einer VHDX-Datei mit dem Patchlevel 2020-05 erzeugt. Hier müssten wesentlich mehr Updates installiert werden! Ich passe den Pfad der Windows Updates an. So kann der Standalone-Server mit meinem WSUS kommunizieren:



Store Suche	fad für den Microsoft Updatedienst iguriert Kommentar: Unterstützt auf: Mind Servi	angeben Vorherige Einstellung Nachste Einstellung estens Windows XP Professional Service Pack 1 oder Windows 2000 e Pack 3, Windows RT ausgenommen	Status Nicht konfigur Nicht konfigur Nicht konfigur Nicht konfigur Nicht konfigur Nicht konfigur	Kommentar Nein Nein Nein Nein Nein
Exchangade Desrmittungsoptimierung Verbinden Windows-farbystem Wind	iguriert Kommentar: Unterstützt auf: Mind Servi	estens Windows XP Professional Service Pack 1 oder Windows 2000 e Pack 3, Windows RT ausgenommen	Nicht konfigur Nicht konfigur Nicht konfigur Nicht konfigur Nicht konfigur	Nein Nein Nein Nein
Verbinden Antora () Antora	Unterstützt auf: Mind Servi	estens Windows XP Professional Service Pack 1 oder Windows 2000 e Pack 3, Windows RT ausgenommen	Nicht konfigur Nicht konfigur Nicht konfigur	Nein Nein
Windows-Anandéoptionen Windows-Fabrysten Windows-Fabrysten Windows-Fabrysten Windows-Fabrysten Windows-Fabrysten Windows-Fabrysten Windows-Reinderen Windows-Rein	Unterstützt auf: Mind Servio	estens Windows XP Professional Service Pack 1 oder Windows 2000 e Pack 3, Windows RT ausgenommen	Nicht konfigur	Nein
Mindows-Fehrberichtestattung Windows-Keineder Windows-Reineter Windows-Reineter Windows-Reineterewaltung (Win Windows-Stencherewaltung (Win Windows-Stencherewaltung (Win Windows-Stencherekattung Windows-Zuverlässigkeistanalyse	Servi	e Pack 3, Windows RT ausgenommen		Nein
Windows-Mobilitätscenter Windows-Remoteshell Windows-Remoteshell Windows-Stenetex-waltung (Winc Windows-Stenetestsigkeitsanalyse			Vicht konfigur	Nein
windows-Remotesneii Windows-Remotesneii Windows-Remotesneii Windows-Zuverlässigkeitsanalyse Windows-Zuverlässigkeitsanalyse		Hilfe:	Nicht konfigur	Nein
> Mindows-Sicherheit Windows-Zuverlässigkeitsanalyse diesen http://ws-cm	tedienst zum Ermitteln von Undates		Nicht konfigur	Nein Nein
	ws.its:8530	Gibt einen Intranetserver an, der als Host für Updates von Microsoft Update fungiert. Mit diesem Updatedienst können Sie	Nicht konfigur	Nein
S Windows Defender Antivirus Windows Defender Exploit Guard Netzwe Aktuali Intranetserver	für die Statistik:	dann die Computer in Ihrem Netzwerk automatisch aktualisierer	Nicht konfigur	Nein
Windows Defender SmartScreen Mindows Helle for Buringer	.ws.its:8530	Mit dieser Einstellung können Sie einen Server im Netzwerk als Host für einen internen Updatedienst bestimmen. Der Client	Nicht konfigur Nicht konfigur	Nein Nein
Windows here for business Sie eine Host für Alternativen E	lownloadserver festlegen:	für automatische Updates durchsucht diesen Dienst nach Updates, die auf die Computer in Ihrem Netzwerk angewend	Nicht konfigur	Nein
Windows Installer Windows Media Digital Rights Man		Werden Konnen.	Nicht konfigur	Nein
Windows Media Player Update Windows Messenger Update Upda	://intranetUpd01) ne URL in den Metadaten	Wenn Sie diese Einstellung verwenden möchten, müssen Sie zwei Werte für Servernamen festlegen: den Server, auf dem der Client für automatische Lindster die Lindster srucht und von dem	^e Nicht konfigur Nicht konfigur	Nein Nein
Windows PowerShell werder herunterlag	len, wenn ein alternativer erver festgelegt ist	er sie herunterlädt, und den Server, auf den die aktualisierten Arbeitsstationen Statistiken hochladen. Sie können für beide	Nicht konfigur	Nein
C Alle Einstellungen	enenesigelegi bi	Werte den gleichen Server festlegen. Außerdem können Sie eine optionalen Servernamenswert angeben, um den Windows	n Nicht konfigur	Nein
i Benutzerkonfiguration zwei W Softwareeinstellungen festleg		Update-Agent so zu konfigurieren, dass er Updates von einem alternativen Downloadserver anstatt vom Updatedienst im	Nicht konfigur Nicht konfigur	Nein Nein
Windows-Einstellungen Client 1		Intranet herunterlädt.	v Nicht konfigur	Maria

Dann starte ich die Suche gegen meinen WSUS. Im Resmon sieht man, dass er mit dem WSUS kommuniziert:

Datei Aktion Medien A	Insicht	?				
⊨∣© ● ● Ⅱ ।►	1					
S Ressourcenmonitor					← Finstellungen	— П Х
Datei Überwachen ?						
Übersicht CPU Arbeitsspei	cher Da	tenträger Netzwer	k			
Prozesse mit Netzwerkaktivitä	it				ភ្លេ Startseite	windows Update
Prozess	PID	Senden (B/s)	Empfangen (B	i/s)	Einstellung suchen	*Einige Einstellungen werden von Ihrer Organisation verwaltet.
✓ svchost.exe (netsvcs -p)	1532	16.888	104.8	00		Konfigurierte Updaterichtlinien anzeigen
svchost.exe (utcsvc -p)	2464	87	1	47	Indate and Cickenbeit	
svchost.exe (NetworkService	1708	32		23	Opdate und sicherneit	Es wird nach Updates gesucht
Netzwerkaktivität			0 KB	it/s Netz	C Windows Update	
Gefiltert von "sychost eve (netsy	"(a- n)"					*Updates werden automatisch heruntergeladen, außer bei getakteten
Branner von svenostieze (netsve	.5 p/	A deserve		Condor	(M) Übermittlummentimiseum	Verbindungen (für die Gebühren anfallen können). In diesem Fall
sychost eve (petryst, p)	1532	Muresse		Senuer	브 Obermittlungsoptimierung	werden nur die Opdates automatisch neruntergeladen, die zur weiteren reihungslosen Ausführung von Windows erforderlich sind
sichoscere (nesses -p)	1552	113-011.113.113			Windows-Sicherheit	Sie werden zur Installation von Updates aufgefordert, nachdem sie heruntergeladen wurden.
					Problembehandlung	Nutzungszeit ändern
					Wiederherstellung	Updateverlauf anzeigen
TCP-Verbindungen		1			⊘ Aktivierung	Erweiterte Optionen
Übenvachungsports						
obernaenangoporto	_				11 Für Entwickler	
						Suchen Sie Infos zu den neuesten Updates?
						Weitere Informationen
						Verwandte Links

Aber auch hier gibt es keine Updates!



Datel Aktion Medien A	Ansient	4						
⊨∣@ ● ● ● Ⅱ ।►	1							
Nessourcenmonitor					←	Einstellungen	- 🗆 X	ŀ
Datei Überwachen ?								
Übersicht CPU Arbeitsspei	cher Da	tenträger Netzwei	k					
Prozesse mit Netzwerkaktivita	ät				ŵ	Startseite	windows Update	
Prozess	PID	Senden (B/s)	Empfangen (I	B/s)	Ei	nstellung suchen	*Einige Einstellungen werden von Ihrer Organisation verwaltet.	Γ
svchost.exe (netsvcs -p)	1532	1.261		341		, , , , , , , , , , , , , , , , , , ,	Konfigurierte Updaterichtlinien anzeigen	
svchost.exe (utcsvc -p)	2464	501	8	382				
SystemSettings.exe	5116	159	4	429	Upo	late und Sicherheit	Sie sind auf dem neuesten Stand	
Svchost.exe (NetworkService	1708	17		54			Latzta Übarprüfung: Hauta 10:13	
Netzwerkaktivität			0 KE	Bit/s Netz	C	Windows Update		
Gefiltert von "svchost.exe (netsv	cs -p)"			_			Nach Updates suchen	
Prozess	PID	Adresse		Sender	曲	Übermittlungsoptimierung		Γ
svchost.exe (netsvcs -p)	1532	52.250.46.236		1			Suchen Sie online nach Undates von Microsoft Undate	
						Windows-Sicherheit	Suchen Sie omme nach opdates von microsoft opdate.	
							*Updates werden automatisch heruntergeladen, außer bei getakteten	
					ß	Droblembebandlung	Verbindungen (für die Gebühren anfallen können). In diesem Fall	
					6	Problembenandlung	werden nur die Updates automatisch heruntergeladen, die zur	
					-		weiteren reibungslosen Ausführung von Windows erforderlich sind.	
					5	Wiederherstellung	Sie werden zur Installation von Updates aufgefordert, nachdem sie	
							heruntergeladen wurden.	
TCP-Verbindungen					\odot	Aktivierung		
							Nutzungszeit ändern	
Überwachungsports					11	Für Entwickler		
							Updateverlauf anzeigen	
							Erweiterte Optionen	

Dann schauen wir mal etwas genauer hin. Die Versionsnummer kann mit winver.exe ermittelt werden:

Info	×	
Windows Server [®] 20	019	
Microsoft Windows Server Version 1809 (Build <mark>17763.1217)</mark>		
© 2018 Microsoyt Corporation. All Recruit vorbenanten. Das Betriebssystem Windows Server 2019 Dataenter und Berutzeberfählte auf durch Marken- und andere rechts bestehende gewerbliche Schutz- und Liheberrechte in der Staaten und anderen Ländern geschützt.	I die zugehörige abhängige bzw. 1 Vereinigten	
Dieses Produkt ist unter den <u>Microsoft-Softwareizenzbedir</u> für: Windows-Benutzer	ngungen lizenziert	
	ОК	

Mit dieser Info suche ich im Netz nach dem Patch-Level. Es ist wie erwartet 2020-05:



Offensichtlich stimmt hier was nicht! Vielleicht fehlen Voraussetzungen für die aktuelleren Updates. Vielleicht ist der Cache auf dem Server beschädigt. Aber da habe ich bei einem neuen Server keine Lust. Ich installiere lieber neu, denn der neue Server soll ja auch einige Jahre problemfrei laufen!

Verlasst euch bitte nicht auf den Update-Dialog. Der kann trügerisch sein!

Aufbau der neuen VM (Neuinstallation)

WS IT-Solutions

Microsoft stellt in unregelmäßigen Abständen neue ISOs mit integrierten Updates bereit. Ich lade das aktuellste mit dem Patchlevel 2020-11 herunter und kopiere es auf meinen Hyper-V-Server:



Die defekte VHDX entferne ich:



Dann erstelle ich eine leere VHDX:







Mit dem ISO und der leeren Festplatte wird die Installation gestartet:

1



Nach dem Start des neuen Windows Servers suche ich nach Updates. Das sieht viel besser aus:





So macht nun auch eine Aktivierung Sinn:

🔁 Administrator: Windows Powe	rShell	_	×
t C:\> C:\>slmgr /ipk	1.74 1.10 AV		^
C:\>	Windows Script Host X Der Product Key installiert. OK		
Administrator: Windows Powe t C:\> C:\>slmgr /ipk	erShell		×
C:\>slmgr /ato C:\>	Windows Script Host X Windows/R), ServerDatacenter edition Das Produkt wurde erfolgreich aktiviert.		

Damit ist der neue Server vorbereitet.

CleanUp PKI

Weiter geht es mit dem Aufräumen in der alten CA. Die grafische Oberfläche bietet hier nur begrenzte Möglichkeiten. Und mit dem Befehl certutil.exe ist das Arbeiten auch nicht immer einfach. Daher hatte ich mir vor einigen Monaten einige PowerShell-Funktionen erstellt. Diese möchte ich heute verwenden:

WS IT-Solutions

🔠 Windows PowerShell ISE	_	×
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe		
Unbenannt1.ps1* ×		
1 ##### Scriptinfo ####################################		^
<pre>8 # functions 9 ⊞ function get-CACertificateList {} 161 162 ■ function get-CATemplateList {}</pre>		
183 184 m function remove-CACertificate {}		
223 224 🕢 function revoke-CACertificate {} 245		
246 🗉 function get-CATemplatesOnCA {}		
278 Function get-CACertificationAuthorityList {}		
298 ■ function get-CATemplatePermission {} 343		
344 break 345		

Aktuell sind 478 abgelaufene Zertifikate in der Datenbank der alten CA. Mit meinen PowerShell-Funktionen ist diese Ermittlung echt einfach:



Die Ausgabe kann auch in ein Gridview-Steuerelement umgelenkt werden. So kann ich also einfach und gezielt nach Zertifikaten suchen: WS IT-Solutions

WSHowTo – Migration einer Windows PKI (WS-CA1) 2020-11-28 Migration auf Windows Server 2019

🛃 Windows Powe	erShell ISE							_		×
Datei Bearbeiten	Ansicht Tools Debuggen Ad	d-Ons <u>H</u> ilfe								
1 🗀 🔒	8 G D X 9 P									
(Unbergrowt) and	Usbarrati v									
2 # 00	persient CA	thority	ist							
3										
4 # ab	ogelaufene Zertifikate	C1-1-		and the state						
6	get-CACertificateList	-State	expired M	turnAs GridView						
	get thether the test of		and the first							
6										~
-										
PS C:\>	🔛 CertificateList						— C) X]	
	Filter									
Count	1 шег							- 0		
Average :	🕂 Kriterien hinzufügen 🔻									
Sum :	Server	RequestID	RequesterName	CommonName	SubmittedWhen	NotBefore	NotAfter	Disposi ^		
Maximum :	WS-ITS-Zertifizierungsstelle-CA1	671	WS\stephan	Walther, Stephan	2019-11-05 09:17:00	2019-11-05 09:07:00	2020-11-04 09:07:00	20 Aı		
Property :	WS-ITS-Zertifizierungsstelle-CA1	672	WS\sysadm	Administrator	2019-11-05 13:49:00	2019-11-05 13:39:00	2020-11-04 13:39:00	20 Aı		
	WS-ITS-Zertifizierungsstelle-CA1	673	WS\Nicole	Widmann, Nicole	2019-11-09 16:15:00	2019-11-09 16:05:00	2020-11-08 16:05:00	20 Aı		
	WS-ITS-Zertifizierungsstelle-CA1	674	WS\Sandro	Widmann, Sandro	2019-11-11 16:50:00	2019-11-11 16:40:00	2020-11-10 16:40:00	20 Aı		
	WS-ITS-Zertifizierungsstelle-CA1	675	WS\stephan	Walther, Stephan	2019-11-14 15:39:00	2019-11-14 15:29:00	2020-11-13 15:29:00	20 Aı		
PS C:\>	WS-ITS-Zertifizierungsstelle-CA1	676	WS\Multimedia	Multimedia	2019-11-14 19:53:00	2019-11-14 19:43:00	2020-11-13 19:43:00	20 Aı		
	WS-ITS-Zertifizierungsstelle-CA1	677	WS\WS-CL4\$	WS-CL4	2019-11-14 20:25:00	2019-11-14 20:15:00	2020-11-13 20:15:00	20 Aı		
	WS-ITS-Zertifizierungsstelle-CA1	678	WS\WS-FS2\$	WS-FS2	2019-11-15 11:47:00	2019-11-15 11:37:00	2020-11-14 11:37:00	20 Ai		
	WS-ITS-Zertifizierungsstelle-CA1	679	WS\stephan-T1	Walther, Stephan - T1	2019-11-15 11:47:00	2019-11-15 11:37:00	2020-11-14 11:37:00	20 Aı		
	WS-ITS-Zertifizierungsstelle-CA1	680	WS\WS-FS1\$	WS-FS1	2019-11-15 15:49:00	2019-11-15 15:39:00	2020-11-14 15:39:00	20 Ai		
	WS-IIS-Zertifizierungsstelle-CA1	681	WS\stephan-11	Walther, Stephan - 11	2019-11-15 15:50:00	2019-11-15 15:40:00	2020-11-14 15:40:00	20 Al		
	WS-ITS-Zertifizierungsstelle-CA1	682	WS\stephan-11	Walther, Stephan - 11	2019-11-15 16:31:00	2019-11-15 16:21:00	2020-11-14 16:21:00	20 AL		
	WS-ITS-Zertifizierungsstelle-CAT	683	WS\WS-HV4\$	W5-HV4	2019-11-28 11:52:00	2019-11-28 11:42:00	2020-11-27 11:42:00	20 At ∨		
									1	
							OK	Abbrechen	1	
<										\rightarrow
					-		0 C-1-1 [
Skript/Auswahl wir	Skript/Auswahl wird ausgeführt. Drücken Sie "Strg+Unterbrechen", um den Vorgang zu beenden, und "", um den Debugger zu öffnen. In 28 Spalte 1 125%									

Meine Funktionen sind Pipeline-fähig. So kann ich mir das Ergebnis einer Suche nicht nur ansehen, sondern auch weiterverarbeiten. Hier suche und lösche ich abgelaufene Zertifikate in einer Zeile:

🔐 Windows PowerShell ISE	-	×
Datei Bgarbeiten Ansicht Iools Debuggen Add-Ons Hilfe		
Unbenannt1.ps1* Unbenannt2.ps1* X		0
1 # Übersicht CA 2 get-CACertificationAuthorityList 3 4 # abgelaufene Zertifikate		-
6 get-CACertificateList -State expired Measure-Object 7 get-CACertificateList -State expired -ReturnAs GridView 7 get-CACertificateList -State expired remove-CACertificate		2
PS C:\> get-CACertificateList -State expired -ReturnAs GridView		^
PS C:\> get-CACertificateList -State expired remove-CACertificate Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt. Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt. Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt. Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.		
Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt. Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt. Gelöschte Reihen: 1 Contitie: -deleterowe Refehl wurde erfolgreich zwegeführt		
Gelöschte Reihen: 1 Gelöschte Reihen: 1 Gelöschte Reihen: 1 Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.		
Geröschte Reihen: 1 Geröschte Reihen: 1 Geröschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.		
Gelöschte Reihen: 1 CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.		
Skript/Auswahl wird ausgeführt. Drücken Sie "Strg+Unterbrechen", um den Vorgang zu beenden, und "", um den Debugger zu öffnen.		125%

Dabei werden die Zertifikate nacheinander durch certutil-Aufrufe gelöscht. Das kann etwas dauern.

Weiter geht es mit ausstehenden Anfragen, die nie abgeschlossen wurden. Das sind nicht so viele:



8 9 10 11 12	8 9 # ausstehende Anforderungen 10 get-CACertificateList -State pending Measure-Object 11 get-CACertificateList -State pending -ReturnAs GridView 12 get-CACertificateList -State pending remove-CACertificate											
PS C:\	>	get-	CACertificateList -St	ate pen	ding Meas	ure-Object						
Count	. :	12	CertificateList								- 0	×
Sum	- : :		Filter									20
Maximu Minimu Proper	m : m :		🕂 Kriterien hinzufügen 👻									
Froper	cy.		Server	RequestID	RequesterName	CommonName	SubmittedWhen	NotBefore	NotAfter	Disposition	Template	Seri ^
			WS-ITS-Zertifizierungsstelle-CA1	616	WS\stephan-T1	Walther, Stephan - T1	2019-10-27 15:41:00	2019-10-27 15:31:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	618	WS\stephan-T1	Walther, Stephan - T1	2019-10-27 15:43:00	2019-10-27 15:33:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
PS C:\	>	get-	WS-ITS-Zertifizierungsstelle-CA1	659	WS\sysadm	Administrator	2019-10-31 09:13:00	2019-10-31 09:03:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
		-	WS-ITS-Zertifizierungsstelle-CA1	702	WS\stephan-T1	Walther, Stephan - T1	2020-01-01 13:29:00	2020-01-01 13:19:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	703	WS\stephan-T1	Walther, Stephan - T1	2020-01-01 13:31:00	2020-01-01 13:21:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	704	WS\stephan-T1	Walther, Stephan - T1	2020-01-01 13:32:00	2020-01-01 13:22:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	707	WS\stephan-T1	Walther, Stephan - T1	2020-01-01 14:06:00	2020-01-01 13:56:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	711	WS\stephan-T1	Walther, Stephan - T1	2020-01-01 16:42:00	2020-01-01 16:32:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	712	WS\stephan-T1	Walther, Stephan - T1	2020-01-02 15:42:00	2020-01-02 15:32:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	713	WS\stephan-T1	Walther, Stephan - T1	2020-01-02 15:42:00	2020-01-02 15:32:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			WS-ITS-Zertifizierungsstelle-CA1	738	WS\stephan-T1	Walther, Stephan - T1	2020-03-17 13:50:00	2020-03-17 13:40:00	2021-10-15 18:15:00	9 Ausstehend	WS-ITS-CodeSignatur-V2	LEEF
			<	700						· · · · ·		>
											OK AI	bbrechen

Aber auch diese benötige ich nicht länger:

8 9 # ausstehende Anforderungen
10 get-CACertificateList - State pending Measure-Object
11 get-CACertificateList -State pending -ReturnAs GridView
12 get-CACertificateList -State pending remove-CACertificate
PS C:\> get-CACertificateList -State pending remove-CACertificate
Geruttil: -deleterow-Refehl wurde erfolgreich ausgeführt.
Gelöschte Reihen: 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.
Geriusi'i - deleterne-Refehl wurde erfolgreich ausgeführt
Gelöschte Reiher. 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.
Geiloschte Reinen: 1 Cartilti: -delaternw-Refehl wurde erfolgreich ausgeführt
Gelöschte Reihen: 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.
Geloschte Reihen: 1 Cartitis, dalaternw-Refehl wurde erfolgreich ausgeführt
Gelöschte Reihen: 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.
Geloschte Reihen: 1 Cartitis, dalaternw-Refehl wurde erfolgreich ausgeführt
Gelöschte Reiher: 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.
Geriusi's -deleterne-Refehl wurde erfolgreich ausgeführt
Gelöschte Reiher. 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.

Es wird Zeit für einen Blick in die grafische Oberfläche. Hier stehen noch etliche fehlgeschlagenen Requests:

Seite 22 von 99



Aber auch diese kann ich mit der PowerShell-Funktion suchen und löschen:

<pre>19 # abgelehnte Anforderungen 20 get-CACertificateList -State denied Measure-Object 21 get-CACertificateList -State denied -ReturnAs GridView 22 get-CACertificateList -State denied remove-CACertificate 23</pre>
certuil: -deleterow-Befehl wurde erfolgreich ausgeführt.
Gelöschte Reihen: 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.
Gelöschte Reihen: 1
CertUtil: -deleterow-Betehl wurde erfolgreich ausgeführt.
Gertutil - delaterow-Refeel wurde erfolgreich ausgeführt
Gelächte Reihen 1
Certutil: -delterow-Befehl wurde erfolgreich ausgeführt.
Gelöschte Reihen: 1
CertUtil: -deleterow-Befehl wurde erfolgreich ausgeführt.
PS C:\Users\stephan-t1>

Anpassungen an der PKI

Weiter geht es mit Anpassungen an der PKI. Ab jetzt soll die alte CA keine Zertifikate mehr ausstellen. Damit beginnt also ein Wartungszeitfenster.

Ich entferne die auszustellenden Vorlagen. Die Vorlagen sind nur Verknüpfungen. Die Definitionen bleiben erhalten und ich kann die Vorlagen jederzeit wieder hinzufügen:



Wenn keine auszustellenden Vorlagen mehr vorhanden sind, dann werden neue Requests abgelehnt. So kann ich nun die Anpassungen eintragen. Ich beginne mit den Sperrlisten-Verteilungspunkten. Zukünftig sollen Sperrlisten nicht mehr über LDAP verteilt werden. Ich kann aber nicht einfach den Record löschen, denn hier hängt nicht nur die Veröffentlichung in den ausgestellten Zertifikaten dran, sondern auch die Veröffentlichung der Sperrlisten selber. In bisher ausgestellten Zertifikaten steht also drin, dass das vorliegende Zertifikat über eine Sperrliste aus dem Active Directory geprüft werden kann:

WS IT-Solutions



Wenn ich nun den LDAP-Record komplett entferne, dann wird dieser Eintrag in neuen Zertifikaten nicht mehr vorhanden sein. Gleichzeitig wird die CA aber auch keine aktuellen Sperrlisten im AD veröffentlichen und alte Zertifikate sind nicht mehr komplett verifizierbar! Das kann ich so also nicht gebrauchen. Daher entferne ich nur die Haken für die Integration in neue Zertifikate. Die Veröffentlichung der Sperrlisten im Hintergrund läuft einfach weiter:

PKI - [Konsolenstamm\Zertifizierungsstelle (V 	WS-CA1.ws.its)\WS-ITS-Zertifizieru	ngsstelle-CA1]
Image: Participation of the second secon	ter ?	Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? X
Konsolenstamm	Name	Speicherung Zertifikatverwaltungen Registrierungs-Agents
> Zertifikatvorlagen (WS-DC1.ws.its)	🧮 Gesperrte Zertifikate	Uberwachung Wiederherstellungs-Agents Sicherheit
✓ J Zertifizierungsstelle (W3-CA1.Ws.its) ✓ J WS-ITS-Zertifizierungsstelle-CA1	Ausgestellte Zertifikate	
🧮 Gesperrte Zertifikate	Ausstehende Anforderungen	Erweiterung <u>a</u> uswahlen:
Ausgestellte Zertifikate	Zertifikatvorlagen	
Fehlgeschlagene Anforderungen	_	Geben Sie Standorte an, von denen Benutzer eine Zertrikatssperfiste erhalten können.
🚆 Zertifikatvorlagen		Idap:///CN= <catruncatedname><crlnamesuffix>.CN=<servershortnar< td=""></servershortnar<></crlnamesuffix></catruncatedname>
> 👸 Unternehmens-PKI		http://crl.ws.its/crld/ <caname><crlnamesuffix><deltacrlallowed>.crl c:\admin>PKI\<caname><cbi_namesuffix><deltacbi_allowed>.crl</deltacbi_allowed></cbi_namesuffix></caname></deltacrlallowed></crlnamesuffix></caname>
> P Online-Responder:		
		< >>
		Hinzifügen Entfernen
		Spentisten an diesem Ort veröffentlichen
		In alle Speriisten einbeziehen. Legt fest, wo dies bei manueller
		Veröffentlichung im Active Directory veröffentlicht werden soll
		n Sperfisten einbeziehen. Wird z. Suche von Deltasperfisten verwendet
		In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen
		Del <u>t</u> asperrlisten an diesem Ort veröffentlichen
		In die IDP-Erweiterung ausgestellter CRLs einbeziehen
		OK Abbrohan Übernehmen Hiffe

Spätestens zum Ablauf des alten Zertifizierungsstellen-Zertifikates Ende 2021 sind alle alten Zertifikate abgelaufen und durch neue ersetzt. Dann kann ich den LDAP-Record gefahrlos entfernen.



Ich möchte auch keinen Download der Sperrliste über http ermöglichen. So bleibt später nur noch der neue Online Responder, mit dem ich eine Echtzeit-Sperrprüfung erzwingen kann:

🗢 🄿 📶 🗐 Q 🗟 🚺 🕨		Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? X						
🧮 Konsolenstamm	Name	Speicherung	Zertifikatverwaltungen	Registri	ierungs-Ag	ents		
 Zertifikatvorlagen (WS-DC1.ws.its) Zertifizierungsstelle (WS-CA1.ws.its) WS-ITS-Zertifizierungsstelle-CA1 Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen MUnternehmens-PKI Online-Responder: 	Name Gesperte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderung Zertifikatvorlagen	Operated ng Oberwachung Allgemein Ric Erweiterung ausw Spentisten-Vertei Geben Sie Standn erhalten könnet. Idap:///CN= <ca alle="" an="" c="" cdp-erweit="" ci.ws.ts="" deltaspentiste="" e="" gie="" idp-erw<="" in="" intio.="" spentisten="" th=""><th>Wiederherstellungs-Ag Miederherstellungs-Ag htlinienmodul Beendigung ählen: Uungspunkt orte an, von denen Benutzer ei TruncatedName><crlnamesuf crlname="" crlnamesvf.=""><crlnamesuffix><d [<="" abbrechen="" active="" an="" ausgestellten="" ausgestellter="" crls="" des="" diesem="" directory="" e="" einbeziehen.="" eir="" eiterung="" en="" erung="" fest,="" im="" inbeziehen.="" legt="" linz="" n="" ng="" ok="" ort="" suche="" th="" veröffent="" veröffentlichen="" veröffentlicher="" vor="" wird="" wo="" z.="" zertifik=""><th>ne Zertifikat ne Zertifikat iuffix>.CN=< ixx>CDetaC eltaCRLAllo uffügen n Deltaspen a Deltaspen tats einbezie hbeziehen</th><th>Sichert Erweiten tssperfiste ServerSho RLAIowed wed>.crl</th><th>vendet</th></d></crlnamesuffix></crlnamesuf></th></ca>	Wiederherstellungs-Ag Miederherstellungs-Ag htlinienmodul Beendigung ählen: Uungspunkt orte an, von denen Benutzer ei TruncatedName> <crlnamesuf crlname="" crlnamesvf.=""><crlnamesuffix><d [<="" abbrechen="" active="" an="" ausgestellten="" ausgestellter="" crls="" des="" diesem="" directory="" e="" einbeziehen.="" eir="" eiterung="" en="" erung="" fest,="" im="" inbeziehen.="" legt="" linz="" n="" ng="" ok="" ort="" suche="" th="" veröffent="" veröffentlichen="" veröffentlicher="" vor="" wird="" wo="" z.="" zertifik=""><th>ne Zertifikat ne Zertifikat iuffix>.CN=< ixx>CDetaC eltaCRLAllo uffügen n Deltaspen a Deltaspen tats einbezie hbeziehen</th><th>Sichert Erweiten tssperfiste ServerSho RLAIowed wed>.crl</th><th>vendet</th></d></crlnamesuffix></crlnamesuf>	ne Zertifikat ne Zertifikat iuffix>.CN=< ixx>CDetaC eltaCRLAllo uffügen n Deltaspen a Deltaspen tats einbezie hbeziehen	Sichert Erweiten tssperfiste ServerSho RLAIowed wed>.crl	vendet		

Auch in den Stelleninformationen muss ich aufräumen. Die Defaults enthalten einen File-Record. Den brauche ich nicht:

PKI - [Konsolenstamm\Zertifizierungsstelle (WS-CA1.ws.its)\WS-ITS-Zertifizierungsstelle-CA1]

🚟 Datei Aktion Ansicht Favoriten Fenster	?					
🔶 🧼 🖄 📰 📓 🍳 🕞 🛛 📷 🕨 🔳		Eigenschaften von	WS-ITS-Zertifi	izierungsstell	e-CA1	? ×
📔 Konsolenstamm 🛛 🛛 Na	me	Speicherung	Zertifikatver	waltungen	Registr	ierungs-Agents
> 🗷 Zertifikatvorlagen (WS-DC1.ws.its) 🔤	Gernerite Zertifikate	Überwachung	Wieder	herstellungs-A	gents	Sicherheit
🗸 🙀 Zertifizierungsstelle (WS-CA1.ws.its)	Ausgestellte Zertifikate	Allgemein Rid	chtlinienmodul	Beendigung	smodul	Erweiterungen
✓ J WS-ITS-Zertifizierungsstelle-CA1 Gesperrte Zertifikate	Ausstehende Anforderungen	Erweiterung <u>a</u> usw	ählen:			
📫 Ausgestellte Zertifikate	Fehlgeschlagene Anforderung	Zugriff auf Steller	ninformationen			\sim
 Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen Auternehmens-PKI Online-Responder: 	Zertifikatvorlagen	Geben Sie Stand Zertifizierungsstell C:\Windows\sys Idap:///CN=cA http://cServerDI file://cServerDI c	orte an, von den le erhalten könne tem 32'\CertSrv\C TruncatedName VSName>/CertEr SName>/CertEr	en Benutzer ei en. :: :: :: :: :: : : : : : :	n Zertifikat verDNSNa Public Key NSName> <u>VSName></u> ufügen ats einbezie Erweiterung	dieser me>_ <caname / Services,CN=S <caname><cer caName><cer > Entfemen hen gen einbeziehen</cer </cer </caname></caname
			OK Abt	brechen) <u>b</u> ernehmer	n Hilfe

Auch soll es keinen Hinweis in den Zertifikaten mehr geben, dass das Zertifizierungsstellen-Zertifikat im Active Directory gefunden werden kann. Das sind alles Grundvoraussetzungen für eine saubere Veröffentlichung von internen Zertifikaten ins Internet:



Also fliegt auch dieser Haken raus:

WS IT-Solutions

PKI - [Konsolenstamm\Zertifizierungsstelle (WS-CA1.ws.its)\WS-ITS-Zertifizierur	igsstelle-CA1]
Tension Ansicht Favoriten Fension (eter ?	Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? X
 Konsolenstamm Zertifikatvorlagen (WS-DC1.ws.its) Zertifizierungsstelle (WS-CA1.ws.its) WS-ITS-Zertifizierungsstelle-CA1 Gesperte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen MI Unternehmens-PKI Online-Responder: 	Name Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderung Zertifikatvorlagen	Speicherung Zertifikatverwaltungen Registrierungs-Agents Überwachung Wiederherstellungs-Agents Sicherheit Allgemein Richtlinienmodul Beendigungsmodul Erweiterungen Erweiterung guswählen: Zugriff auf Stelleninformationen ✓ Geben Sie Standorte an, von denen Benutzer ein Zertifikat dieser Zertifizierungsstelle erhalten können. C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<caname< td=""> \CaName Idap:///CN=<catrancatedname>/CertEnroll<serverdnsname>_<caname> \CaName \data \mathbf{Mame} \CertEnroll<serverdnsname>_<caname> \data \mathbf{Mame} \CertEnroll \ServerDNSName> \data \mathbf{Mame} \CertEnroll<<serverdnsname>_<caname> \CertEnroll \data \mathbf{Mame} \CertEnroll \ServerDNSName> \CertEnroll \data \mathbf{Mame} \CertEnroll \ServerDNSName> \CertEnroll \data \mathbf{Mame} \CertEnroll \ServerDNSName> \CertEnroll \mathbf{Mame} \data \mathbf{Mame} \mathbf{Linzufturgen} \mathbf{Enroll} \mathbf{Linzufturgen} \mathbf{Linzufturgen} \dott Li</caname></serverdnsname></caname></serverdnsname></caname></serverdnsname></catrancatedname></caname<></serverdnsname>

Diesen Default-Record benötige ich ebenfalls nicht:

🚰 PKI - [Konsolenstamm\Zertifizierungsstelle (WS-CA1.ws.its)\WS-ITS-Zertifizieru	ngsstelle-CA1]				
Datei Aktion Ansicht Favoriten Fension	ster ?	Eigenschaften von	WS-ITS-Zertifizierungsstell	e-CA1	?	×
 Konsolenstamm Zertifikatvorlagen (WS-DC1.ws.its) Zertifizierungsstelle (WS-CA1.ws.its) WS-ITS-Zertifizierungsstelle-CA1 Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen Muternehmens-PKI Online-Responder: 	Name Gesperrte Zertifikate Ausgestellte Zertifikate Fehlgeschlagene Anforderungen Zertifikatvorlagen	Speicherung Überwachung Allgemein Rich Erweiterung auswä Zugriff auf Stelleni Geben Sie Standor Zertfizierungsstelle Ctwindows/systel Idap:///CN= <cat http://<serverdn <</serverdn </cat 	Zertifikatverwaltungen Wiederherstellungs-Ar ntlinienmodul Beendigung ihlen: informationen te an, von denen Benutzer ei erhalten können. em32\CertSrv\CertEnroll\ <se runcatedName>.CN=AIA.CN SName>/CertEnroll\<serverd Hinz ung des ausgestellten Zertifika cate Status-Protokoll (OCSP)-</serverd </se 	Registr gents gsmodul in Zertifikat =Public Key DNSName>, ufügen ats einbezie Erweiterung	ierungs-Age Sicherh Erweiterun dieser Services,C_ _ <caname; _<caname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canname; _<canna< th=""><th>anne N=S ><ce ></ce </th></canna<></canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </canname; </caname; </caname; 	anne N=S > <ce ></ce
		C	OK Abbrechen (Demehmer	1 Hil	fe

Und dieser Default ist auf den FQDN der CA ausgelegt. Damit wird also immer der interne Name der CA in den Zertifikaten veröffentlicht:

Datei Aktion Ansicht ?	?							
Zertifikate - Lokaler Computer	Ausgestellt für		Ausgeste	ellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	St
Image: Constant Computer Image: Constant Constant Image: Constant <th>Ausgestellt für</th> <th>Zertifikat gemein Details zeigen: <ali><ali><ali><ali><ali><ali><ali><ali></ali></ali></ali></ali></ali></ali></ali></ali></th> <th>Ausgeste WS-ITS-2 Zertifizierungsp >> geninformatio Ilüsselverwen chtlinien ung des Antra elkennung rteilungspunkte elleninformatio netzastellerna s, CN=Services, (C ?objectClass=cc onszugriff e=Zertfizierungs me: WS-CA1.ws.its/ e-CA1(1).ort</th> <th>III von Zertifizierungsstelle-CA1 fad Wert Vorlage=WS-ITS-Computer Clentauthentifizierung (1.3 [1]Anwendungszertifikatrid e 15a 1f9bd72848c2fe0b6a5 Schlüssel-ID=b53b9af6ba [1]Sperristen-Verteilungspu [1]Stelleninformationszugrif DNS-Alame=WS-C1 1.ws.its DNS-Alame=WS-C1 1.ws.its DNS-DNS-DNS-DNS-DNS-DNS-DNS-DNS-DNS-DNS-</th> <th>Ablaufdatum 15.02.2021 × -V2 .6 rd4 .6 rft s-ITS- v en OK</th> <th>Beabsichtigte Zwec Clientauthentifizier</th> <th>Anzeigename <keine></keine></th> <th>St R</th>	Ausgestellt für	Zertifikat gemein Details zeigen: <ali><ali><ali><ali><ali><ali><ali><ali></ali></ali></ali></ali></ali></ali></ali></ali>	Ausgeste WS-ITS-2 Zertifizierungsp >> geninformatio Ilüsselverwen chtlinien ung des Antra elkennung rteilungspunkte elleninformatio netzastellerna s, CN=Services, (C ?objectClass=cc onszugriff e=Zertfizierungs me: WS-CA1.ws.its/ e-CA1(1).ort	III von Zertifizierungsstelle-CA1 fad Wert Vorlage=WS-ITS-Computer Clentauthentifizierung (1.3 [1]Anwendungszertifikatrid e 15a 1f9bd72848c2fe0b6a5 Schlüssel-ID=b53b9af6ba [1]Sperristen-Verteilungspu [1]Stelleninformationszugrif DNS-Alame=WS-C1 1.ws.its DNS-Alame=WS-C1 1.ws.its DNS-DNS-DNS-DNS-DNS-DNS-DNS-DNS-DNS-DNS-	Ablaufdatum 15.02.2021 × -V2 .6 rd4 .6 rft s-ITS- v en OK	Beabsichtigte Zwec Clientauthentifizier	Anzeigename <keine></keine>	St R

Also raus mit dem Record:

WS IT-Solutions



• 🔶 📶 🖾 🙆 🖾 👘 🕨		Eigenschaften vo	on WS-ITS-Zert	itizierungsstelle	e-CA1	7
Konsolenstamm	Name	Speicherung	Zertifikatv	erwaltungen	Registr	ierungs-Agents
Zertifikatvorlagen (WS-DC1.ws.its)	Gesperrte Zertifikate	Überwachung	g Wiede	erherstellungs-Ag	gents	Sicherheit
Zertifizierungsstelle (WS-CA1.ws.its) WS-ITS-Zertifizierungsstelle-CA1	Ausgestellte Zertifikate Ausstehende Anforderungen	Allgemein F	Richtlinienmodul swählen:	Beendigung	gsmodul	Erweiterunge
	📔 Fehlgeschlagene Anforderung	Zugriff auf Stel	leninformationen			~
		I I I I I I I I I I I I I I I I I I I				Construction Child
 Internehmens-PKI Online-Responder: 		Idap:///CN=<0 http:// <server< th=""><th>,A fruncated Nam DNSName>/Cert</th><th>ne>,CN=AIA,CN= tEnroll/<serverd< th=""><th>=Public Key)NSName></th><th>/ Services,CN= _<caname><c< th=""></c<></caname></th></serverd<></th></server<>	,A fruncated Nam DNSName>/Cert	ne>,CN=AIA,CN= tEnroll/ <serverd< th=""><th>=Public Key)NSName></th><th>/ Services,CN= _<caname><c< th=""></c<></caname></th></serverd<>	=Public Key)NSName>	/ Services,CN= _ <caname><c< th=""></c<></caname>
AU Unternehmens-PKI		Idap:///CN= <c http://<server< td=""><td>,A I runcated Nam DNSName>/Cert</td><td>ne>,CN=AIA,CN= tEnroll/<serverd< td=""><td>=Public Key)NSName></td><td>/ Services,CN= <<u>CaName><c< u=""></c<></u></td></serverd<></td></server<></c 	,A I runcated Nam DNSName>/Cert	ne>,CN=AIA,CN= tEnroll/ <serverd< td=""><td>=Public Key)NSName></td><td>/ Services,CN= <<u>CaName><c< u=""></c<></u></td></serverd<>	=Public Key)NSName>	/ Services,CN= < <u>CaName><c< u=""></c<></u>
Hunternehmens-PKI		Idap:///CN= <c http://cServer</c 	.A IruncatedNam DNSName>/Cert	tEnroll/ <serverd< td=""><td>=Public Key DNSName></td><td>/ Services,CN= <caname><c< td=""></c<></caname></td></serverd<>	=Public Key DNSName>	/ Services,CN= <caname><c< td=""></c<></caname>

Als Ersatz trage ich nun einen neuen http-Record ein. Hier verwende ich einen neuen CNAME, den ich später auch aus dem Internet heraus erreichbar machen kann:

PKI - [Konsolenstamm\Zertifizierungsstelle (W Datei Aktion Ansicht Favoriten Favoriten Fenster PKI - [Konsolenstamm\Zertifizierungsstelle (W Image: State of the s	S-CA1.ws.its)\WS-ITS-Zertifizierur er ?	ngsstelle-CA1] Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? X
 Konsolenstamm Zertifikatvorlagen (WS-DC1.ws.its) Zertifizierungsstelle (WS-CA1.ws.its) WS-ITS-Zertifizierungsstelle-CA1 Gesperte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen Muternehmens-PKI Mine-Responder: 	Name Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderung Zertifikatvorlagen	Speicherung Zertifikatverwaltungen Registrierungs-Agents Überwachung Wiederherstellungs-Agents Sicherheit Allgemein Richtlinienmodul Beendigungsmodul Erweiterungen Erweiterung auswählen:
		In AIA-Erweiterung des ausgestellten Zertfikats einbeziehen In Online Certificate Status-Protokoll (OCSP)-Erweiterungen einbeziehen OK Abbrechen Übernehmen Hilfe

Und ebenso registriere ich hier einen neuen Record für meinen noch nicht vorhandenen Online Responder:



		Eigenschaften von	WS-ITS-Zertifizierungsstell	le-CA1	?	×	
 Konsolenstamm Zertifikatvorlagen (WS-DC1.ws.its) Zertifizierungsstelle (WS-CA1.ws.its) Zertifizierungsstelle-CA1 Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen Junternehmens-PKI 	me Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderung Zertifikatvorlagen	Speicherung Zertifikatverwaltungen Registrierungs-Agent Überwachung Wiederherstellungs-Agents Sicherher Allgemein Richtlinienmodul Beendigungsmodul Erweiterung Im Erweiterung auswählen: Im Im Geben Sie Standorte an, von denen Benutzer ein Zertifikat dieser Zertifizierungsstelle erhalten können. Idap:///CN= <catruncatedname>,CN=AIA,CN=Public Key Services,CN Inttp://ca.ws-its.de/certs/<caname>,CertificateName>,ct</caname></catruncatedname>					
		< ☐ In AIA-Erweiter ☑ In Online Certif	Hinz ung des ausgestellten Zertifik icate Status-Protokoll (OCSP)-	zufügen ats einbezie Erweiterun,	Entfer ehen gen einbez	> iehen	

Nach den Anpassungen muss der CA-Service neugestartet werden:



Bevor ich hier was testen kann muss ich den neuen Namen ca.ws-its.de über DNS auflösbar gestalten. Da es aktuell noch keinen Grund für eine Veröffentlichung im Internet gibt, erstelle ich eine interne DNS-Zone mit dem Namen des CNAMEs:





In der neuen DNS-Zone erstelle ich nun einen Host-A-Record:





Wichtig ist, dass der neue Record keinen Namen hat. So lenke ich Clients auf die interne IPv4:

Ein Test von einem Client zeigt den Erfolg:

🔀 Windows PowerShell	-	\times
PS C:\> PS C:\> ping ca.ws-its.de		^
Ping wird ausgeführt für ca.ws-its.de [192.168.1 Antwort von 192.168.100.6: Bytes=32 Zeit≺1ms TTL Antwort von 192.168.100.6: Bytes=32 Zeit≺1ms TTL		
Ping-Statistik für 192.168.100.6: Pakete: Gesendet = 2, Empfangen = 2, Verlore (0% Verlust), Ca. Zeitangaben in Millisek.:		
Minimum = Oms, Maximum = Oms, Mittelwert = O STRG-C PS C:\> _		

Backup PKI

Die Migration des Services wird durch ein simples Backup & Restore erreicht. Also sichere ich jetzt auf dem alten Server alle Bestandteile. Die Konfiguration des Services liegt in der Registry. Diese exportiere ich in eine Datei:





Die eigentliche Datenbank und die Zertifikate kann ich mit certutil sichern:

WS IT-Solutions



Die lokal erstellten Sicherungsdateien kopiere ich auf mein AdminShare:

Schnellzugriff Kopieren Einfügen	Verschieben nach * X Löschen *	Neuer Ordner	Eigenschaften	Alles auswählen Nichts auswählen		An Schnell anheft	Izugriff Kopieren Einfügen	Verschieber	n nach • 🗙 Löschen •	Neuer Ordner	Eig
Zwischenablage	Organisieren	Neu	Öffnen	Auswählen			Zwischenablage		Organisieren	Neu	
• -> • 🛧 📙 > Netzwerk > ws-	ca1 > c\$ > Admin		v ق "Ad	min" durchsuchen	Q	$\leftarrow \rightarrow$	* 个 🦲 « Services > Ze	rtifikatstelle > N	figration → auf Windows Se	rver 2019 >	
A Schnellzugriff	Name		Änderungsdatum	Тур	Größe	>	RemoteAccess	^	Name		
Deeldern	📙 Backup		08.12.2020 08:13	Dateiordner			SCCM		Backup		
Desktop	- PKI		07.12.2020 16:28	Dateiordner		>	SCEP				
Walther, Stephan - 11	PSTranscript		10.11.2020 00:20	Dateiordner			Sharepoint		🌛 20201125-075735 ws-ca	1.ws.its.pfx	
Dieser PC	🛃 20201125-075735 ws-ca	a1.ws.its.pfx	25.11.2020 07:58	Privater Informati		>	SQL-Server		CheckCRL.cer		
🏪 System (C:)	🔐 backup.log		08.12.2020 03:16	LOG-Datei			Tasks				
🛖 Freigaben (M:)	CheckCRL.cer		29.11.2020 10:57	Sicherheitszertifikat			WAP				
🐂 Bibliotheken							wos				
💣 Netzwerk							WLAN				
ws-ca1							WEAR				
📮 cS							- WSUS				
Admin						×.	Zertifikatstelle				
Backup						>	CertReqTool				
PKI							Konfiguration				
DETransmint						~	Migration				
PS nanscript							> 🔄 auf Windows Server 20	16			
Benutzer							> 🔄 auf Windows Server 20	19			
inetpub							Zertifikate				
Logs						>	Sicherheit				

Jetzt kann die Migration starten.

Migration

Austausch des Servers

Eine Maintenance für den Service brauche ich nicht einrichten, denn automatische Zertifikatanforderungen werden alle 8 Stunden auf den Clients getriggert. Sollte mal ein Request nicht beantwortet werden, dann kommt der Client eben später wieder.

Weiter geht es also mit dem Abschalten der alten Windows Server 2016 Maschine:

• 🔿 🙍 📰 🚺							
Hyper-V-Manager	Virtuelle Computer						
WS-HV1.WS.ITS	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio.
WS-HV3.WS.ITS	WS-ACAD	Wird ausgeführt	0 %	2048 MB	3.01:00:45		8.0
	WS-CA1-alt	Aus					8.0
	WS-CA1-neu	Wird ausgeführt	0 %	1260 MB	10.02:17:42		9.0
	WS-CL6	Wird ausgeführt	0 %	1198 MB	19.09:23:06		9.0
	WS-CL8	Wird ausgeführt	0 %	1418 MB	20.09:31:01		9.0
	WS-DC2	Wird ausgeführt	2 %	4170 MB	19.06:31:20		9.0
	🗄 WS-DPM	Wird ausgeführt	2 %	4096 MB	14.08:24:04		9.0
	WS-FS2	Wird ausgeführt	0 %	1678 MB	12.08:21:44		9.0
	WS-MON	Wird ausgeführt	3 %	3362 MB	04:19:39		8.0
	WS-MX2	Wird ausgeführt	3 %	16384 MB	14.08:31:30		9.0
	WS-PFS1b	Wird ausgeführt	0 %	5120 MB	36.23:47:26		8.0
	WS-RDS2	Wird ausgeführt	0 %	3372 MB	20.08:40:43		8.0
	WS-Steuer-alt	Aus					8.0
	WS-WAC	Wird ausgeführt	0 %	1902 MB	20.08:14:03		9.0

Damit ich die Identität des Computerkontos übertragen kann, setze ich im Active Directory das Konto zurück:

WS IT-Solutions



Auf dem neuen Server ändere ich den Computernamen, ohne die Domain zu betreten:

Andern des Computernamens bzw. der Dom	näne X				
Sie können den Namen und die Mitgliedschaft de ändern. Änderungen wirken sich möglicherweise auf Netzwerkressourcen aus.	es Computers Com auf den Zugriff	nputers		AUFGAB	EN
	_		N-19Q2G6C5PPC	Zuletzt installierte Updates	2
Computername:	ode	er	RKGROUP	Windows Update	1
WS-CA1				Zuletzt auf Updates geprüft	2
Vollständiger Computername:					
WS-CAT			vat: Ein	Windows Defender Antivirus	
	Weitere	n	iviert	Feedback und Diagnose	
Mitglied von			aktiviert	Verstärkte Sicherheitskonfiguration für I	ΕI
O Domäne:			aktiviert	Zeitzone	
			4-Adresse wird über DHCP zugewiesen, IPv6-fähig	Produkt-ID	(
Arbeitsgruppe:					
WORKGROUP					
			rosoft Windows Server 2019 Datacenter	Prozessoren	
ОК	Abbrechen		rosoft Corporation Virtual Machine	Installierter Arbeitsspeicher (RAM)	
				Speicherplatz insgesamt:	1
OK	Abbasebee				
UK	Abbrechen	emenmen			_

Ebenso passe ich die Netzwerkkonfiguration an und trage die alte IPv4 ein. Der Server ist jetzt im Server-VLAN:

Einst	ellur Organisieren	hernet s.its icrosoft Hyper-V Netw	Eigenschaften von Ethernet Ketwerk	
🖨 St	atus		Vertexter von Internetprotokoll, Version 4 (TCP/IPv4)	
野 Et	hen		Allgemein Die IP-Einstellungen können automatisch zugewiesen werden, wenn das	
n Di	ΞÜ		Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.	
~~ V	PN		O IP-Adresse automatisch beziehen Solgende IP-Adresse verwenden:	den
🕀 Pr	оху		S IP-Adresse: 192.168.100.6 S Subnetzmaske: 255.255.255.0 Standardgateway: 192.168.100.252	
			DNS-Serveradresse automatisch beziehen	
			Bevorzugter DNS-Server: 192 . 168 . 100 . 2	
			Alternativer DNS-Server: 192 - 108 - 100 - 1	
	1 Element	1 Element ausgewählt	Erweitert	
			OK Abbrechen	

Nach einem Neustart nehme ich den Server in die Domain auf:

	EIGENSCHAFTEN				
🔛 Dashboard	Systemeigenschaften	×			AUFGABEN 🔻
Lokaler Sen	Ändern des Computernamens bzw. der Domäne	×		Zuletzt installierte Updates	28.11.2020 10:3
Alle Server	Sie können den Namen und die Mitgliedschaft des Compu ändern. Änderungen wirken sich möglicherweise auf den ä auf Netzwerkressourcen aus.	uters Zugriff		Windows Update Zuletzt auf Updates geprüft	Nur Updates m 28.11.2020 10:
	Computemame:	Windows-Sicherhe	it	×	Echtzeitschutz:
	Vollständiger Computername:	Ändern des	Computerr	namens bzw. der	ür IE Ein
	WS-CA1	Domäne			(UTC+01:00) Ar 00430-70395-3
	Weitere Mitglied von © Domäne:	Geben Sie Nam dieser Domäne	en und Kennwort beitreten dürfen.	eines Kontos ein, mit dem Sie	
	ws.its	ws\stephan-t3			AMD Ryzen 7 3 2 GB
	WORKGROUP	••••••	••••	୕	99,4 GB
	OK Abbrect	n			
	OK Abbrech	C	Ж	Abbrechen	AUFGABEN 🔻
			0		

Damit ist das Betriebssystem ausgetauscht.

Rolleninstallation

Jetzt installiere ich die erforderlichen Rollen und Features:

WS IT-Solutions

erverrollen au	swählen	ZIELSERVER WS-CA1.ws.its
Vorbereitung	Wählen Sie mindestens eine Rolle aus, die auf dem ausgewählte	en Server installiert werden soll.
Installationstyp	Rollen	Beschreibung
Serverauswahl Serverrollen Features AD-Zertifikatdienste Rollendienste Bestätigung Ergebnisse	Active Directory Lightweight Directory Services Active Directory-Domänendienste Active Directory-Rechteverwaltungsdienste Active Directory-Verbunddienste Active Directory-Zertifikatdienste Datei-/Speicherdienste (1 von 12 installiert) Device Health Attestation DHCP-Server Druck- und Dokumentdienste Faxserver Host Guardian-Dienst Hyper-V Netzwerkcontroller Netzwerkcichtlinien- und Zugriffsdienste Remotedesktopdienste Remotezugriff Volumenaktivierungsdienste Webserver (IIS)	Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) wird zum Erstellen von Zertifizierungsstellen und dazugehörigen Rollendiensten verwendet, die Ihnen das Ausstellen und Verwalten von Zertifikaten ermöglichen, die in einer Vielzahl von Anwendungen verwendet werden.
	< Zurück Weiter	r > Installieren Abbrechen
Assistent zum Hinzufügen eatures auswä	< Zurück Weiter	r > Installieren Abbrechen — ZIELSERVER WS-CA1.ws.its
Assistent zum Hinzufügen eatures auswä	< Zurück Weiter von Rollen und Features hlen Wählen Sie die auf dem ausgewählten Server zu installierenden	r > Installieren Abbrechen — — — — — — — — — — — — — — — — — — —
Assistent zum Hinzufügen eatures auswä Vorbereitung Installationstyp	< Zurück Weiter von Rollen und Features hlen Wählen Sie die auf dem ausgewählten Server zu installierenden Features	r > Installieren Abbrechen — — — — — — — — — — — — — — — — — — —

In den Details der Rolle "Active Directory Zertifikatdienste" wähle ich zusätzlich noch den Online Responder und CEP-CES aus. Der Zertifikatregistrierungsrichtlinien-Webdienst ist CEP, der Zertifikatregistrierungs-Webdienst ist CES:
🚘 Assistent zum Hinzufügen von	Rollen und Features	- 🗆 X
Assistent zum Hinzufügen von Rollendienste aus Vorbereitung Installationstyp Serverauswahl Serverrollen Features AD-Zertifikatdienste Rolle 'Webserver' (IIS) Rollendienste Bestätigung Ergebnisse	Rollen und Features SWÄhlen Wählen Sie die Rollendienste aus, die für "Active Directory Rollendienste Zertifizierungsstelle Conline-Responder Registrierungsrichtlinien-Webdienst Zertifikatregistrierungs-Webdienst Zertifizierungsstellen-Webregistrierung	ZIELSERVER WS-CA1.ws.its -Zertifikatdienste" installiert werden müssen. Beschreibung Mit dem Zertifikatregistrierungs- Webdienst können Benutzer und Computer sich für Zertifikate registrieren und Zertifikate verlängern, auch wenn der Computer kein Mitglied einer Domäne ist oder zwar einer Domäne angehört, sich aber vorübergehend nicht in der Sicherheitsbegrenzung des Firmennetzwerks befindet. Der Zertifikatregistrierungs-Webdienst arbeitet mit dem Zertifikatregistrierungsrichtlinien- Webdienst zusammen, um eine richtlinienbasierte automatische Zertifikatregistrierung für diese Benutzer und Computer bereitzustellen.
	< Zurück	Weiter > Installieren Abbrechen

Der Rest passt:

VS IT-Solutions

📥 Assistent zum Hinzufügen vor	Rollen und Features	– 🗆 X
Rollendienste au	swählen	ZIELSERVER WS-CA1.wz.its
Vorbereitung Installationstyp Serverauswahl	Rollendienste	Beschreibung Webserver bietet Unterstützung für HTML-Websites und optionale
Features AD-Zertifikatdienste Rollendienste Rolle 'Webserver' (IIS)		Unterstützung für ASP.NET, ASP und Webservererweiterungen. Sie können Webserver verwenden, um eine interne oder externe Website zu hosten oder eine Entwicklerumgebung zum Erstellen von webhasierten Anwendrungen
Rollendienste Bestätigung Ergebnisse	 Leistung Komprimierung statischer Inhalte Komprimieren dynamischer Inhalte Sicherheit Anforderungsfilterung Authentifizierung über Clientzertifikatzuorc 	bereitzustellen.
	Authentifizierung über IIS-Clientzertifikatzu Digestauthentifizierung IP- und Domäneneinschränkungen Standardauthentifizierung Unterstützung zentraler SSL-Zertifikate <	
	< Zurück Weiter	> Installieren Abbrechen

Problem mit 802.1x

Meine eigenen Migrationen führe ich in meiner Freizeit aus. Da kann es schon einmal vorkommen, dass ich nicht am Stück arbeiten kann, auch wenn es beim Lesen meiner WSHowTo`s vielleicht so scheinen mag. So ist es auch bei dieser Migration. Zwischen den bisherigen Arbeitsschritten und jetzt sind leider einige Tage vergangen. In dieser Zeit war die alte Windows CA nicht mehr erreichbar und der neue Server führt den Service noch nicht aus. Ich dachte mir, das wird schon kein Problem sein und im Vorfeld habe ich natürlich auch nach demnächst ablaufenden Zertifikaten Ausschau gehalten. Da gab es aber keine. Leider hatte ich aber eine andere Abhängigkeit vergessen: Meinen Netzwerkschutz mit 802.1x...

Mein WLAN-Segment für meine internen Clients ist mit einer zertifikatbasierten Authentifizierung konfiguriert. Ein Client, der sich am WLAN-Accesspoint anmelden möchte, muss also ein gültiges Clientzertifikat verwenden. Der Accesspoint leitet

diese Information weiter an meinen WS-NPS1 – das ist ein Radiusserver. Und dieser Server beweist seine Identität ebenfalls mit einem Serverzertifikat.

Der NPS (Network Policy Server) prüft die Identität des Clients anhand der Gültigkeit des Client-Zertifikates. Dabei verwendet er auch eine Sperrprüfung. Nur in meinem aktuellen Fall ist die Gültigkeit der auf dem NPS zwischengespeicherten Sperrliste abgelaufen, da die für die Erneuerung zuständige Zertifizierungsstelle offline ist. Daher verweigert der NPS alle Anfragen für eine WLAN-Anmeldung. Das wäre bei einer zügigen Bereitstellung der neuen CA nicht passiert.

Für meinen Fall ist es einfach: Ich ignoriere das WLAN-Problem, da es nur einen betroffenen Client gibt (mein Notebook ist meist verkabelt ans Netzwerk angeschlossen). In der realen Welt wäre jetzt eine Verlängerung der Sperrliste mit manueller Veröffentlichung sinnvoll.

Es geht also weiter mit dem Austausch.

Migration der ADCS

Nun starte ich das Post-Deployment der ADCS:

📥 Assistent zum Hinzufügen von	Rollen und Features	- (×
Installationsstatus	;	ZI WS-0	ELSERV CA1.ws.	ER its
	Installationsstatus anzeigen			
	Featureinstallation			
	•			
	Konfiguration erforderlich.Die Installation auf "WS-CA1.ws.its" war erfolgreich.			
	Active Directory-Zertifikatdienste			\wedge
AD-Zertifikatdienste	Es sind weitere Schritte zur Konfiguration der Active Directory-Zertifikatdienste au	f dem		
	Zielserver erforderlich.			
	Active Directory-Zertifikatolenste auf dem Zielserver konfigurieren			
	Zertifikatregistrierungsrichtlinien-Webdienst			
Restätigung	Zertifikatregistrierungs-Webdienst			
Eraobaisse	Online-Responder			
LIGEDHISSE	.NET Framework 4.7-Funktionen ASP.NET 4.7			~
	Sie können diesen Assistenten schließen, ohne die ausgeführten Aufgaben zu u Zeigen Sie den Aufgabenstatus an, oder öffnen Sie diese Seite erneut, indem S Befehlsleiste auf "Benachrichtigungen" klicken. Konfigurationseinstellungen exportieren	interbred ie auf de	chen. er	
	< Zurück Weiter > Schließer	Ab	brech	en

Wichtig ist hier, dass die AD-Integration nur von einem Enterprise-Administrator vorgenommen werden kann:





Mein Admin stephan-t1 ist aber nur Memberserver-Admin. Also bereite ich meine T3-Kennung vor:

Zeitraum: 1 Stunde Ziel-DC:	~					
a	✓ zu DC replizieren zu	u allen DC replizieren Die automatische AD-Replikation	n ist a	ktiv.		
Security-Tiers: Adr	lmins:	mögliche Gruppen:		aktive Mitgliedschaften:		
alle Tard - DomainAdministration Tard 1- ServerAdministration Tard 2- ClentAdministration Terd 3 - ServiceAdmin	phan-T3	Dominen-Admine GG-Admin-AD-GPO GG-Admin-AD-Join GG-Admin-ATA GG-Admin-Backup GG-Admin-DHCP GG-Admin-Thegaben GG-Admin-HyperV-Storage GG-Admin-HyperV-Storage GG-Admin-HyperV-Storage GG-Admin-HyperV-Storage GG-Admin-Phys-Storage GG-Admin-WACActini		Gittigkeit Gruppe 2020-12-11 20:27:00 GG-Admin-PKI 2020-12-11 20:27:00 GG-SEC-Server-Standard-Admins 2020-12-11 20:27:00 Organisations-Admins		
		IGG-SEC:Clerts-UB-Admins GG-SEC:Clerts-Standard-Admins GG-SEC:Clerts-Standard-Admins GG-SEC:Clerts-Standard-Admins GG-SEC:Clerts-WSITS-Admins GG-SEC:Clerts-WSITS-Admins GG-SEC:DomainC-Antrules-Admins GG-SEC:Serts-Bin-RDP GG-SEC:Serts-Bin-RDP GG-SEC:Serts-Bin-RDP GG-SEC:Serts-Bin-RDP GG-SEC:Serts-Whort-Minits GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-With-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Admins GG-SEC:Serts-Bin-Bin-Bin-Bin-Bin-Bin-Bin-Bin-Bin-Bin	~	entierren entierne alle		

Anschließend wechsle ich den Sicherheits-Kontext:





Ich installiere nur die Rolle ADCS:

🔁 Server-Manager				- 0	×
€∋- Se	AD CS-Konfiguration		- 0 X	ls Ansicht	Hilfe
Dashboard Lokaler Server Alle Server AD-Zertifikatdiens Datei-/Speicherdi IIS	Rollendienste Anmeldeinformationen Rollendienste Installationstyp ZS-Typ Privater Schlüssel Kryptografie ZS-Name Zertifikatanforderung Zertifikatdatenbank Bestätigung Status Ergebnisse	Wählen Sie die zu konfigurierenden Rollendienste aus. Zertifizierungsstellen Certifizierungsstellen-Webregistrierung Online-Responder Registrierungsdienst für Netzwerkgeräte Zertifikatregistrierungs-Webdienst Zertifikatregistrierungsrichtlinien-Webdienst	ZIELSERVER WS-CA1.ws.its	Ausblenden	
		Weitere Informationen zu AD CS-Serverrollen < Zurück	ren Abbrechen	1	~

Der neue Server soll eine Enterprise Root-CA werden – so wie vorher:





Aber anders als bei einer Neuinstallation muss ich hier die Zertifikate des alten Servers verwenden. Diese definieren die Identität:





Die Zertifikate wurden durch das Backup mit Certutil in PFX-Dateien exportiert. Ich muss aber nur noch das aktuell gültige auswählen und importieren:

🚡 Server-Manager			– 🗆 X
€⊙• Se	AD CS-Konfiguration		. 🗆 🗙 ^I s Ansicht Hilfe
Dashboard Lokaler Server Alle Server AD-Zertifikatdiens Datei-/Speicherdi IIS	Vorhandenes Zertifi Anmeldeinformationen Rollendienste Installationstyp ZS-Typ Privater Schlüssel Vorhandenes Zertifikat Zertifikatdatenbank Bestätigung Status Ergebnisse		ZIELSERVER WS-CA1.ws.its Ingsstelle len Sie dieses Zielcomputer diese Importieren Eigenschaften Ausblenden
		leitere Informationen zum vorhandenen Zertifikat < Zurück Weiter > Konfigurieren	1 Abbrechen





Die Pfade belasse ich im Default:

🔁 Server-Manager				- 0	×
€∋- Se	AD CS-Konfiguration		×	ls Ansicht	Hilfe
Dashboard	Zertifizierungsste	llendatenbank	ZIELSERVER WS-CA1.ws.its		^
Lokaler Server	Anmeldeinformationen Rollendienste	Geben Sie die Orte der Datenbank an.			
Datei-/Speicherdi	Installationstyp ZS-Typ	Ort der Zertifikatdatenbank: C:\Windows\system32\CertLog			
	Privater Schlüssel Vorhandenes Zertifikat Zertifikatdatenbank	Ort des Zertifikatdatenbankprotokolls: C:\Windows\system32\CertLog			
	Bestätigung Status				
				Ausblenden	
		Weitere Informationen zur Datenbank der Zertifizierungsstelle		1	
		< Zurück Weiter >	Konfigurieren Abbrechen		

Das sieht gut aus. Der alte Name der CA wurde über das alte Zertifikat gefunden:





Das hat funktioniert:

🚘 Server-Manager					- 0	×	
€∋- Se	AD CS-Konfiguration	-		×	ls Ansicht	Hilfe	
🔛 Dashboard	Ergebnisse		ZIELSERVE WS-CA1.ws.i	R ts			^
Lokaler Server Alle Server AD-Zertifikatdiens		Die folgenden Rollen, Rollendienste oder Features wurden konfiguriert:					
Datei-/Speicherdi	Installationstyp ZS-Typ Privater Schlüssel Vorhandenes Zertifikat Zertifikatdatenbank Bestätigung Status Ergebnisse	Zertifizierungsstelle Serfolgreiche Konfiguration Weitere Informationen zur Konfiguration der Zertifizierungsstelle			Ausblender	1	
		< Zurück Weiter > Schließen	Abbrecher	n	1		~

Bei Neuinstallationen werden ohne weitere Anpassungen die Standardvorlagen aktiviert. Da ich aber eine Migration ausführe und die Vorlagen vorab auf der alten Maschine entfernt hatte und die Identität wiederverwende, ist die Liste der auszustellenden Vorlagen leer. So werden dann keine Zertifikate versehentlich ausgestellt:



Die Datenbank der Windows CA wurde neu erstellt. Deshalb gibt es noch keine aktiven Zertifikate:



Nun deaktiviere ich den Service für die Wiederherstellung:

WS IT-Solutions



Die auf dem alten Server angepasste Konfiguration importiere ich nun auf dem neuen Server:





Die gesicherte Datenbank spiele ich mit certutil ein:

ightarrow 🔺 📥 > Die	:ser PC > Lokaler Datenträger (C:) > Admin >	> CA			5 √	"CA" durchsuchen	,	Q
Schnellzugriff	Name	Änderungsdatum	Тур	Größe				
🔜 Desktop 🛛 🖈	DataBase	11.12.2020 19:37	Dateiordner					
🕹 Downloads 🖈	B WS-ITS-Zertifizierungsstelle-CA1.p12	08.12.2020 08:15	Privater Informati	6 KB				
Dokumente 🖈	Administrator: Eingabeaufforderung						- 0	
📰 Bilder 🛛 🖈								
Desisters	C:\>certutil -† -restore C:\Ad	min\ca						
Desktop	Geben Sie das PFX-Kennwort ein							
🗶 Walther, Stephar	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate f	: für WS-CA1.ws.it	s\WS-ITS-Zertifi	zierungsstelle-	CA1 wurden von	c:\Admin\CA\WS-	ITS-Zert:	ifi
Walther, Stephan	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate f erungsstelle-CA1.p12 wiederherg Die Datenbank fün MS-CA1 we it	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zentifi	s\WS-ITS-Zertifi	zierungsstelle-	CA1 wurden von	c:\Admin\CA\WS-	ITS-Zert	ifi
 Desktop Walther, Stephar Dieser PC Lokaler Datenti 	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate erungsstelle-CA1.p12 wiederher Die Datenbank für WS-CA1.ws.it: Databankdateien werden wiederhe	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi ergestellt: 100%	s\WS-ITS-Zertifi zierungsstelle-C	zierungsstelle- CA1 wird wiederh	CA1 wurden von ergestellt.	c:\Admin\CA\WS-	ITS-Zert	ifi
Walther, Stephar Dieser PC Lokaler Datenti	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate erungsstelle-CA1.p12 wiederher Die Datenbank für WS-CA1.ws.its Databankdateien werden wiederhe Protokolldateien werden wiederhe	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi ergestellt: 100% hergestellt: 100 restellung für WS	s\WS-ITS-Zertifi zierungsstelle-C % -CA1 ws its\WS-T	Zierungsstelle- A1 wird wiederh	CA1 wurden von ergestellt.	c:\Admin\CA\WS-	ITS-Zert:	ifi
Walther, Stephar Dieser PC Lokaler Datenti Admin	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate erungsstelle-CA1.p12 wiederher Die Datenbank für WS-CA1.ws.its Databankdateien werden wiederhe Protokolldateien werden wiederhe Vollständige Datenbankwiederher Active Directory-Zertifikatdier	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi ergestellt: 100% hergestellt: 100 rstellung für WS nste anhalten un	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.WS.its\WS-I d neu starten, u	izierungsstelle- CA1 wird wiederh ITS-Zertifizieru um die Wiederher	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D	c:\Admin\CA\WS- atenbank von c:\/	ITS-Zert: Admin\CA	ifi fe
Walther, Stephar Dieser PC Lokaler Datenti Admin CA Benutzer	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate- erungsstelle-CAI.p12 wiederher Die Datenbank für WS-CAI.ws.it: Databankdateien werden wiederh Protokolldateien werden wiederh Vollständige Datenbankwiederher Active Directory-Zertifikatdier ig zu stellen. Cortiliti- crestore-Befehl wurd	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi ergestellt: 100% hergestellt: 100 rstellung für WS nste anhalten un e erfolgreich au	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.ws.its\WS-I d neu starten, u sgeführt	izierungsstelle- CA1 wird wiederh ITS-Zertifizieru um die Wiederher	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D	c:\Admin\CA\WS-: atenbank von c:\/	ITS-Zert: Admin\CA	ifi fe
Walther, Stephar Dieser PC Lokaler Datenti Admin CA Benutzer inetpub	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate- erungsstelle-CA1.p12 wiederher Die Datenbank für WS-CA1.ws.it: Databankdateien werden wiederhe Protokolldateien werden wiederhe Vollständige Datenbankwiederher Active Directory-Zertifikatdier ig zu stellen. CertUtil: -restore-Befehl wurde Der Dienst "CertSvc" muss neu f	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi ergestellt: 100% hergestellt: 100 rstellung für WS nste anhalten un e erfolgreich au gestartet werden	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.ws.its\WS-I d neu starten, u sgeführt. , damit die Ände	zierungsstelle- CA1 wird wiederh CTS-Zertifizieru um die Wiederher erungen wirksam	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D werden.	c:\Admin\CA\₩5-: atenbank von c:\∤	ITS-Zert: Admin\CA	ifi fe
Vesktop Walther, Stephar Dieser PC Lokaler Datenti Admin CA Benutzer intetpub PerfLogs	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate- erungsstelle-CA1.p12 wiederhen Die Datenbank für WS-CA1.ws.it: Databankdateien werden wiederhe Protokolldateien werden wiederhe Vollständige Datenbankwiederher Active Directory-Zertifikatdier ig zu stellen. CertUtil: -restore-Befehl wurde Der Dienst "CertSvc" muss neu g	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi ergestellt: 100% hergestellt: 100 rstellung für WS nste anhalten un e erfolgreich au gestartet werden	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.ws.its\WS-I d neu starten, u sgeführt. , damit die Ände	zierungsstelle- Al wird wiederh TS-Zertifizieru m die Wiederher erungen wirksam	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D werden.	c:\Admin\CA\WS-	ITS-Zert: Admin\CA	ifi fe
Vesktop Westop Westop Westop Dieser PC Lokaler Datenti Admin CA Benutzer inetpub PerfLogs Program Files	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate- erungsstelle-CA1.p12 wiederhen Die Datenbank für WS-CA1.ws.it/ Databankdateien werden wiederh Protokolldateien werden wiederh Vollständige Datenbankwiederhen Active Directory-Zertifikatdier ig zu stellen. CertUtil: -restore-Befehl wurd Der Dienst "CertSvc" muss neu g C:\>_	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi hergestellt: 100% hergestellt: 100% rstellung für WS nste anhalten un e erfolgreich au gestartet werden	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.ws.its\WS-I d neu starten, u sgeführt. , damit die Ände	zierungsstelle- CAI wird wiederh CTS-Zertifizieru um die Wiederher erungen wirksam	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D werden.	c:\Admin\CA\WS- atenbank von c:	ITS-Zert: Admin\CA	ifi fe
Veskop Wather, Stephar Dieser PC Lokaler Datenti Admin CA Benutzer inetpub PefLogs Program File: Programme	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate- erungsstelle-CA1.p12 wiederhen Die Datenbank für WS-CA1.ws.it Databankdateien werden wiederhe Protokolldateien werden wiederh Vollständige Datenbankwiederhen Active Directory-Zertifikatdier ig zu stellen. CertUtl1: -restore-Befehl wurd Der Dienst "CertSvc" muss neu g C:\>_	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi hergestellt: 100% hergestellt: 100 rstellung für WS nste anhalten un e erfolgreich au gestartet werden	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.ws.its\WS-I d neu starten, u sgeführt. , damit die Ände	zierungsstelle- CAI wird wiederh CTS-Zertifizieru um die Wiederher erungen wirksam	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D werden.	c:\Admin\CA\WS- atenbank von c:	ITS-Zert	ifi fe
Veskop Wather, Stephar Dieser PC Lokaler Datenti Admin CA Genutzer inetpub PefLogs Program Files Programme Windows	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate- erungsstelle-CAI.p12 wiederhen Die Datenbank für WS-CAI.ws.it. Databankdateien werden wiederhe Protokolldateien werden wiederh Vollständige Datenbankwiederhen Active Directory-Zertifikatdier ig zu stellen. CertUtil: -restore-Befehl wurd Der Dienst "CertSvc" muss neu g C:\>_	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi hergestellt: 100% hergestellt: 100 rstellung für WS nste anhalten un e erfolgreich au gestartet werden	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.ws.its\WS-I d neu starten, u sgeführt. , damit die Ände	zierungsstelle- CAI wird wiederh CTS-Zertifizieru um die Wiederher erungen wirksam	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D werden.	c:\Admin\CA\WS-	ITS-Zert∶ Admin\CA	ifi fe
Vesktop Wesktop Wesktop Dieser PC Lokaler Datenti Admin CA Benutzer inetpub PerfLogs Program Files Programme Windows DVD-Laufwerk	Geben Sie das PFX-Kennwort ein Die Schlüssel und Zertifikate- erungsstelle-CAI.p12 wiederhen Die Datenbank für WS-CAI.ws.it Databankdateien werden wiederh Protokolldateien werden wiederh Vollständige Datenbankwiederher Active Directory-Zertifikatdier ig zu stellen. CertUtil: -restore-Befehl wurd Der Dienst "CertSvc" muss neu g C:\>_	: für WS-CA1.ws.it gestellt. s\WS-ITS-Zertifi hergestellt: 100% hergestellt: 100 rstellung für WS nste anhalten un e erfolgreich au gestartet werden	s\WS-ITS-Zertifi zierungsstelle-C % -CA1.ws.its\WS-I d neu starten, u sgeführt. , damit die Ände	zierungsstelle- CAI wird wiederh CTS-Zertifizieru um die Wiederher erungen wirksam	CA1 wurden von ergestellt. ngsstelle-CA1. stellung der D werden.	c:\Admin\CA\WS-	ITS-Zert: Admin\CA	ifi fe

Jetzt kann der Services wieder starten:

VS IT-Solutions

certsrv - [Zertifizierungsstelle (Lokal)]				\times
Datei Aktion Ansicht ?				
♦ ♦ 8				
 Zertifizierungsstelle (Lokal) WS-ITS-Zertifizierungsstelle-CA1 Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderung Zertifikatvorlagen 	Name WS-ITS-Zertifizierungsstelle Die Active Directory-Zertifikatdiens	Beschreibung Zertifizierungsstelle		
< >>				

Durch die Wiederherstellung wurde die leere Datenbank durch die alte DB ausgetauscht. Somit sind auch wieder alle alten Zertifikate im Bestand enthalten:

🚋 certsrv - [Zertifizierungsstelle (Lokal)\\	WS-ITS-Zertifizierung	sstelle-CA1\Ausgestellt	e Zertifikate]	- 0	×				
Datei Aktion Ansicht ?									
🗢 🔿 🙍 🗟 🗟									
 ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	Anforderungs-ID 327 328 329 330 331 332 455 455 455 455	Antragstellername WS\WS-IPMS WS\WS-HV2S WS\WS-HV2S WS\WS-RDS1S WS\	Binäres ZertifikatBEGIN CERTIBEGIN CERTI	Zertifikatvorlage WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv WS-ITS-Webserv	Serienr ^ 160000 160000 160000 160000 160000 160000 160000 160000 160000 160000 160000 160000 160000 160000 160000				
	564	WS\WS-ATA\$	BEGIN CERTI	WS-ITS-Webserv	160000				
	572	WS\stephan-T1	BEGIN CERTI	WS-ITS-Webserv	160000				
	574	WS\stephan-T1	BEGIN CERTI	WS-ITS-Webserv	1b0000 ¥				
	•								

Die auszustellenden Vorlagen werden über ein Attribut im Active Directory zugewiesen. Die Wiederherstellung ist aber eine rein lokale Angelegenheit. Daher ist der Speicher der auszustellenden Vorlagen immer noch leer:

🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-Zertifizierungsstelle-CA1\Zertifikatvorlagen] —					
Datei Aktion Ansicht ?					
🗢 🔿 🙍 🙆 🔯					
🙀 Zertifizierungsstelle (Lokal)	Name	Beabsichtigter Zweck			
V J WS-ITS-Zertifizierungsstelle-CA1	In dieser Ansicht we	rden keine Elemente angezeigt			
Ausgestellte Zertifikate					
📔 Ausstehende Anforderungen					
📔 Fehlgeschlagene Anforderung					
🞽 Zertifikatvorlagen					
	<u> </u>				

Anpassung und Überarbeitung der Sperrlistenverteilung

VS IT-Solutions

Nun kommen wir zu den Nacharbeiten und dem Feintuning. Für die Sperrlistenveröffentlichung habe ich in der Konfiguration ein lokales Verzeichnis angegeben. Dieses muss ich noch erstellen:

	certsrv - [Zertifizierungsstell	Eigenschaften von WS-ITS-Zertifizierungsstelle-	-CA1 ? X
	Datei Aktion Ansicht ?	Überwachung Wiederherstellungs-Age	ents Sicherheit
	🗢 🔿 🙇 🖪 🛛	Speicherung Zertifikatverwaltungen	Registrierungs-Agents
		Allgemein Richtlinienmodul Beendigungs	amodul Erweiterungen
	✓	Erweiterung auswählen:	
	Gesperrte Zertifikate	Sperlisten-Verteilungspunkt	\sim
	📔 Ausgestellte Zertifikat	Geben Sie Standorte an, von denen Benutzer ein	e Zertifikatssperrliste
	Ausstehende Anforde	erhalten können.	
	Zertifikatvorlagen	Idap:///CN= <catruncatedname><crlnamesu< td=""><td>ffix>,CN=<servershortnar< td=""></servershortnar<></td></crlnamesu<></catruncatedname>	ffix>,CN= <servershortnar< td=""></servershortnar<>
		c:\admin\PKI\ <caname><crlnamesuffix><del< td=""><td>taCRLAllowed>.crl</td></del<></crlnamesuffix></caname>	taCRLAllowed>.crl
📕 📝 📑 = PKI	– 🗆 X	<	>
Datei Start Freigeben Ansicht	~ 😲	Hinzu	fügen Entfemen
$\leftarrow \rightarrow \checkmark \uparrow \Box C(Admin)PKI \checkmark $	"PKI" durchsuc P	Spentisten an diesem Ort veröffentlichen	
	× ,	In alle Sperilisten einbeziehen. Legt fest, wo di	ies bei manueller
A Schnellzugriff	Anderun	Veröffentlichung im Active Directory veröffentli	cht werden soll
Dieser Orde	ner ist leer.	In Sperfisten einbeziehen. Wird z. Suche von	Deltasperfisten verwendet
🖶 Downloads 🖈		In CDP-Erweiterung des ausgestellten Zertifika	its einbeziehen
🛱 Dokumente 🖈		Deltasperfisten an diesem Ort veröffentlichen	
🔚 Bilder 🖈		In die IDP-Erweiterung ausgestellter CRLs einb	beziehen
E. Desktop			
& Walther, Stephar		OK Abbrechen Ü	emehmen Hilfe
Dieser PC			
0 Elemente			
v ciemente			

Der Verteilungspunkt LDAP ist weiter mit dabei, denn die bisher ausgestellten Zertifikate haben einen Verweis auf das LDAP. Nur neue Zertifikate werden nicht mehr über LDAP verifizierbar sein: Die Option "In CDP-Erweiterung des ausgestellten Zertifikates Einbeziehen" ist nicht mehr aktiv.

Dennoch habe ich mit meinem 802.1x-Problem während der Downtime der CA festgestellt, dass ich auf eine Sperrlistenprüfung angewiesen bin. Bis hier wollte ich diese Funktion nur noch über OCSP bereitstellen. NPS wäre dazu auch in der Lage. Aber der OSCP-Server muss dafür immer online sein, denn der NPS wird die Antworten nicht cachen. In



meinem Fall ist der OCSP-Service aber nicht hochverfügbar. Ein Ausfall würde also WLAN-Anmeldungen verhindern. Ich möchte jetzt aber keinen zweiten Server aufbauen. Also werde ich einen Sperrlistenverteilungspunkt über http erstellen. Dort kann sich mein NPS-Server die Sperrliste herunterladen, zwischenspeichern und somit WLAN-Zugriffsanfragen auf bei ausgefallener CA validieren. Den Verteilungspunkt lenke ich auf einen "öffentlichen FQDN":

	الواديا وجهزا المتقارب					
	📮 certsrv - [Zertifizierungsstell	Eigenschaften von WS-ITS-Zertifiz	ierungsstelle-CA1	? ×	_	
	Datei Aktion Ansicht ?	Überwachung Wiederh	erstellungs-Agents	Sicherheit		
	🗢 🔿 🙍 🗟 👔	Speicherung Zertifikatverv	valtungen Regis	trierungs-Agents		
	Tartifizionungestelle (Lokal)	Allgemein Richtlinienmodul	Beendigungsmodul	Erweiterungen		
-	WS-ITS-Zertifizierungsste	Erweiterung auswählen:			¢	
	Gesperrte Zertifikate	Sperilisten-Verteilungspunkt		~	ingezeigt.	
	📔 Ausgestellte Zertifikat	Geben Sie Standorte an von dene	n Benutzer eine Zertifik	atssperdiste		
	Ausstehende Anforde	erhalten können.				
	Fehlgeschlagene Anfe	Idap:///CN= <catruncatedname></catruncatedname>	<crlnamesuffix>.CN</crlnamesuffix>	= <servershortnar< th=""><th></th><th></th></servershortnar<>		
	Zertifikatvorlagen	c:\admin\PKI\ <caname><crlna< th=""><th>meSuffix><deltacrla< th=""><th>lowed>.crl</th><th></th><th></th></deltacrla<></th></crlna<></caname>	meSuffix> <deltacrla< th=""><th>lowed>.crl</th><th></th><th></th></deltacrla<>	lowed>.crl		
				7		
			Hinzufügen	Entfernen		
		Sperfisten an diesem Ort veröffe	antlichen			
		In alle Speriisten einbeziehen. I	Ort hinzufügen			×
			Ein Ort kann jeder gü	iltige URL oder Pfad	sein. Geben Sie eine	n HTTP-, LDAP-,
		In Sperflisten einbeziehen. Wird	Dateiadress-, UNC- o Sie auf "Finfügen" u	oder lokalen Pfad ein meine Variable in d	ı. Wählen Sie eine Va en URI hzw. Pfad eir	ariable und klicken
		In CDP-Erweiterung des ausges	ole dar Einingen ,e			izurugen.
		Deltasperfisten an diesem Ort v	Ort:	14 0 N		
		In die IDP-Erweiterung ausgeste	http://cja.ws-its.de/c	cn/ <caname><crl< th=""><th>NameSuffix><deltacf< th=""><th>RLAllowed>.crl</th></deltacf<></th></crl<></caname>	NameSuffix> <deltacf< th=""><th>RLAllowed>.crl</th></deltacf<>	RLAllowed>.crl
			Variable:			
	<		<deltacrlallowed></deltacrlallowed>	•	~	Einfügen
		OK Abb	Beschreibung der au	sgewählten Variable	n:	
			Wird in URLs und P	faden verwendet.		
			Ersetzt die Dateinam Beispielofad: http://	ensuffix der Sperilist	e durch die der Delta	ispentiste, falls ∈ BLNameSuffix⊃
			beispicipiau. http://	Cell	Linos/ Containe/Ch	Lindine Junix /
			<			>
					014	
					OK	Abbrechen

Die Optionen verankern den Verteilungspunkt in den neu ausgestellten Zertifikaten:

	Speichening Zertifikatverwaltungen Registrienings-Agents
Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderung Echlosophaceae Anforderu	Uberwachung Wederherstellungs-Agents Sicherheit Allgemein Richtlinienmodul Beendigungsmodul Erweiterungen Erweiterung auswählen:
Zertifikatvorlagen	Sperifisten-Verteilungspunkt ✓ Geben Sie Standorte an, von denen Benutzer eine Zertifikatssperifiste erhalten körnen. Idap:///CN= <catuncatedname><crlnamesuffix>:CN= Idap:///CN=<catuncatedname><crlnamesuffix>:DeltaCRLAllowed>.ct (*\dimpicted avertises de/crl/<caname><crlnamesuffix>:DeltaCRLAllowed>.ct Inttp://ca.ws=ts.de/crl/<caname><crlnamesuffix>:DeltaCRLAllowed>.ct Inttp://ca.ws=ts.de/crl/<caname><crlnamesuffix>:DeltaCRLAllowed>.ct Interview > Interview > Interview > Interview > In alle Sperifisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung in Active Directory veröffentlicht werden soll In Sperifisten einbeziehen. Wird z. Suche von Deltasperifisten verwendet In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen Deltasperifisten an diesem Ott veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen OK Abbrechen</crlnamesuffix></caname></crlnamesuffix></caname></crlnamesuffix></caname></crlnamesuffix></catuncatedname></crlnamesuffix></catuncatedname>

Die neue URL ca.ws-its.de soll auf meiner Windows CA aufsetzen. Daher erstelle ich im IIS-Manager ein neues virtuelles Verzeichnis "certs" für die AIA-Stelleninformationen:



💐 Internetinformationsdienste (IIS)-Manager								- 🗆 X
← → ♥ WS-CA1 →									📴 🖂 🙆 🔹 -
Datei Ansicht ?									
Verbindungen		◎ WS-CA1 St	artsoito						Aktionen
Startseite Startseite Stortseite Anwendungspools Sites	Im Explorer Berechtigu	röffnen ngen bearbeiten	Start	Alle anzeigen C	Gruppieren nach: Bere	ich •	Anbieter	- ^ ^	Server verwalten Verwalten Verwalten Verwalten Beenden Anwendungspools anzeigen Sites anzeigen Neue Veuplattformkomponenten abrufen
	Virtuelles V Bindungen	erzeichnis hinzufügen bearbeiten	puterschlüssel	Seiten und Steuerelemente	Sitzungszustand	SMTP-E-Mail	Verbindungszeiche		Hiffe
×	Website ve Aktualisiere Entfernen	rwalten 🕨	Contraction of the second seco	(Reference to the second secon	Ausgabezwischen	Authentifizierung	Fehlerseiten	- ^	
	Umbenenn Zur Ansich	en t "Inhalt" wechseln	- Antworthea	HTTP-Umleitung	ISAPI- und CGI-Einschränkun	ISAPI-Filter	Komprimierung		
		MIME-Typ	Adule Module	Protokollierung	Serverzertifikate	Standarddokument	Verzeichnis durchsuchen		
		Verwaltung	Ansicht "Inhalt"	1					
Bereit									•=

Dieses lasse ich auf den lokalen Speicherpfad zeigen, in dem meine CA ihre Sperrlistendateien und die Zertifikate bei der Veröffentlichung ablegt:

Image: Section of the section of th	💐 Internetinformationsdienste (IIS)-Manager	– 🗆 X
Datei Ansicht ? Verbindungen	(← →) (%] + WS-CA1 +	🔯 🗵 🏠 🔞 🗸
Verbindungen WS-CA1 Startseite Startseite Startseite Startseite Startseite Anwendungspools Ster Ster Default Web Site NET-Autorisierun NET Anwendungspools Stename: Default Web Site Pfad: // Anwendungspools Stes anzeigen Stes anzeigen Stes anzeigen	Datei Ansicht ?	
Bereit durchsuchen	Verbindungen Verbinden als Einstellungen testen Verweitung V	Aktionen Server verwalten Neu staften Starten Beenden Anwendungspools anzeigen Sites anzeigen Webplatformkomponenten abrufen P Hiffe

Ein weiteres virtuelles Verzeichnis "crl" wird für die Sperrlistenveröffentlichung über <u>http://ca.ws-its.de/crl</u> benötigt:



💐 Internetinformationsdi	ienste (IIS)-Manager	r							– 🗆 X
← → 8 + WS-0	CA1 🕨 Sites 🕨 E	Default Web Site 🕨 cert	s)						😰 🖂 🙆 🛛 🕶
Datei Ansicht ?									
Verbindungen		Corts St	artsoito						Aktionen
Startseite WS-CA1 (WS\stephi WS\stephi Gites Gi	an-T1) iols Site Im Explorer öffner	Filter:	Start Start NET-Benutzer	Alle anzeigen G	iruppieren nach: Bere	ich • III	• .NET-Profil	• •	Im Explorer offnen Berechtigungen bearbeiten Grundeinstellungen Virtuelles Verzeichnis durchsuchen
> 🔬 cer 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Berechtigungen b Anwendung hinzu Virtuelles Verzeich Bindungen bearbe Website verwalten Aktualisieren Entfernen	earbeiten Jfügen nis hinzufügen eiten	.NET-Vertrauense SMTP-E-Mail	Anbieter Tebindungszeiche	Final Anwendungseinst	Computerschlüssel	Seiten und Steuerelemente		Atta (http:) durchsuchen Virtuelles Verzeichnis bearbreiten Erweitente Einstellungen Hilfe
R	Umbenennen Zur Ansicht "Inhal	t" wechseln Ablaufverfolgungs. für Anforderungsf HTTP-Antworthea SSL-Einstellungen	Anforderungsfilte	Ausgabezwischen Q Komprimierung Verzeichnis	Authentifizierung	Fehlerseiten	Handlerzuordnum	~	
Bereit		Ansicht "Features"	Ansicht "Inhalt"						€≣.:

Auch dieses Verzeichnis zeigt auf den lokalen Ordner c:\admin\pki:

📬 Internetinformationsdienste (IIS)-Manager	- 🗆 X
	😨 🛛 🟠 🔞 🕶
Datei Ansicht ?	
Verbindungen	Aktionen Im Explorer öffnen Berechtigungen bearbeiten Grundeinstellungen Virtuelles Verzeichnis durchauchen Virtuelles Verzeichnis bearbeiten Virtuelles Verzeichnis bearbeiten Enweiterte Einstellungen Iffe
Bereit	•

Ich aktiviere das Directory Browsing, damit ich den Inhalt des Verzeichnisses direkt im Browser ansehen kann:



💐 Internetinformationsdienste (IIS)-Manager		– 🗆 X
← → ₩S-CA1 → Sites → De	fault Web Site 🔸 crl 🔸	📴 🐼 🟠 🔞 🗸
Datei Ansicht ?		
Datei Ansicht ? Verlindungen 	rll Startseite Filter Start Alle anzeigen Gruppieren nach: Bereich Start Ablaufverfolgungs Anforderungsfilte Start Start Start HTTP-Antworthea HTTP-Umleitung Somprimierung MIME-Typ Module Protokollierung SSI-Einstellungen Standarddokument Verzeichnis durchsuchen Verzeichnis durchsuchen	Aktionen Im Explorer öffnen Berechtigungen bearbeiten Grundeinstellungen Virtuelles Verzeichnis durchsuchen Virtuelles Verzeichnis bearbeiten Virtuelles Verzeichnis bearbeiten Virtuelles Verzeichnis bearbeiten Erweiterte Einstellungen P Hilfe
Provide	🔝 Ansicht "Features" 🔐 Ansicht "Inhalt"	62.
Deleit		TL ::
Internetinformationsdienste (IIS)-Manager ← → ↓ WS-CA1 → Sites → De	fault Web Site → crl →	×
Date: Ansicht ?		41.1
Verbindungen •	Konfigurations-Editor Abschnitt: system.webServer/directoryBrowse • Von: Default Web Site/crl Web.config • V Unterste Pradebene: MACHINE/WEBROOT/APPHOST • • • enabled True • • showNilaps Date,Time,Size,Extension •	Aktionen Image: Construction of the second secon

Da der FQDN in meinem DNS-Server bereits erstellt wurde und auf die interne IPv4 meiner Windows CA zeigt, kann ich das Verzeichnis einfach im Browser aufrufen und testen:

ca.ws-its.d	de - /crl/	×	+	
← → C ⁱ	۵	0 🔏	ca.ws-its.de/crl/	⊘ ☆
O DuckDuckGo	🗀 ws.its 📋] Links 🗎 Ku	nden 📋 JB 🛅 Microsoft 🗎 wichtig	
ca.ws-i	ts.de -	/crl/		
Ca.WS-i	ts.de -	/crl/		
Ca.ws-i	ts.de -	/crl/	web.config	
Ca.ws-i [Zum überged 11.12.2020 11.12.2020	ts.de -	/crl/	web.config WS-TIS-Zertifizierungsstelle-CA1(1)+.crl	
Ca.ws-i [Zum überged 11.12.2020 11.12.2020 11.12.2020	ts.de -	/crl/	<pre>web.config WS-ITS-Zertifizierungsstelle-CA1(1)+.crl WS-ITS-Zertifizierungsstelle-CA1(1).crl</pre>	
Ca.WS-i [Zum übergeo 11.12.2020 11.12.2020 11.12.2020 11.12.2020	ts.de -	/crl/ rzeichnis] 168 533 517 531	web.config WS-ITS-Zertifizierungsstelle-CA1(1)+.crl WS-ITS-Zertifizierungsstelle-CA1(1).crl WS-TIS-Zertifizierungsstelle-CA1+.crl	

Grundkonfiguration und Ausstellung eines neuen Zertifizierungsstellen-Zertifikates

Es wird Zeit für ein neues Zertifizierungsstellen-Zertifikat, denn das bisherige läuft bald ab:

Datentyp:bool

🖺 Ansicht "Features" 🛅 Ansicht "Inhalt"

onfiguration: Default Web Site/crl Web.config

abled'-Attribute Attribut sper Hilfe

Abschnitt Abschnitt sperren ٢

(~)



🛱 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-Zertifizierung	ngsstelle-CA1] — 🗆	\times
Datei Aktion Ansicht ?		
← ⇒ 2 □ Q ⇒ 2 ▶ ■	Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? X	
 Zertifizierungsstelle (Lokal) WS-ITS-Zertifizierungsstelle-C Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderung Fehlgeschlagene Anforder Zertifikatvorlagen 	Speicherung Zertfikatverwaltungen Regis Zertfikat X Algemein Richtiniermodul Beendigungsmodul Algemein Detwachung Zertfikat X Zertfikat Name: WS-ITS-Zertfizierungsstelle Algemein Details Zertfikatsinformationen Zertfikat N. 0 (abgelaufen) Zertfikat ist für folgende Zwecke beabsichtigt: Alle ausgegebenen Richtlinien Zertfikat N. 0 (abgelaufen) Zertfikat ist für folgende Zwecke beabsichtigt: Zertfikat N. 0 (abgelaufen) Alle ausgespelbenen Richtlinien Alle ausgespelbenen Richtlinien Kryptografieeinstellungen Anbieter: Microsoft Software Key Storage F Ausgestellt für: WS-ITS-Zertfizierungsstelle-CA1 Hashalgorthmus: SHA256 SHA256 Ausstellererklärung OK Abbrechen Dbemehme CK	
•		

Der Vorgang kann einfach weil grafisch durchgeführt werden:

🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-Zertifi	izierungsstelle-CA1]	-	×
Datei Aktion Ansicht ?			
🗢 🔿 🖄 🗐 🕢 🕞 🖉 🕨 🔳			
Zertifizierungsstelle (Lokal) Name			
V 🛃 WS-ITS-Zer Alle Aufgaben >	Dienst starten		
Ausgest Ansicht >	Dienst anhalten		
Aussteh	Neue Anforderung einreichen		
Zertifika Liste exportieren	Zertifizierungsstelle sichern		
Eigenschaften	Zertifizierungsstelle wiederherstellen		
Hilfe	Zertifizierungsstellenzertifikat erneuern		
< >>			
Die Gültigkeitsdauer der Zertifizierungsstelle wird verläng	gert, indem ein neues Zertifikat angefordert wird.		

🙀 certsrv - [Zertifizierungsstelle (Lol	kal)\WS-ITS-Zertifizierung	sstelle-CA1]	_	×
Datei Aktion Ansicht ?				
🗢 🔿 🖄 🗐 🙆 🛃 🚺	•			
 Zertifizierungsstelle (Lokal) WS-ITS-Zertifizierungsstelle-C Gesperrte Zertifizier Ausgestellte Zertifiziate Ausgestellte Zertifiziate Ausstehende Anforderung Fehigeschlagene Anforder Zertifikatvorlagen 	Name Gesperrte Zertifikate Nusgestellte Zertifik Nusstehende Anforc Fehlgeschlagene An Zertifikatvorlagen	ate lerungen forderungen		
		Zertifizierungsstellenzertifikat installieren X Die Active Directory-Zertifikatdienste können während des Vorgangs nicht ausgeführt werden. Möchten Sie die Active Directory-Zertifikatdienste jetzt beenden?		
		Ja Nein		
< >				

Ich erstelle dabei gleich ein neues Schlüsselpaar:

WS IT-Solutions

certsrv - [Zertifizierungsstelle (Loka)\WS-ITS-Zertifizierungsstelle-CA1]	- L X							
Datei Aktion Ansicht ?									
 Zertifizierungsstelle (Lokal) WS-ITS-Zertifizierungsstelle-C Gesperte Zertifikate Ausgetellte Zertifikate Ausgetellte Zertifikate Ausstehende Anforderung Fehlgeschlagene Anforder Zertifikatvorlagen 	Name Gesperte Zertif Ausgestellte Ze Ausgestellte Ze Ausstehende A Stattehende A Zertifikat vorlag Ein neues Zertifikat zu erhalten, haben Option einen neuen Signaturschlüssel zu erstellen. Ein neues Zertifikat für die Zertifikaterungsstelle ist efforderlich, wen: Image: Signaturschlüssel ist efforderlich, wenn: Image: Signaturschlüssel gefährdet ist. Sie ein Programm haben, dass einen neuen Signaturschlüssel gefährdet ist. Gie Gütigkeitasperistie zu groß ist und Sie best Informationen in eine neue Zertifikatsperistie zu groß ist und Sie best Informationen in eine neue Zertifikatsperiste verschie Wichtgrografiedentanbieter und Haasdagothmus bleiben enhalten. vorhandene Schlüssellänge kleiner als 1024 Bt ist, wird sie verlänger Image: Ima	Sie auch die nn: Igert wurde. chlüssel für das timmte eben möchten. be Enstellungen Fals die nt. Abbrechen							

Nach Abschluss ist das neue Zertifikat im Speicher sichtbar. 2025 ist für eine interne Windows CA nicht viel, aber ich bin damit zufrieden.



2 '	igenscharten von v	73-113-Zerunzie	erungsstelle-CAT		📰 Zertifikat		×	
zie	Speicherung	Zertifikatverwa	altungen Regi	strierungs	Details a use			
S-1	Überwachung	Wiederher	rstellungs-Agents	Sic	Allgemein Details Zertifizierungsp	otad		
G	Allgemein Richt	linienmodul	Beendigungsmodul	Erwei	Anzeigen: <alle></alle>	~		
4	Zertifizierungsstelle	e			CAIC2	-		
2	Name:	WS-ITS-Ze	rtifizien ingsstelle-CA1		Feld	Wert		
7	Nume.	11511520	ranzierangsstelle er ti		Version	V3		
4	Zertifizierungsstelle	anzertifikate:			Seriennummer	5a91b154687d54b945f913d2		
	Zertifikat Nr.0 (ab	gelaufen)			Signaturalgorithmus	sha256RSA		
	Zertifikat Nr. 1 Zertifikat Nr. 2				📴 Signaturhashalgorithmus	sha256		
					Aussteller	WS-ITS-Zertifizierungsstelle-C		
					Gültig ab	Samstag, 12. Dezember 2020		
					Gultg bis	Freitag, 12. Dezember 2025 1		
					TEL ANT ANSTELET	WK-TK-Zermizieri Innostelle-1		
					Freitag, 12. Dezember 2025 15:3	7:27		
			Zer	tifikat anz				
				_				
	Kryptografieeinstel	lungen						
	Anbieter:	Microsoft So	oftware Key Storage	Provider				
	Hashaloorithmus	SH4256						
	ridandigona inda.	511/250						
					Eigenschaften bearbeit	In Datei kopieren		
							_	
						OK		
	O	K Abbre	chen Übernehm	en		OK		

Das Zertifikat hat einen neuen öffentlichen Schlüssel. Diesen exportiere ich in eine Datei:

🙀 certsrv - [Ze	ertifizierungsstelle (Lokal)\WS-ITS-Zertifizierungsstel	le-CA1]	- 🗆 ×
Datei Akțion	Ansicht ?		
🗢 🔿 🛿 Eig	genschaften von WS-ITS-Zertifizierungsstelle-C/ 1	з.	×
Zertifizie V J WS-I G	Speicherung Zertifikatverwaltungen Überwachung Wiederherstellungs-Agent: Allgemein Richtlinienmodul	F Zertifikatexport-Assistent	
A A F 7	Zertifizierungsstelle Name: WS-ITS-Zertifizierungsstelle	Format der zu exportierenden Datei Zertifikate können in verschiedenen Dateiformaten exportiert werden.	
	Zertifizierungsstellenzertifikate: Zertifikat Nr.0 (abgelaufen) Zertifikat Nr. 1 Zertifikat Nr. 2	Wählen Sie das gewünschte Format:	-
	Zertilikat Nr. 2	DER-codiert-binär X.509 (.CER)	
		O Base-64-codiert X.509 (.CER)	
		Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)	
		Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen	
		O Privater Informationsaustausch - PKCS #12 (.PFX)	
		Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen	
	Kryptografieeinstellungen	Privaten Schlüssel nach erfolgreichem Export löschen	
	Anbieter: Microsoft Software Key Stor	Alle erweiterten Eigenschaften exportieren	
	Hashalgorithmus: SHA256	Zertifikatdatenschutz aktivieren	
		Microsoft Serieller Zertifikatspeicher (.SST)	
	OK Abbrechen Über	Weiter Abbrechen	
<	>		
	- 1		

Diese Datei lege ich im AIA-Verzeichnis ab, denn hier könnte ein Client danach suchen:



Datei Aktion	Ansicht ?	ITS-Zertifizierupgsstelle-CA1 2						
(= =) 2 ··	genscharten von we	-H3-Zerunzierungssteile-Ci				×		
Zertifizie	Speicherung	Zortifikatuonualtungen						×
✓ 🛃 WS-I	Uberwachung Allgemein Dightli	Speichern unter						
	Tuchai	\leftarrow \rightarrow \checkmark \uparrow \square \Rightarrow Dieser PC \Rightarrow System	em (C:) → Admin → PKI		5 V	"PKI" durchsucher	ı	Q
🚆 A 🛅 F	Zertifizierungsstelle Name:	Organisieren 👻 Neuer Ordner						?
🚞 Z	Zertifizierungssteller	🏪 System (C:) 🔺 Name	^	Änderungsdatum	Тур	Größe		
	Zertifikat Nr.0 (abo	Admin		1				
	Zertifikat Nr. 1 Zertifikat Nr. 2	PKI	Es wu	den keine Suchergebni	sse gefunden.			
	Lorenteer m. L	Benutzer						
		inetpub						
		Perflogs						
		Brogram Filer						
		Dregramme						
	Kryptografieeinstellu	Users						
	Anbieter:	.NET v4.5						
	Hashalgorithmus:	.NET v4.5 CI *						
		Dateiname: WS-ITS-Zertifizierung	sstelle-CA1(2).crt					\sim
		Dateityp: DER-codiertes binäres	X.509 (*.cer)					\sim
		∧ Ordner ausblenden			[Speichern	Abbrech	en
	ок							

Achtung: Die Dateiendung wurde nicht korrekt erstellt und muss korrigiert werden:

📙 🛃 📕 🖛 PKI							_		×
Datei Start Freigeben	Datei Start Freigeben Ansicht								~ 🕐
← → × ↑ 📙 > Dieser PC	← → < ↑ 📙 > Dieser PC > System (C:) > Admin > PKI								Q
👻 📌 Schnellzugriff	^	Name	Änderungsdatum	Тур	Größe				
Cesktop		web.config	11.12.2020 19:54	CONFIG-Datei	1 KB				
Downloads	*	E WS-ITS-Zertifizierungsstelle-CA1(1).crl	11.12.2020 19:49	Zertifikatssperrliste	1 KB				
Dokumente		🙀 WS-ITS-Zertifizierungsstelle-CA1(1).crt.cer	12.12.2020 15:45	Sicherheitszertifikat	1 KB				
Eilder	<u> </u>	WS-ITS-Zertifizierungsstelle-CA1(1)+.crl	11.12.2020 19:49	Zertifikatssperrliste	1 KB				
E bide	- 1	🙀 WS-ITS-Zertifizierungsstelle-CA1(2).crt.cer	12.12.2020 15:44	Sicherheitszertifikat	1 KB				
🗸 📃 Desktop		E WS-ITS-Zertifizierungsstelle-CA1.crl	11.12.2020 19:49	Zertifikatssperrliste	1 KB				
> 🤱 Walther, Stephan - T1		WS-ITS-Zertifizierungsstelle-CA1+.crl	11.12.2020 19:49	Zertifikatssperrliste	1 KB				
🗸 💻 Dieser PC									
🗸 🏪 System (C:)									
🗸 📙 Admin									
PKI									
> Benutzer									

Nun erstelle ich eine neue Sperrliste für die beiden gültigen Zertifizierungsstellen-Zertifikate:

🙀 certsrv - [Zertifizierung	🗊 certsrv - [Zertifizierungsstelle (Lokal)\\WS-ITS-Zertifizierungsstelle-CA1]						
Datei Aktion Ansicht	?						
🗢 🔿 🖄 🔚 🙆 📄	🛛 🕨 🔳						
Zertifizierungsstelle (Lo	kal) Name ngsstelle-C Gesperrte	Zertifikate					
Gesperrte Ze	Alle Aufgaben >	Veröffentlichen					
Ausstehende Fehlgeschlag	Aktualisieren	gene Anforderungen					
Zertifikatvor	Eigenschaften	rlagen					
	Hilfe						

WS IT-Solutions

WSHowTo – Migration einer Windows PKI (WS-CA1) 2020-11-28 Migration auf Windows Server 2019



OK, das scheint noch nicht zu funktionieren. Im Active Directory gab es keine Veröffentlichung:

🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS	S-ITS-Zertifizierungsstelle-CA1]	_	\times
Datei Aktion Ansicht ?			
🗢 🔿 🙍 🗐 🧟 🕞 🖌 🕨 💻			
 Zertifizierungsstelle (Lokal) WS-ITS-Zertifizierungssteller.C Gesperte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderung Fehlgeschlagene Anforder Zertifikatvorlagen 	ne iesperte Zertifikate usstehende Anforderungen ehlgeschlagene Anforderungen sertifikatvorlagen Microsoft-Active Directory-Zertifikatdienste Verzeichnisobjekt nicht gefunden. 0x8007208d (WIN32: 8333 ERROR_DS_OBJ_NOT_FOUND) OK		

Im Dateisystem dagegen ist die neue Sperrliste erstellt worden:

📙 🛃 🧧 🖛 PKI							-	×
Datei Start Freigeben	Ansicht							~
← → × ↑ 🔒 > Dieser P	C → Syster	m (C:) > Admin > PKI				~ 0	"PKI" durchsuchen	Q
🖌 📌 Schnellzugriff	^	Name	Änderungsdatum	Тур	Größe			
E Desktop	*	web.config	11.12.2020 19:54	CONFIG-Datei	1 KB			
Downloads	*	WS-ITS-Zertifizierungsstelle-CA1(1).crl	12.12.2020 15:46	Zertifikatssperrliste	1 KB			
Dokumente		🐺 WS-ITS-Zertifizierungsstelle-CA1(1).crt	12.12.2020 15:45	Sicherheitszertifikat	1 KB			
Dida.	-	₩S-ITS-Zertifizierungsstelle-CA1(1)+.crl	12.12.2020 15:46	Zertifikatssperrliste	1 KB			
Ellder	*	WS-ITS-Zertifizierungsstelle-CA1(2).crl	12.12.2020 15:46	Zertifikatssperrliste	1 KB			
📃 Desktop		🔄 WS-ITS-Zertifizierungsstelle-CA1(2).crt	12.12.2020 15:44	Sicherheitszertifikat	1 KB			
> 🤱 Walther, Stephan - T1		WS-ITS-Zertifizierungsstelle-CA1(2)+.crl	12.12.2020 15:46	Zertifikatssperrliste	1 KB			
V Dieser PC		E WS-ITS-Zertifizierungsstelle-CA1.crl	12.12.2020 15:46	Zertifikatssperrliste	1 KB			
V System (C:)		WS-ITS-Zertifizierungsstelle-CA1+.crl	12.12.2020 15:46	Zertifikatssperrliste	1 KB			
Admin								
PKI								
> Benutzer								

Also ist es ein reiner Fehler im Active Directory...

TroubleShooting – Korrektur des LDAP-Sperrlistenverteilungspunktes

Im Active Directory veröffentlicht meine Windows Zertifizierungsstelle in der Konfigurationspartition ihre Sperrlisten. Hier finde ich 2 Sperrlisten – je eine pro altes Zertifizierungsstellen-Zertifikat. Aber für das neue Zertifikat fehlt der Eintrag! Stimmen hier vielleicht die Berechtigungen nicht?

WS IT-Solutions

Die Berechtigung für das Bearbeiten der beiden alten Sperrlisten ist an den Computer-Account gebunden:



Aber auf dem darüberliegenden Container "CN=WS-CA1" fehlt die Berechtigung! Normal wird der Record einer neuen Sperrliste durch den Benutzer-Account des Administrators automatisch erzeugt und dann wird das Recht automatisch an den Computer-Account delegiert. Aber meine Admin-Kennung ist kein Mitglied der Gruppe Enterprise-Admins, wie es eigentlich üblich ist. Daher wurde der Record nicht erstellt und die Windows CA kann ihn danach auch nicht aktualisieren.

Der Versuch, die Berechtigung auf dem Container direkt an die Windows CA bzw. an den Computer-Account zu delegieren wird nicht ausreichen. Aber dennoch wage ich einen Versuch und nehme den Computer-Account in die ACL auf:

Z ADSI-Editor				
Datei Aktion Ansicht ?				
<table-cell-rows> 🔿 🔁 📰 🗙 🖾 🗟 📑</table-cell-rows>				
ADSI-Editor Standardmäßiger Namenskontext [WS-DC1.ws.its] CN=Configuration [WS-DC1.ws.its] CN=Configuration, DC= ws,DC= its CN=DisplaySpecifiers CN=DisplaySpecifiers CN=Extended-Rights CN=ForestUpdates CN=ForestUpdates	Name CN=WS-ITS-Zertifizierungsstelle-CA1 CN=WS-ITS-Zertifizierungsstelle-CA1(1) Eigenschaften von CN=WS-CA1 Attribut-Editor Sicherheit	Klasse cRLDistributi cRLDistributi ? ×	Definierter Name CN=WS-ITS-Zertifizierungsstelle-CA1,CN=WS-CA CN=WS-ITS-Zertifizierungsstelle-CA1(1),CN=WS-	11,CN=CDP,CN=Public K CA1,CN=CDP,CN=Public
CN=NTDS Quotas CN=Partitions CN=Physical Locations CN=Services CN=Services CN=CarthN Policy Configuration CN=Carton Key Distribution Service CN=Group Key Distribution Service CN=Microsoft Exchange	Gruppen- oder Benutzemamen: & Jeder & Domänen-Admins (WS\Domänen-Admins) & Zettifkatherausgeber (WS\Zettifkatherausgeber) & Organisations-Admins (WS\Corganisations-Admins) & Administratoren (WS\Administratoren)	Benutzer, Co Objekttyp: Benutzer, Co Suchpfad:	omputer, Dienstkonten oder Gruppen auswählen omputer, Gruppen oder Integrierte Sicherheitsprinzipale	X
CN=Microsoft Exchange Autodiscover CN=Microsoft SPP CN=Microsoft SPP CN=NetServices CN=Public Key Services CN=ALA CN=CDP CN=CDP CN=CDP CN=WS-CA1	Hinzufügen Berechtigungen für "Zertfikatherausgeber" Zulassen Vollzugriff Lesen Schreiben Alle untergeordneten Objekte enstellen Alle untergeordneten Objekte enstellen	ws.its Geben Sie d ws-ca1 Erweite	ie zu verwendenden Objektnamen ein (<u>Beispiele</u>): nt OK	Pfade Namen überprüfen Abbrechen
CN=Certification Authorities CN=Enrollment Services CN=KRA CN=OID CN=RAS CN=RAS	Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen.	Erweitert		

Denn hier kann ich auch das Recht auf untergeordnete Objekte delegieren:





Nun muss ich nur noch ein cRLDistributionPoint-Object erzeugen – das würde ein Admin mit Enterprise-Permission automatisch bei Ausstellen eines neuen Zertifizierungsstellen-Zertifikates in der Windows CA mit erledigen:



Der Datentyp ist leicht zu finden:

WS IT-Solutions

Absiliation						
Datei Aktion Ansicht ?						
🗢 🔿 📩 🖾 🖾 🖾						
ADSI-Editor Standardmäßiger Namenskontext [WS-DC1.ws.its	Name	S-Zertifizierungss	Klasse cRLDistributionPoint	Definierter Name CN=WS-ITS-Zertifizierungsstelle-1		
Konfiguration [WS-DC1.ws.its] CN=Configuration,DC=ws,DC=its CN=DisplaySpecifiers	CN=WS-ITS	CN=WS-ITS-Zertifizierungsstelle-CA1(1) Objekt erstellen		cRLDistributionPoint	CN=WS-IT	S-Zertifizierungsstelle-CA1(1
 CN=DisplaySpecifiers CN=Extended-Rights CN=ForestUpdates CN=LostAndFoundConfig CN=NTDS Quotas CN=Partitions CN=Partitions CN=Physical Locations CN=Services CN=Carbox AuthN Policy Configuration CN=Claims Configuration CN=Claims Configuration CN=Group Key Distribution Service CN=Microsoft Exchange Autodiscover CN=Microsoft SPP CN=Microsoft SPP CN=Microsoft SPP CN=VetServices CN=Public Key Services CN=AIA CN=COP CN=Certificate Templates CN=Enrollment Services CN=Enrollment Services CN=Enrollment Services 		Wählen Sie e G G G G G G G G G G G G G G G G G G	tine [Jasse aus: assStore mConnectionPoint nitart nitainer nitrolAccessRight RLDistributionPoint evice Scomfguration fCPClass splaySpecifier splayTemplate isZone soument	er > Abbrechen	Hilfe	
CN=KRA CN=CN=OD CN=OD CN=RRAS						

Der Name des neuen CRL-Objektes muss sich an dem Schema der Benennung orientieren. Das neue Zertifizierungsstellen-Zertifikat hat den Zähler (2). Der muss hier mit aufgenommen werden:



Ein Blick in die ACL der neuen CRL zeigt, dass meine Windows CA nicht berechtigt wurde. Egal, dann füge ich den erforderlichen Eintrag manuell ein: WS IT-Solutions

📝 ADSI-Editor						
Datei Aktion Ansicht ?						
ADSI-Editor Standardmäßiger Namenskontext [WS-DC1.ws.its]	Name	-i	Klasse		Definierter Name	
 Konfiguration [WS-DC1.ws.its] CN=Configuration.DC=ws.DC=its 	CN=WS-ITS-Zertifi	zierungsstelle-CA1 zierungsstelle-CA1(1)	cRLDist	tributionPoint	CN=WS-ITS-Zertifizierung	sstelle-CA1,
CN=DisplaySpecifiers	CN=WS-ITS-Zertifi	zierungsstelle-CA1(2)	cRLDist	tributionPoint	CN=WS-ITS-Zertifizierung	sstelle-CA1(
CN=ForestUpdates	Eigensch	aften von CN=WS-ITS-Zer	tifizierungsstelle-C	? ×		
CN=LostAndFoundConfig CN=NTDS Quotas	Attribut-E	ditor Sicherheit				
CN=Partitions CN=Physical Locations	Grupper St. Je	n- oder Benutzemamen: der		^		
CN=Services CN= AuthN Bolizy Configuration	🧟 Au 🕵 Si	thentifizierte Benutzer /STEM	Benutzer, Computer	r, Dienstkonter	n oder Gruppen auswählen	
CN=Claims Configuration	SE Do	omänen-Admins (WS\Domäne utifikatherausgeber (WS\Zerti	Obiekttyp:			
CN=Group Key Distribution Service CN=Microsoft Exchange	52 Or	ganisations-Admins (WS\Orga	Benutzer, Computer,	Gruppen oder In	ntegrierte Sicherheitsprinzipale	Objekt
CN=Microsoft Exchange Autodiscover	Add Add	ministratoren (VV-5 (Administra	Suchpfad:			
CN=MsmqServices	Berecht	igungen für "Jeder"	Gabar Sia dia muura	waa daa daa Ohio		Ptac
CN=NetServices	Vollz	Jgriff	WS-CA1	wendenden Obje	ektriamen ein (<u>beispiele</u>).	Namen ü
CN=AIA	Lese	n eiben				
CN=WS-CA1	Spez	ielle Berechtigungen	Erweitert		ОК	Abbre
Che Certification Authorities	Klicken	Sie auf "Erweitert", um spezie	elle	-		
CN=Enrollment Services	Berecht	igungen anzuzeigen.		Erweitert		
				1.147		
		OK Abbie	Obernenmen	niie		
Z ADSI-Editor Datei Aktion Ansicht ?						
					1	
ADSI-Editor Standardmäßiger Namenskontext [WS-DC1.ws.its	Name	zierungsstelle-CA1	Klasse cRI Dist	tributionPoint	Definierter Name	sstelle-CA1
 Konfiguration [WS-DC1.ws.its] CN=Configuration DC=ws.DC=its 	CN=WS-ITS-Zertifi	zierungsstelle-CA1(1)	cRLDist	tributionPoint	CN=WS-ITS-Zertifizierung	sstelle-CA1,
CN=DisplaySpecifiers	CN=WS-ITS-Zertifi	zierungsstelle-CA1(2)	cRLDist	tributionPoint	CN=WS-ITS-Zertifizierung	sstelle-CA1(
CN=Extended-Rights	Eigensch	aften von CN=WS-ITS-Zer	tifizierungsstelle-C	? ×		
CN=LostAndFoundConfig	Attribut-E	ditor Sicherheit				
CN=Partitions	Gruppe St. St.	n- oder Benutzernamen: /STEM		^		
 CN=Services 	SE Do	mänen-Admins (WS\Domäne ttifikatherausgeber (WS\Zetti	en-Admins) fikatherausgeber)			
CN=AuthN Policy Configuration CN=Claims Configuration		ganisations-Admins (WS\Orga	anisations-Admins)			
CN=Group Key Distribution Service CN=Microsoft Exchange	2.0	S-CA1\$ (WS\WS-CA1\$)	tolen)			
CN=Microsoft Exchange Autodiscover			Hinzufügen	Fatfemen		
CN=MsmqServices	Berecht	igungen für "WS-CA1\$"	7.1			
CN=NetServices CN=Public Key Services	Vollz	Jgriff	Zulassen			
CN=AIA	Lese	n eiben				
CN=WS-CA1	Spez	ielle Berechtigungen				
CN=Certificate Templates CN=Certification Authorities	Klicken	Sie auf "Erweitert" um sparie				
CN=Enrollment Services	Berecht	igungen anzuzeigen.		Erweitert		
		01				
CIVERRAS		OK Abbre	chen Ubernehmen	Hilfe		

Nun starte ich auf meinem CA-Server die CRL-Generierung erneut – das geht auch über die cmd. Und jetzt ist der Vorgang erfolgreich:



Fortsetzung der Grundkonfiguration

IT-Solutions

Jede Anpassung an den Zertifizierungsstellen-Zertifikaten, den AIA-Positionen oder den Sperrlisten sollte mit PKIVIEW kontrolliert werden. Ich starte die msc. Das Ergebnis überrascht mich nicht. Es gibt noch Korrekturbedarf bei der Deltasperrliste und OCSP ist noch nicht installiert:

🏨 pkiview - [Unternehmens-PKI\WS-ITS-Zertifizierungsstelle-CA1 (V2.2)]								
Datei Aktion Ansicht ?								
🗢 🔿 🛛 🖻 🔒 🛛								
👸 Unternehmens-PKI	Name	Status	Ablaufdatum	Ort				
WS-ITS-Zertifizierungsstelle-CA1 (V2.2)	🙀 Zertifizierungsstellenzertifikat	Verifizierung	12.12.2025 15:37					
	AIA-Speicherort #1	ОК	12.12.2025 15:37	http://ca.ws-its.de/certs/WS-ITS-Zertifizierungsstelle-CA1(2).crt				
	🗵 Speicherort für Sperrlisten-Verteilungspunkte #1	OK	20.12.2020 04:09	http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2).crl				
	E DeltaCRL-Speicherort #1	Download ni		http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2)+.crl				
	OCSP-Speicherort #1	Fehler		http://ca.ws-its.de/ocsp				

Die Deltasperrliste enthält ein plus-Zeichen. Dieses Sonderzeichen ist in einer URL nicht gerne gesehen. Ein IIS kann das nur mit dem sogenannten "Double-Escaping". Das Feature muss manuell im IIS-Manager aktiviert werden:

💐 Internetinformationsdienste (IIS)-	-Manager	- 🗆 ×
← → ² → WS-CA1 → Sit	ites > Default Web Site > crl >	🔯 🚿 🟠 🔞 -
Datei Ansicht ?		
Verbindungen Image: Startseite Image: Startseite Image: Startseite Image: Startseite	Konfigurations-Editor Abschnitt: system.webServer/security/requestFiltering Von: Default Web Site/crl Web.config	Aktionen
Anwendungspools	Unterste Pfadebene: MACHINE/WEBROOT/APPHOST	Skript generieren
 ✓ Sites ✓ ♦ Default Web Site 	allowDoubleEscaping True allowHighBitCharacters True	Konfiguration Konfiguration suchen
> - aspnet_client	alwaysAllowedQueryStrings (Count=0) alwaysAllowedUrls (Count=0)	Abschnitt
> 💭 crl	denyQueryStringSequences (Count=0)	Abschnitt sperren
	denyUrlSequences (Count=0)	'allowDoubleEscaping'-Attri bute
	filteringRules (Count=0)	Attribut sperren
	> hiddenSegments	Hilfe
	removeServerHeader False	
	unescapeQueryString True	
	> verbs	

Nach einer PKIVIEW-Aktualisierung ist die Deltasperrliste erreichbar:

🟥 pkiview - [Unternehmens-PKI\WS-ITS-Zertifizie	erungsstelle-CA1 (V2.2)]			
Datei Aktion Ansicht ?				
🗢 🔿 🙍 🗟 🗟				
Unternehmens-PKI WS-ITS-Zertifizierungsstelle-CA1 (V2.2)	Name	Status	Ablaufdatum	Ort
	🐺 Zertifizierungsstellenzertifikat	ОК	12.12.2025 15:37	
	🗊 AIA-Speicherort #1	OK	12.12.2025 15:37	http://ca.ws-its.de/certs/WS-ITS-Zertifizierungsstelle-CA1(2).crt
	📱 Speicherort für Sperrlisten-Verteilungspunkte #1	OK	20.12.2020 04:09	http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2).crl
	E DeltaCRL-Speicherort #1	OK	14.12.2020 04:09	http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2)+.crl
	Proceeding of the second secon	Fehler		http://ca.ws-its.de/ocsp

Nun schließe ich noch einige andere Konfigurationen ab. Dazu gehört die Aktivierung des Loggings. Eine erforderliche Voraussetzung ist die Aktivierung und die Konfiguration des Advanced Audits. Diese habe ich global über Gruppenrichtlinien bereits abgeschlossen. So fehlen nur noch einige Haken in den Properties meiner neuen CA:



-Zertifizierungsstelle-CA1]	$ \Box$ \times
Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? X	
Speicherung Zertifikatverwaltungen Registrierungs-Agents	
Allgemein Richtlinienmodul Beendigungsmodul Erweiterungen	
Überwachung Wiederherstellungs-Agents Sicherheit	
Sie müssen die Überwachung des Objektzugriffs in der Gruppenrichtlinie aktivieren, um die Ereignissprotokollierung im Sicherheitsprotokoll zu starten.	
Zu überwachende Ereignisse:	
Datenbank der Zertifizierungsstelle sichem/wiederherstellen	
Zertifizierungsstellenkonfiguration ändem	
Sicherheitseinstellungen der Zertifizierungsstelle ändern	
Zertifikatanforderungen verwalten und ausstellen	
Zertifikate sperren und Spertisten veröffentlichen	
Archivierte Schlüssel sichem und abrufen	
Active Directory-Zertifikatdienste starten/beenden	
OK Abbrechen Übernehmen Hilfe	
	-Zertifizierungsstelle-CA1] Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? × Speicherung Zertifikatverwaltungen Registrierungs-Agents Algemein Richtlinienmodul Beendigungsmodul Erweiterungen Überwachung Wiederherstellungs-Agents Sicherheit Sie müssen die Überwachung des Objektzugriffs in der Gruppernichtlinie aktivieren, um die Ereignisser: Debenhark der Zertifizierungsstelle sichem/wiederherstellen Zertifizierungsstellenkonfiguration ändem Sicherheitseinstellungen der Zertifizierungsstelle ändem Zertifizierungsstellenkonfiguration ändem Zertifizierungsstellen veröffentlichen Zertifizierungstellen und abnufen Zertifizierungstellen und abnufen Zertifizierungstellen und abnufen Zertifizierungstellenkonfiguration beenden

Damit ist die Grundkonfiguration abgeschlossen.

Bereitstellung des Online Responders

Weiter geht es mit den Zusatzdiensten. Der Online Responder ist eine Web-Anwendung, mit der ein Client ein einzelnes Zertifikat durch seine Seriennummer auf eine Sperrung überprüfen kann, ohne dabei selbst die komplette Sperrliste herunterladen und durchsuchen zu müssen. Ohne den Download der Sperrliste umgehe ich das Abwarten der Cache-Dauer der Sperrliste im Falle einer Zertifikatsperrung. Oder kurz gesagt: Jeder Client kann Zertifikate live und in "Echtzeit" auf Sperrung validieren lassen.

Der Online Responder muss seine Antworten digital signieren, damit der Client ihm vertraut. Dafür benötige ich eine spezielle Zertifikatvorlage. Diese erstelle ich in meiner Zertifizierungsstelle:



Ich kopiere das Original:

WS IT-Solutions

Datei Aktion Ansicht ?							_	~
Zertifikatvorlagen (WS-DC1.ws.i	Vorlagenanzeigename		Schemaversion	Version	Beabsicht ^	Aktionen		
	🖳 Key Recovery Agent		2	105.0	Key Recov	Zertifikatvorlagen (WS-DC1.ws.its)		-
	🗷 Nur Benutzersignatur		1	4.1		Weitere Aktionen		
	🚇 Nur Exchange-Signatur		1	6.1				
	OCSP-Antwortsignat		2	101.0	OCSP-Sig	OCSP-Antwortsignatur		-
	🗷 RAS- und IAS-Server	Vorlage duplizieren		101.0	Clientautł	Weitere Aktionen		•
	Router (Offlineanford	Alle Zertifikatinhabe	er erneut registrieren	4.1				
	🖳 Smartcard-Anmeldu	Alle Aufgaben		, 6.1				
	Smartcard-Benutzer	5		11.1				
	Stammzertifizierungs	Eigenschaften		5.1				
	🚇 Übergreifende Zertifi	Hilfe		105.0				
	Untergeordnete Zerti			5.1				
	Vertrauenslistensignatur		1	3.1				
	Verzeichnis-E-Mail-Replik	ation	2	115.0	Verzeichn			
	Webserver		1	4.1				
	WS-ITS-Benutzer		2	101.0	Clientaut			
	WS-ITS-Benutzer-V2		3	100.5	Clientaut			
	WS-ITS-Bitlocker		4	100.6	BitLocker			
	WS-ITS-CodeSignatur		2	100.4	Codesign			
	WS-ITS-CodeSignatur-V2		3	100.11	Codesign			
	WS-ITS-Computer		2	100.11	Clientauti			
	WS-ITS-DomainController		2	100.15	Septeraut			
	WS ITS DomainControlle	- 1/2	2	100.4	KDC Auth			
	WS-ITS-SmartCard	1-12	4	100.0	Smartcarr			
	WS-ITS-SmartCard-V2		4	100.4	Smartcarc			
	INC ITS VIDIL agin		2	100.11	Cmarteare V			
< >	<				>			

Oder auch nicht. Denn auch hierfür sind Enterprise-Adminrechte erforderlich...

Datei Aktion Ansicht ?	/orlagenanzeigename a Key Recovery Agent a Nur Benutzersignatur Nur Exchange-Signatur 0 COSP-Antworksionatur		Schemaversion 2	Version	Beabsicht ^	Aktionen
← →	/orlagenanzeigename 2 Key Recovery Agent 2 Nur Benutzersignatur 2 Nur Exchange-Signatur 0 CCSP-Antwordsignatur		Schemaversion 2	Version	Beabsicht ^	Aktionen
Zertifikatvorlagen (WS-DC1.ws.i	/orlagenanzeigename ^ 2 Key Recovery Agent 2 Nur Benutzersignatur 2 Nur Exchange-Signatur 3 OCSP-Antwortsignatur		Schemaversion 2	Version	Beabsicht ^	Aktionen
19 19 19 19 19 19 19 19 19 19 19 19 19 1	교 Key Recovery Agent 고 Nur Benutzersignatur 고 Nur Exchange-Signatur OCSP-Antwortsignatur		2	105.0		
2 2 2 2 2	Nur Benutzersignatur Nur Exchange-Signatur OCSP-Antwortsignatur			105.0	Key Recov	Zertifikatvorlagen (WS-DC1.ws.its)
ي الا الا	Nur Exchange-Signatur OCSP-Antwortsignatur		1	4.1		Weitere Aktionen
	OCSP-Antwortsignatur		1	6.1		Treffere Aktorien
4			3	101.0	OCSP-Sig	OCSP-Antwortsignatur
	RAS- und IAS-Server		2	101.0	Clientautł	Weitere Aktionen
	Router (Offlineanforderung)		1	4.1		
	Smartcard-Anmeldung		1	6.1		
	Smartcard-Benutzer		1	11.1		
	🛛 Stammzertifizierungsstelle		1	5.1		
	🗟 Übergreifende Zertifizierungsstelle		2	105.0		
	Untergeordnete Zertifizierungsst	7				
	Vertrauenslistensignatur '	Zertifikatvori	agen			~
	Verzeichnis-E-Mail-Replikation					
	Webserver	🛕 Die	e Zertifikatvorlage "OCSF	-Antwortsignat	t	
49	WS-ITS-Benutzer	🔼 ko	piert werden. Zugriff ver	weigert		
49	WS-ITS-Benutzer-V2					
	WS-ITS-Bitlocker				C C K	
49	WS-ITS-CodeSignatur					
4	WS-ITS-CodeSignatur-V2		3	100.11	Codesign	
4	WS-ITS-Computer		2	100.11	Serveraut	
4	WS-ITS-Computer-V2		3	100.13	Clientautł	
	WS-ITS-DomainController		3	100.4	Serverautl	
4	WS-ITS-DomainController-V2		3	100.8	KDC-Autł	
	WS-ITS-SmartCard		4	100.4	Smartcarc	
4	WS-ITS-SmartCard-V2		4	100.11	Smartcarc	
< > <			1	100 /	Constrair ×	

Das hatte ich für meine PKI nie angepasst. Aber heute ist dafür der richtige Zeitpunkt. Ich wechsle auf meinen Domain Controller mit meiner TO-Kennung. Diese nehme ich zuvor in die Gruppe Enterprise-Admins auf. Im ADSIEdit navigiere ich zum Container, in dem die Templates liegen. Hier editiere ich die ACL und nehme meine eigene Gruppe LD-Admin-PKI mit Schreibrechten auf:



📝 ADSI-Editor Datei Aktion Ansicht ? 🗢 Þ 🙋 📰 🗙 🗐 🔂 🖬 ADSI-Editor Name Klasse Definierter Name Standardmäßiger Namenskontext [WS-DC1.ws.its CN=Administrato pKICertificateTem.. CN=Administrator, CN=Certificate T Ξ Konfiguration [WS-DC1.ws.its] CN=CA pKICertificateTem... CN=CA, CN=Certificate Templates, C CN=Configuration,DC=ws,DC=its CN=CAExchange pKICertificateTem... CN=CAExchange,CN=Certificate Ter CN=DisplaySpecifiers CN=CEPEncryption pKICertificateTem.. CN=CEPEncryption,CN=Certificate CN=Extended-Rights CN=ClientAuth N=Certificate Tem Eigenschaften von CN=Certificate Templates ? Х CN=ForestUpdates CN=CodeSigning CN=Certificate Te CN=LostAndFoundConfig Attribut-Editor Sicherheit CN=CrossCA Certificate Templa CN=NTDS Quotas CN=CTLSigning N=Certificate Terr CN=Partitions Gruppen- oder Benutzemamen: CN=DirectoryEmailRepli ilReplication CN= **CN=Physical Locations** Authentifizierte Benutzer CN=Services CN=DomainController oller, CN=Certifica SYSTEM . CN=AuthN Policy Configuration CN=DomainController ollerAuthenticatio Domänen-Admins (WS\Domänen-Admins) **CN=Claims Configuration** CN=EFS LD-Admin-PKI (WS\LD-Admin-PKI) ficate Templates,C CN=Group Key Distribution Service CN=EFSRecovery Se Organisa tions-Admins (WS\Organisations-Admins) CN=Certificate Ter CN=Microsoft Exchange CN=EnrollmentAgent ent CN=Certificat CN=Microsoft Exchange Autodiscover CN=EnrollmentAgentOf entOffline,CN=Ce CN=Microsoft SPP CN=ExchangeUse Hinzufügen... Entfernen ,CN=Certificate To CN=MsmqServices CN=ExchangeUserSigna Signature, CN=Ce CN=NetServices Berechtigungen für "LD-Admin-PKI CN=IPSECIntermediateC Zula diateOffline,CN=C CN=Public Key Services CN=IPSECIntermediated Vollzugriff diateOnline CN=C 📔 CN=AIA CN=KerberosAuthentica \checkmark entication,CN=Ce Lesen CN=CDP CN=KeyRecoveryAgent Schreiben \checkmark gent, CN=Certific CN=Certificate Templates Alle untergeordneten Objekte erstellen \checkmark CN=Machine Certificate Templa CN=Certification Authorities \square CN=MachineEnrollmen Alle untergeordneten Objekte löschen IlmentAgent,CN= CN=Enrollment Services CN=OCSPResponseSig seSigning,CN=Cer Klicken Sie auf "Erweitert", um spezielle CN=KRA Erweitert CN=OfflineRouter Berechtigungen anzuzeigen CN=Certificate Te CN=OID CN=RASAndIASServer rver,CN=Certificat CN=RRAS CN=SmartcardLogon jon,CN=Certificate CN=Shadow Principal Configuration Abbrechen Übernehmen OK CN=SmartcardUser r,CN=Certificate 1 CN=Windows NT CN=Sites CN=SubCA.CN=Certificate Template CN=SubCA pKICertificateTem...

Die Aktion wiederhole ich auf dem dazugehörigen Container OID:



Anschließend dupliziere ich erfolgreich die Vorlage in meiner Zertifizierungsstelle. Nun kann ich noch einige Parameter anpassen. Dazu gehört die Kompatibilitätsebene:

WS IT-Solutions

Zertifikatvorlagenkonsole					_			
Datei Aktion Ansicht ?					Г			
		Eigenschaften der neuen Vo	rlage	×				
R Zertifikatvorlagen (WS-DC1.ws.i	Vorlagenanzeigename	Schlüsselnachweis	Antragstellemame	Server	Aktionen			
		Ausstellungsvoraussetzungen	Abgelöste Vorlagen Erweiter	rungen Sicherheit				
	Kerberos-Authentinz	Kompatibilitat Allgemein	Anforderungsverarbeitung	Kryptografie	Zertifikatvorlagen (WS-DC1.WS.Its)	•		
	Rey Recovery Agent	Die verfügbaren Vorlagenop	tionen basieren auf den frühester	Weitere Aktionen	•			
	Rur Exchange-Signa	"Kompatibilitätseinstellungen	"festgelegten Betriebssystemver	OCSP-Antwortsignatur				
	OCSP-Antwortsigna	_			Weitere Aktionen	•		
	RAS- und IAS-Server	Resultierende Änderunge	en anzeigen		,			
	Router (Offlineanfor	March March 1991						
	🚇 Smartcard-Anmeldu	Kompatibilitatseinstellunger	1					
	Smartcard-Benutzer	Zertifizierungsstelle						
	Stammzertifizierung	Windows Server 2008 R	2 ~					
	🚇 Übergreifende Zertif							
	Untergeordnete Zert	Zertifikatsempfänger						
	Vertrauenslistensigna	Windows 7 / Server 200	8 R2 ~					
	Websenies							
	WS-ITS-Benutzer							
	WS-ITS-Benutzer-V2							
	WS-ITS-Bitlocker							
	WS-ITS-CodeSignate							
	WS-ITS-CodeSignati	Diese Einstellungen verhinde	em möglicherweise nicht, dass fri	ühere				
	Reference WS-ITS-Computer	Betriebssystemversionen die	se Vorlage verwenden.					
	Reference WS-ITS-Computer-V							
	WS-ITS-DomainCon							
	WS-ITS-DomainCon							
	WS-ITS-SmartCard	ОК	Abbrechen Übernehm	ien Hilfe				
< >	<			>				

Auch der Name darf sich in mein Namensschema einfügen:

Zertifikatvorlagenkonsole		- 🗆 ×
Datei Aktion Ansicht ?	Eigenschaften der neuen Vorlage X]
Retifikatvorlagen (WS-DC1.ws.i Vorlagenanzeigename	Schlüsselnachweis Antragstellemame Server	Aktionen
I Kerberos-Authentif	Ausstellungsvoraussetzungen Abgeloste Vorlagen Erweiterungen Sicherheit	Zertifikatvorlagen (WS-DC1.ws.its)
Rey Recovery Agen	Rompatolicat Performance Performance and a respiration	Weitere Aktionen
🗷 Nur Benutzersignat	Vorlagenanzeigename:	Trettere / Matorien
🚇 Nur Exchange-Sign	WS-ITS-Online Responder-V1	OCSP-Antwortsignatur
OCSP-Antwortsign		Weitere Aktionen
RAS- und IAS-Serve		
Router (Offlineanfo	Vorlagenname:	
B Smartcard-Anmeld	WS-ITS-OnlineResponder-V1	
Stammantifiziorum		
I Übergreifende Zerti		
	Gültigkeitsdauer: Erneuerungszeitraum:	
2 Vertrauenslistensign	2 Wochen V 2 Tage V	
Reverse Verzeichnis-E-Mail-		
R Webserver	Zertifikat in Active Directory veröffentlichen	
Reputer WS-ITS-Benutzer	Nicht automatisch neu registrieren, wenn ein identisches Zertifikat	
WS-ITS-Benutzer-V	bereits in Active Directory vorhanden ist	
Reference WS-ITS-Bitlocker		
Regional WS-ITS-CodeSignat		
WS-ITS-CodeSignat		
WS-ITS-Computer		
WS-ITS-Computer-		
WS-ITS-DomainCol		
WS-ITS-SmartCard	OV Alberton Observer	
In the state of th	OK Abbrechen Übernehmen Hilfe	
	>	

Die Kryptografie passt für den Anwendungsfall:



Zertifikatvorlagenkonsole					— [□ ×
Datei Aktion Ansicht ?				~	Г	
		Eigenschaften der neuen Vo	riage	~		
R Zertifikatvorlagen (WS-DC1.ws.i	Vorlagenanzeigename	Schlüsselnachweis	Antragstellemame	Server	Aktionen	
		Ausstellungsvoraussetzungen	Abgelöste Vorlagen Erweiten	ungen Sicherheit		
	Key Recovery Agent	Kompatibilität Allgemeir	Anforderungsverarbeitung	Kryptografie	Zertifikatvoriagen (WS-DCT.ws.its)	•
	Rey Recovery Agent	Anbieterkategorie:	Schlüsselsneicheranhieter	~	Weitere Aktionen	•
	Rur Exchange-Signa	News des Alexables			OCSP-Antwortsignatur	
	OCSP-Antwortsigna	Name des Algonthmus:	RSA	~	Weitere Aktionen	•
	RAS- und IAS-Server	Minimale Schlüsselgröße:	2048			
	Router (Offlineanfor	Auswählen der für Anforden.	ngen verwendbaren Kryptografie	anbieter		
	🚇 Smartcard-Anmeldu	Verwendung aller auf der	n Computer des Antragstellers ver	fügbaren		
	Renutzer Smartcard-Benutzer	Anbieter für Anforderung	en möglich			
	Stammzertifizierung	Für Anforderungen muss	einer der folgenden Anbieter verv	vendet		
	Ubergreifende Zertif	- werden:				
	Untergeordnete Zert	Anbieter:				
	Vertrauenslistensign	Microsoft Software Key S	torage Provider Provider	1		
	Websenies	Microsoft Smart Card Key	Storage Provider			
	Webserver					
	WS-ITS-Benutzer-V2					
	WS-ITS-Bitlocker	Anforderungshash:	SHA256	\sim		
	WS-ITS-CodeSignati		at vonvondon			
	WS-ITS-CodeSignati					
	Reference WS-ITS-Computer					
	Reference WS-ITS-Computer-V					
	🚇 WS-ITS-DomainCon					
	WS-ITS-DomainCon					
	WS-ITS-SmartCard	ОК	Abbrechen Ü <u>b</u> ernehme	en Hilfe		
< >	<			>		

Das Recht zur Editierung passe ich in der Sicherheit an. Hier kommt meine Admin-Gruppe wieder dazu:

Zertifikatvorlagenkonsole	- 🗆 X
Datei Aktion Ansicht ?	Financia da server Verland
	Eigenschaften der neuen vorlage
Retifikatvorlagen (WS-DC1.ws.i Vorlagenanzeigename	Schlüsselnachweis Antragstellemame Server
🗷 Kerberos-Authenti	Kompatibilitat Aligemein Antorderungsverarbeitung Kryptograne
Rey Recovery Age	tt Grunnen, oder Benitzemanen:
🚇 Nur Benutzersigna	u gopper o dei bei accentamen.
Reference - Signal -	a Schuleninizente benuzen OCSP-Antwortsignatur
OCSP-Antwortsign	a BLD-Admin-PKI (WS\LD-Admin-PKI) Weitere Aktionen
RAS- und IAS-Serv	er 🤐 Organisations-Admins (WS\Organisations-Admins)
Router (Offlinean	of WS-CA1 (WS-WS-CA1\$)
Smartcard-Anmei	
Stammzertifizierur	
Untergeordnete Zei	Hinzufügen Entfermen
2 Vertrauenslistensig	
🚇 Verzeichnis-E-Mail	Berechtigungen für "LD-Admin-PKI" Zulassen Verweigem
R Webserver	Vollzugriff
Representation with the second	Lesen 🗹 🗌
🗷 WS-ITS-Benutzer-	/2 Schreiben
🕮 WS-ITS-Bitlocker	Registrieren
Regional WS-ITS-CodeSignation	iti Automatisch registineren 🗹 🗌
WS-ITS-CodeSigna	tu
WS-ITS-Computer	Klicken Sie auf "Frweitet" um snezielle Berechtigungen
WS-ITS-Computer	anzuzeigen.
WS-ITS-DomainCo	
WS-ITS-DomainCo	
	OK Abbrechen Ubernehmen Hilfe
	>

Der Online Responder wird in einem Sicherheitskontext ausgeführt. Die dazugehörige Identität muss in der Lage sein, Zertifikate auf Basis der neuen Vorlage zu ziehen. Mein Online Responder wird im System-Kontext der Windows CA laufen. Also berechtige ich den Computer-Account für ein Enrollment:



Zertifikatvorlagenkonsole		- 0	×
Datei Aktion Ansicht ?			
← → □		Eigenschaften der neuen Vorlage	
🖳 Zertifikatvorlagen (WS-DC1.ws.i	Vorlagenanzeigename	Schlüsselnachweis Antragstellemame Server Kompathilität Alloemein Anforden nosverarbeitung Komtografie	
	🚇 Kerberos-Authentifiz	Ausstellungsvoraussetzungen Abgelöste Vorlagen Erweiterungen Sicherheit Zertifikatvorlagen (WS-DC1.ws.its)	-
	Key Recovery Agent Nur Benutzersignatu	Gruppen- oder Benutzemamen: Weitere Aktionen	۲
	Rur Exchange-Signa	Authentifizierte Benutzer OCSP-Antwortsignatur	•
	OCSP-Antwortsignal RAS- und IAS-Server	LD-Admin-PKI (WS\LD-Admin-PKI) Weitere Aktionen	►
	Router (Offlineanfor	WS_CA1 (WS_VUS_CA1e)	
	Real Smartcard-Anmeldu		
	Smartcard-Benutzer		
	🗷 Stammzertifizierung		
	🚇 Übergreifende Zertif		
	🚇 Untergeordnete Zert	Hinzufügen Entfernen	
	🖳 Vertrauenslistensign	Berechtigungen für "WS-CA1"	
	🚇 Verzeichnis-E-Mail-R	Zulassen Verweigem	
	Rebserver	Vollzugriff	
	Renutzer WS-ITS-Benutzer		
	WS-ITS-Benutzer-V2		
	WS-ITS-Bitlocker		
	WS-ITS-CodeSignati		
	WS-ITS-CodeSignati		
	WS-ITS-Computer	Klicken Sie auf "Erweitert" um spezielle Berechtigungen	
	WS-ITS-Computer-V	anzuzeigen.	
	WS-ITS-DomainCon		
	WS-ITS-DomainCon		
	We ITE SmartCard V	OK Abbrechen Ubernehmen Hilfe	
<	<	>	

Damit ist die Vorlage fertig. Nun nehme ich die Vorlage in die auszustellenden Vorlagen auf. Erst danach können passende Zertifikate angefragt werden:

🚋 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-Zertifizierungsstelle-CA1\Zertifikatvorlagen]							×
Datei Aktion Ansicht ?							
🗢 🔿 🙍 🖪 🗟 🔒							
Zertifizierungsstelle (Lokal)	Name			Beabsichtigter Zweck			
 WS-ITS-Zertifizierungsstelle-CA1 Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen 				In dieser Ansicht werden keine Elemente angezeigt.			
		Verwalten					
		Neu	>	Auszustellende Zertifikatvorlage			
		Aktualisieren					
		Ansicht	>				
	Sy	Symbole anordnen Am Raster ausrichten	>				
		Hilfe					

Eventuell wird die Vorlage nicht sofort angezeigt. Dann muss noch eine Domain Controller Replikation abgewartet werden. Bei mir hat der zeitliche Versatz ausgereicht:

🚡 certsrv - [Zertifizierungsstelle (Lokal)\WS-I		_	\times		
Datei Aktion Ansicht ?	Zertifikatvorlagen aktivieren	×			
	Wählen Sie eine Zertifikatvorlage aus, die für d Hinweis: Wird eine kürzlich erstellte Zertifikatvo waten, bis die Informationen zu dieser Vorlage Möglicherweise sind für die Zertifizerungsstelle Weitere Informationen finden Sie unter <u>Ko</u>	iese Zettfizierungsstelle aktiviert werden soll. rlage nicht in dieser Liste angezeigt, müssen Sie möglicherweise auf alle Domänencontroller repliziert wurden. nicht alle Zetfikavtorlagen Inter Organisation verfügbar. Inzepte für Zertifikatvorlagen.			
 Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen Zertifikatvorlagen 	Name WS-ITS-Computer-V2 WS-ITS-DomainController WS-ITS-DomainController-V2 WS-ITS-OmineReeponder-V1 WS-ITS-SmartCard WS-ITS-SmartCard WS-ITS-WPLLogin WS-ITS-WPLLogin WS-ITS-Webserver-OhneCRL WS-ITS-Webserver-V1 <	Beabsichtigter Zweck Clientauthentfizierung Serverauthentfizierung, Clientauthentfizierung KDC-Authentfizierung, Smartcard-Anmeldung, Serverauth OCSP-Signatur Smartcard-Anmeldung, Clientauthentfizierung Smartcard-Anmeldung, Clientauthentfizierung Serverauthentfizierung Serverauthentfizierung	~		



Weiter geht es mit dem Einrichten der Rolle. Die Rolleninstallation ist bereits abgeschlossen. Es fehlt noch das Post-Deployment. Dieses kann im Server Manager gestartet werden:

ᡖ Server-Manager		- 🗆 X
Server-N	1anager • Dashboard	🕶 🕝 🍢 Verwalten Tools Ansicht Hilfe
Dashboard	WILLKOMMEN BEI SERVER-MANAGER	Konfiguration nach der Bere AUFG V X
Alle Server Alle Server AD-Zertifikatdienste Datei-/Speicherdienste	1 Diesen lokalen S Schnellstart	Zertifikatdienste* auf "WS-CA1" erforderlich. Active Directory-Zertifikatdienste auf dem Zielserver Konfigurieren Aurgabendertails
Ko IIS	2 Rollen und Featur 3 Weitere zu verwa	res hinzulugen Iltende Server hinzulfügen
	Neuigkeiten 4 Servergruppe ers 5 Diesen Server mit	tellen t Cloud-Diensten verbinden
	Weitere	Ausblenden

Der Online Responder benötigt nur lokal administrative Rechte. Meine T1-Kennung ist Mitglied in den lokalen Admins:

AD CS-Konfiguration		- 0	ı x	
Anmeldeinformat	ionen	ZIEL WS-CA	SERVER A1.ws.its	
Anmeldeinformationen Rollendienste Bestätigung	Geben Sie Anmeldeinformationen zur Konfiguration de Rollendienste an.	r		
	Zum Installieren der folgenden Rollendienste müssen Sie der <mark>lokalen Administrate</mark> angehören: • Eigenständige Zertifizierungsstelle • Zertifizierungsstellen-Webregistrierung	orgruppe		
	 Unime-Kesponder Um die folgenden Rollendienste installieren zu können, müssen Sie der Gruppe d Unternehmensadministratoren angehören: Unternehmenszertifizierungsstelle verwenden Zertifikatregistrierungsrichtlinien-Webdienst Zertifikatregistrierungs-Webdienst Registrierungsdienst für Netzwerkgeräte 	er		
	Anmeldeinformationen: WS\stephan-T1 Ändern			
	< Zurück Weiter > Konfigurier	Abb	rechen	

Ich aktiviere nur den Online Responder. Die anderen Rollen kommen später dran:

AD CS-Konfiguration	an an an an an an	-		×
Rollendienste		w	ZIELSER	VER s.its
Anmeldeinformationen Rollendienste Bestätigung Status Ergebnisse	Wählen Sie die zu konfigurierenden Rollendienste aus. ✓ Zertifizierungsstelle ✓ Online-Responder Registrierungsdienst für Netzwerkgeräte Zertifikatregistrierungs-Webdienst Zertifikatregistrierungsrichtlinien-Webdienst			
	weitere informationen zu AD CS-Serverrollen			
	< Zurück Weiter > Konfiguriere	en	Abbrech	ien

Mehr ist hier nicht erforderlich:

WS IT-Solutions

AD CS-Konfiguration		··· ·· ··	- 🗆	×
Ergebnisse			ZIELSE WS-CA1.	RVER ws.its
	Die folgenden Rollen, Rollendienste oder Featur	es wurden konfiguriert:		
Bestatigung Status Ergebnisse	Online-Responder Weitere Informationen zur OCSP-Konfiguration	S Erfolgreiche Konfiguration		
	< Zurück	Weiter > Schließen	Abbre	chen

Der Online Responder hat eine eigene Management-Konsole. Hier muss ich nun noch die Sperrlisten zuweisen, die er bedienen soll:

🐏 ocsp - [Online-Respon	💱 ocsp - [Online-Responder: WS-CA1.ws.its\Sperrkonfiguration]					×
Datei Aktion Ansicht	?					
🗢 🔿 🖄 🗟 🛛						
Part Online-Responder: WS	-CA1.ws.its Name		Auswahl des Signaturzer	Registrierungsvorl	Aktionen	
Sperrkonfiguration Praykonfigura	Sperrkonfiguration hinzufügen	lieser Ansicht werden kein	e Elemente angezeigt.		Sperrkonfiguration	•
	Ansicht	>			Sperrkonfiguration hinzufügen	
	-				Ansicht	•
	Aktualisieren				Aktualisieren	
	Liste exportieren				📑 Liste exportieren	
	Hilfe				? Hilfe	

Jede Sperrliste wird durch einen Namen gekennzeichnet. Ich nehme hier den Namen meiner Zertifizierungsstelle:



🐏 ocsp - [Online-Responder: WS-	CA1.ws.its\Sperrkonfiguration]		
Datei Aktion Ansicht ?			
🗢 🔿 🙍 🗟 🛛			
Dolline-Responder: WS-CA1.ws.	Sperrkonfiguration hinzufügen	?	×
> 📬 Arraykonfiguration	Sperrkonfig	uration benennen	
	Erste Schritte beim Hinzu	Der Name der Sperrkonfiguration soll Ihnen die Identifikation dieser Sperrkonfiguration	
	Sperrkonfiguration benen	erleichtern. Es wird empföhlen, einen Namen zu verwenden, der auf die Zertifizierungsstelle für diese Sperrkonfiguration hinweist.	
	Pfad des Zertifizierungsst	Name: WS ITS Zotificierungsstelle CA1	1
	Zertifizierungsstellenzertif	W3-H3-Zettilizierungsstelle-CAI	
	Sperranbieter		
	openanolecci		
		< Zurück Weiter > Fertig stellen Abbrechen	

Im nächsten Schritt wird die dazugehörige Zertifizierungsstelle gesucht. Ich kann das durch meine AD-Integration einfach halten:



Der Auswahldialog zeigt meine interne Windows CA:



← ➡	s. Sperrkonfiguration hinzufügen			?
 Sperrkonfiguration Arraykonfiguration 	Zertifizieru	ngssteller	Zertifizierungsstelle auswählen Wählen Sie die Zertifizierungsstelle, die Sie verw	? X
	Erste Schritte beim Hinzu Sperrkonfiguration benen Pfad des Zertifizierungsst Zertifizierungsstellenzertif Signierendes Zertifikat au Sperranbieter	Um den S Zertifizien identifizie Sie könne veröffentli Zertifizien In Activ Zertifiz Anhan Zertifiz Zertifizien	Zertifizierungsstelle Comp WS-ITS-Zertifizierungsstelle-CA1 WS-C <	OK Abbrechen
			< Zurück Weiter >	Fertig stellen Abbrechen

Für diese CA und ihre Sperrliste muss ein Signaturzertifikat gewählt werden. Dieses wird sich mein Online Responder auf der neuen Zertifikatvorlage basierend automatisch ausstellen. Die Vorlage wurde bereits automatisch gefunden und zugewiesen:

🐏 ocsp - [Online-Responder: WS-	CA1.ws.its\Sperrkonfiguration]				
Datei Aktion Ansicht ?					
🗢 🄿 🖄 🗟 🛛					
 Online-Responder: WS-CA1.ws. Sperrkonfiguration P Arraykonfiguration 	Sperrkonfiguration hinzufügen	es Zertifikat auswählen		?	×
	Erste Schritte beim Hinzu Sperrkonfiguration benen Pfad des Zertifizierungsst Zertifizierungsstellenzertif Signierendes Zertifikat au Sperranbieter	Sperrinformationen werden Online-Responder kann aut manuell ein Signaturzertifika	signiert, bevor sie an einen Cliei omatisch ein Signaturzertifikat a at für jeden Online-Responder a ttisch auswählen DCSP-Signaturzertifikat registriei WS-CA1.ws.its/WS-ITS-Zertifiz WS-ITS-OnlineResponder-V1 II auswählen Bignaturzertifikat für jedes Mitgli ngeben. fikat für die Sperrkonfiguration	nt gesendet werden. Der nuswählen, oder Sie können uswählen. ren tierungsstelle-CA1 Durchsuchen verwenden	
		< Zur	ück Weiter > Fert	tig stellen Abbrechen	

Nach einem Kontakt zur Zertifizierungsstelle werden die möglichen Sperrlistenverteilungspunkte gelistet und zur Auswahl angeboten. Der Online Responder lädt sich die Listen selber herunter und prüft damit die Anfragen der Clients. Bei mir ist nur noch der neue Verteilungspunkt über http sichtbar. Das soll genügen. Aber die Aktualisisierungsfrequenz darf gerne wesentlich kleiner sein als als der Wert, der auf den Sperrlisten steht. So erhalte ich ein "Echtzeit-Sperrverhalten":
🐏 ocsp - [Online-Responder: WS-CA1.	ws.its\Sperrkonfiguration]		
Datei Aktion Ansicht ?			
🗢 🔿 🙍 🗟			
 Image: Specific control of the system of the	errkonfiguration hin: Sperranbietereigensc Dieser Sperranbieter b Zertifikatsperrlisten, di Identifizieren Sie die Sp ste Schritte beim Hi perrkonfiguration be fad des Zertifizierung ertifizierungsstellenz ignierendes Zertifikat perranbieter Deltasperrlisten: Hinzufügen Celtasperrlisten basierer Aktualisierungsinte	haften estimmt den Sperrstatus von Zertifikaten basie e von der Zertifizierungsstelle ausgestellt wurd eicherorte für die Zertifikatsperrlisten. //WS-TTS-Zertifizierungsstelle-CA1 Nach //WS-TTS-Zertifizierungsstelle-CA1 Nach	x ? X rend auf ien. , die en des Sperranbieters unten unten unten
		OK Abbre < Zurück Weiter >	echen Fertig stellen Abbrechen

Nach der Bestätigung organisiert sich der Online Responder ein OSCP-Signaturzertifikat und meldet seine Einsatzbereitschaft:

🐏 ocsp - [Online-Responder: WS-CA1	.ws.its]			-		×	
Datei Aktion Ansicht ?							
⇐ ➡ 👔							
Part Online-Responder: WS-CA1.ws.its	Coline Bernenderkenfiguration	^	Akt	ionen			
Sperrkonfiguration	Verwenden Sie dieses Spap-In zum Konfigurieren und Verwalten von Zertifikatsperrrespondern.		On	line-Responder: WS-C	A1.ws.its	•	
WS-CA1.ws.its			Respondereigenscha	ften			
	Übersicht		Responder neu zuweise				
Ubersicht Die Verwaltungs-Snap-Ins für den Online-Responder unterstützen Sie bei der Konfiguration und Verwaltung von OSCP-Respondern (Online Certificate Status-Protokoll) mit einer oder mehreren				Ansicht		•	
		^	Aktualisieren	Aktualisieren			
	Verwältung von USCP-Respondern (Unline Certificate Status-Protokoll) mit einer oder mehreren Zertifizierungsstellen.		?	Hilfe			
	Verwenden Sie dieses Tool für folgende Aufgaben: - Verwelten von Zertifikktsperrkonfigurationen für ein Online-Responderarray Übewachen des Ertiebestehtun inder Miteliede einer Online Responderarrau						
	Sperrkonfigurationsstatus	•					
	Im Statusbereich werden Online-Responderkonfigurationen angezeigt, die einwandfrei arbeiten oder vom Administrator überprüft werden müssen. Wählen Sie die Arraymitglieder aus, um weitere Informationen zu erhalten. Hinweis: Sie müssen ogf. auf "Aktualisieren" klicken, wenn kürzlich vorgenommene Konfigurationsänderungen oder andere administrative Aktionen hier nicht angezeigt werden. Weitere Informationen finden Sie im Thema zum Überprüfen der einwandfreien Funktion der Sperrkonfiguration. WS-ITS-Zettifizierungsstelle-C Wird ausgefüht A1						

Ein abschließender Blick im PKIVIEW zeigt nun alle Services fehlerfrei an:

🏥 pkiview - [Unternehmens-PKI/WS-ITS-Zertifizierungsstelle-CA1 (V2.2)] -							
Datei Aktion Ansicht ?							
🗢 🔿 🙍 🗟 📓							
🚔 Unternehmens-PKI	Name	Status	Ablaufdatum	Ort	Aktionen		
WS-ITS-Zertifizierungsstelle-CA1 (V2.2)	🙀 Zertifizierungsstellenzertifikat	OK	12.12.2025 15:37		WS-ITS-Ze 🔺		
	AIA-Speicherort #1	ОК	12.12.2025 15:37	http://ca.ws-its.de/certs/WS-ITS-Zertifizierungsstelle-CA1(2).crt	Weite ►		
	E Speicherort für Sperrlisten-Verteilungspunkte #1	OK	20.12.2020 04:09	http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2).crl			
	EltaCRL-Speicherort #1	OK	14.12.2020 04:09	http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2)+.crl			
	OCSP-Speicherort #1	OK		http://ca.ws-its.de/ocsp			

Einen realen Testlauf werde ich später ausführen.

Bereitstellung von CEPCES

Vorher möchte ich einen weiteren Service integrieren: CEPCES. Die Idee dahinter habe ich bereits in der Zielsetzung erklärt.

Für die Anfrage und die Ausstellung von Zertifikaten über https benötigt mein CEPCES ein Webserver-Zertifikat. Das alte Zertifikat habe ich im PKCS12-Format mit privatem Schlüssel auf meinem AdminShare liegen. Ich importiere das Zertifikat auf meinen neuen WS-CA1:

🖳 🏹 🔜 🛨	Extrahieren	20201125-0	075735 ws-ca1.ws.its.zip		
Datei Start Freigeben Ansicht	Tools für komprimierte Ordner				
← → × ↑ 🚺 « Freigaben (M:) > Ad	minArea > Services > Zertifikat	stelle > Cert	ReqTool > 20201125-075735 v	vs-ca1.ws.its.zip	~
20200126-132705 ws-pfs2.ws.it	^ Name		Тур	Komprimierte Größe	Kennwortg
20200512-181551 test.ws.its.zip	🙀 20201125-075735 ws-ca	1.ws.its.cer	Sicherheitszertifikat	2 KB	Nein
20200522-113348 drucker-1.ws	20201125-075735 ws-ca	1.ws.its.csr	CSR-Datei	2 KB	Nein
20200602-114718 laps-history.	20201125-075735 ws-ca	1.ws.its.inf	Setup-Informationen	1 KB	Nein
20200602-173200 wlan.ws.its.zi	p 20201125-075735 ws-ca	1.ws.its.key	KEY-Datei	6 KB	Nein
🔋 20200711-084348 .zip	20201125-075735 ws-ca	1.ws.its.pem	PEM-Datei	2 KB	Nein
🕌 20200712-170139 ws-gate1.ws.	20201125-0/5/35 ws-ca	1.ws.its.pfx	Privater Informationsaust	6 KB	Nein
📳 20200712-170702 ws-gate2.ws.	20201125-075735 ws-ca	i.ws.its.rsp	KSP-Datei	4 K.B	Nein
🔋 20200717-171436 gv.ws-its.de.:					
20200804-092040 testme.ws.its					
20201020-145315 testme.ws.its					
20201125-075735 ws-ca1.ws.its					
Vanfiguration					
	gewährleisten. Geben Sie das Kenr	wort für den	privaten Schlüssel ein.		
	Kennikora				
	••••••	•••••			
	Kennwort an:	zeigen			
	Importoptionen:				
	Hohe Sicherh aktivieren, w Anwendung Schlüssel als einem später Privaten Schl exportierbar	eit für den p erden Sie im verwendet w exportierbar en Zeitpunkt üssel mit virt) ten Eigensch	rivaten Schlüssel aktivieren. N mer dann, wenn der private S ird, zur Kennworteingabe auf markieren. Dadurch können S sichern bzw. überführen. ualisierungsbasierter Sicherhe aften mit einbeziehen	Wenn Sie diese Option ichlüssel von einer Tgefordert. Sie Ihre Schlüssel zu eit schützen (nicht	
			Γ	Weiter Abbr	echen

WS IT-Solutions

WSHowTo – Migration einer Windows PKI (WS-CA1) 2020-11-28 Migration auf Windows Server 2019

.	← 😺 Zertifikatimport-Assistent	×
20201125-075735 ws-ca1.ws.its.pfx	Fertigstellen des Assistenten	
	Das Zertifikat wird importiert, nachdem Sie auf "Fertig stellen" geklickt haben.	
	Sie haben folgende Einstellungen ausgewählt:	
	Gewählter Zertifikatspeicher Auswahl wird vom Assistenten automatisch festgelegt Inhalt PFX	
	Dateiname C:\Users\stephan-T1\Desktop\20201125-075735 ws-ca1.v	
	< >>	
	Fertig stellen Abbrechen	

Das Zertifikat binde ich nun im IIS-Manager an den Port 443 meiner Default Website:

🍓 Internetinformationsdienste (IIS)-Manager		– 🗆 X
← → Sites → WS-CA1 → Sites → Default Web	Site >	🔯 🗟 🏠 🔞 -
Datei Ansicht ?		
Verbindungen Image: Provide the state of the state o	ult Web Site Startseite → ♥ Start - _ Alle anzeigen Gruppieren nach: Bereich + _ + + + + + + + + + + + + + + + + +	Aktionen Im Explorer öffnen Berechtigungen bearbeiten
ASP.NET Anwendungspools Sites Sites Defar Sig C Manuella provident Sig C Manuella provident Sig C Manuella provident Sig C Manuella provident Sig C Manuella provident Sig C Manuella provident Sig Sig Sig Sig Sig Sig Sig Sig	ET-Senutzer .NET-Fehlerseiten .NET-Globalisierung .NET-Kompilierung .NET-Profil .NET-Rollen Image: Anbieter Anwendungseinst Computerschlüssel Seiten und Steuerelemente Sitzungszustand SMTP-E-Mail Image: Im	Site bearbeiten Bindungen Grundeinstellungen Anwendungen anzeigen Virtuelle Verzeichnisse anzeigen Website everwalten Starten Beenden Website durchsuchen Tribuiten fürstellungen Konfigurieren Ahlaufverfolgung für
Internetinformationsdienste (IIS)-Manager	Site >	Anfordenunodebler
Verbindungen Q. Defa Startseite V. W. VSCAI (WS)stephan-T1) W. W. Sites V. Sites V. W. Sites V. Sites V. W. Sites V. W. Sites V. S	Typ: IP-Adresse: Port: Intps Keine zugewiesen 443 Hostname: Hostname: Intp SNI (Server Name Indication) erforderlich Inn HTTP/2 deaktivieren OCSP Stapling deaktivieren E-Mail SSL-Zertifikat: Muswählen ws-ca1.ws.its Auswählen	Aktionen Im Explorer öffnen Berechtigungen bearbeiten Site bearbeiten Bindungen Grundeinstellungen Anwendungen anzeigen Virtuelle Verzeichnisse anzeigen Website verwalten Colorer Starten Benden Wirkein durchungen

Danach starte ich das Post-Deployment der Rolle im Server Manager. Die Rolleninstallation hatte ich ja bereits ausgeführt:



CEPCES wird im Active Directory in der Konfigurationspartition als Endpunkt registriert. Das kann nur ein Enterprise-Admin durchführen. Daher privilegiere ich meine T3-Kennung und wechsle den Sicherheitskontext im Assistenten:

📥 AD CS-Konfiguration	– 🗆 X
Anmeldeinformati	ONEN ZIELSERVER WS-CA1.ws.its
Anmeldeinformationen	Geben Sie Anmeldeinformationen zur Konfiguration der
Rollendienste Bestätigung	Rollendienste an.
Status Ergebnisse	Zum Installieren der folgenden Rollendienste müssen Sie der lokalen Administratorgruppe angehören:
	 Eigenständige Zertifizierungsstelle Zertifizierungsstellen-Webregistrierung Online-Responder
	Um die folgenden Rollendienste installieren zu können, müssen Sie der Gruppe der Unternehmensadministratoren angehören:
	Unternehmenszertifizierungsstelle verwenden Zertifikatregistrierungsrichtlinien-Webdienst Zertifikatregistrierungs-Webdienst Registrierungsdienst für Netzwerkgeräte
	Anmeldeinformationen: WS\stephan-T3 Ändern
	Weitere Informationen zu AD CS-Serverrollen
	< Zurück Weiter > Konfigurieren Abbrechen

Die Privilegierung übernimmt mein PAM-Script:

WS IT-Solutions

드 PAM-AdminGUI	- verbunden mit V	WS-DC1.ws.it	ts (Version V2.00)							-	×
Zeitraum: Ziel-DC:	5 Stunden	~		ZU		Die automatische AD-Replika	ition ist	aktiv.			
Security-Tiers:		Admins:			mögliche Gruppen:			aktive Mitgliedschaften:			
	x			x			x				x
alle Tier0 - DomainAdmini Tier1 - ServerAdminist Tier2 - ClientAdministr Tier3 - ServiceAdmin	stration tration ation	stephan-T3			Domänen-Admins GG-Admin-AD-GPO GG-Admin-AD-Join GG-Admin-ATA GG-Admin-Backup GG-Admin-Backup GG-Admin-Preigaben GG-Admin-Freigaben GG-Admin-HyperV GG-Admin-HyperV	275	~	Gültigkeit 2020-12-12 20:33:13 2020-12-12 20:33:13 2020-12-12 20:33:13	Gruppe GG-Admin-PKI GG-SEC-Server-Standard-Admins Organisations-Admins		

CEP und CES gehören hier zusammen. Daher starte ich das Post-Deployment gemeinsam:

WS IT-Solutions

ollendienste		Z WS	ZIELSER S-CA1.w	V
Anmeldeinformationen Rollendienste ZS für CES	Wählen Sie die zu konfigurierenden Rollendienste aus.			
Authentifizierungstyp für	Zertifizierungsstellen-Webregistrierung Vonline-Responder			
Authentifizierungstyp für	Registrierungsdienst für Netzwerkgeräte			
Bestätigung	 Zertifikatregistrierungsrichtlinien-Webdienst 			
	Weitere Informationen zu AD CS-Serverrollen			

Zuerst ist CES an der Reihe. CES muss mit einer Windows Zertifizierungsstelle "verheiratet" werden. Wird CES auf einem Zertifizierungsstellen-Server installiert, dann muss dieser gewählt werden. Ich hab es einfach, denn es gibt nur eine Windows CA:

📥 AD CS-Konfiguration	- 🗆 X
Zertifizierungsstel	e für CES ZIELSERVER WS-CA1.ws.its
Anmeldeinformationen Rollendienste ZS für CES	Geben Sie die Zertifizierungsstelle für die Zertifikatregistrierungs- Webdienste an.
Authentifizierungstyp für Dienstkonto für CES Authentifizierungstyp für Bestätigung Status Ergebnisse	Wählen Sie die Zertifizierungsstelle aus, die Zertifikate auf Anforderung dieses Zertifikatregistrierungs-Webdiensts ausstellen soll. Auswählen: © [ZS-Name Computername Zielzertifizierungsstelle: WS-CA1.ws.its\WS-ITS-Zertifizierungsstelle-CA1 Auswählen
	Ovraussetzung für den Nur-Erneuerungen-Modus ist, dass von der Zielzertifizierungsstelle mindestens Windows Server 2008 R2 ausgeführt wird. Weitere Informationen zur Zertifizierungsstelle für CES
	< Zurück Weiter > Konfigurieren Abbrechen

Clients und Benutzer sollen sich mit Kerberos am Webservice vom CES anmelden. So gibt's Sicherheit und Single-Sign-On:

WS IT-Solutions

Authentifizierung	istyp für CES	WS-CA1.ws
Anmeldeinformationen Rollondionsto	Wählen Sie den Authentifizierungstyp aus.	
ZS für CES	Integrierte Windows-Authentifizierung	
Authentifizierungstyp für	O Clientzertifikatauthentifizierung	
Authentifizierungstyp für Bestätigung Status Ergebnisse	O Benutzername und Kennwort	
	Weitere Informationen zum Authentifizierungstyp für CES	

CES selber läuft im einfachen Sicherheitskontext des Application Pools im IIS. Damit spare ich mir einige Anpassungen rund um das Thema SPN:

📥 AD CS-Konfiguration		_		×
Dienstkonto für C	ES	w	ZIELSER\ VS-CA1.ws	/ER s.its
Anmeldeinformationen Rollendienste ZS für CES Authentifizierungstyp für Dienstkonto für CES Authentifizierungstyp für Bestätigung Status	Geben Sie das Dienstkonto an. Wählen Sie die Identität aus, die der Zertifikatregistrierungs-Webdienst zur Ko der Zertifizierungsstelle und anderen Diensten im Netzwerk verwenden soll. O Dienstkonto angeben (empfohlen) Das ausgewählte Konto muss der Gruppe "IISIUSRS" angehören. Wenn Sie Authentifizierungstyp "Kerberos" ausgewählt haben, benötigt das Dienstko Dienstprinzipalnamen.	mmunik als onto eine	ation mit n uswählen	
	Integrierte Anwendungspoolidentität verwenden Weitere Informationen zum Dienstkonto für CES			
	< Zurück Weiter > Konfigu	rieren	Abbrech	en

Mehr braucht mein CES nicht. Nahtlos geht es mit CEP weiter. Hier muss ich die gleiche Authentifizierung wie beim CES wählen:

		_
Authentifizierung	ZIELSERVE WS-CA1.ws.it	
Anmeldeinformationen	Wählen Sie den Authentifizierungstyp aus.	
Rollendienste		
ZS für CES	Integrierte Windows-Authentifizierung	
Authentifizierungstyp für	O Clientzertifikatauthentifizierung	
Dienstkonto für CES	Reputzername und Kennwort	
Authentifizierungstyp für	O behazemane and kennikore	
Bestätigung		
	Weitere Informationen zum Authentifizierungstyp für CEP	

Dann ist alles angegeben. Der Assistent richtet beide Webservices ein:

WS IT-Solutions

📥 AD CS-Konfiguration		-		×
Bestätigung			ZIELSER	VER s.its
Anmeldeinformationen Rollendienste	Klicken Sie zum Konfigurieren d "Konfigurieren".	ler folgenden Rollen, Rollendienste oder Features au	f	
ZS für CES	Active Directory-Zertifika	atdienste		^
Authentifizierungstyp für	Zertifikatregistrierungs-Web	dienst		
Dienstkonto für CES	ZS-Name:	WS-CA1.ws.its\WS-ITS-Zertifizierungsstelle-CA1		
Authentifizierungstyp für	Nur-Erneuerungen-Modus:	False		
Bestätigung	Authentifizierungstyp:	Integrierte Windows-Authentifizierung		
Status	Schlüsselbasierte Erneuerung zulassen:	False		
	Konto:	Anwendungspoolidentität		
	Serverauthentifizierungszertifik at:	Bereits für SSL konfiguriert		
	Zertifikatregistrierungsrichtli	nien-Webdienst		
	Authentifizierungstyp:	Integrierte Windows-Authentifizierung		
	Schlüsselbasierte Erneuerung aktivieren:	False		
	Serverauthentifizierungszertifik at:	Bereits für SSL konfiguriert		~
		< Zurück Weiter > Konfigurieren	Abbrech	ien

VS IT-Solutions



Ich hatte bereits vorher einen CEPCES im Einsatz. Daher muss ich meine Clients und Benutzer nicht mehr neu informieren. Die bestehende Gruppenrichtlinie passt unverändert:



CEPCES benötigt aber noch einige Anpassungen im IIS, die nicht vom Post-Deployment vorgenommen werden. Also geht es in den IIS in die Webanwendung vom CEP. Hier brauche ich die Anwendungseinstellungen:

WS IT-Solutions

WSHowTo – Migration einer Windows PKI (WS-CA1) 2020-11-28 Migration auf Windows Server 2019



Das Feld Friendly Name darf nicht leer sein. Das ist aber leider der Default. Damit meine Gruppenrichtlinie weiter passt, trage ich den gleichen Text ein, den auch meine vorherige Zertifizierungsstelle verwendete:

📬 Internetinformationsdienste (IIS)-Manager				- 🗆 X
← → WS-CA1 → Sites → Default Web Site →	ADPolicyProvider_C	CEP_Kerberos >		🔯 🗟 🟠 🔞 -
Datei Ansicht ?				
Verbindungen	Mit diesem Feature werden.	ndungseinstellungen re können Sie Name-Wert-Paare speichern, die von Anwendungen mit verv	waltetem Code zur Laufzeit verwendet	Aktionen Hinzufügen Bearbeiten K Entfernen
✓ iii Sites	Gruppieren nach:	Keine Gruppierung 🔹		Hilfe
Original Web Site ADPolicyProvider CEP Kerberos	Name	Wert	Eintragstyp	
 Appendix integration appendix period in the second s	FriendlyName ID KeyBasedRenewa URI	(DB9320E4-A7EF-441A-A232-E0D3955ED1E9) Anwendungseinstellung bearbeiten ? X Name: FriendlyName Wert: WS IT-Solutions Zertifikatverteilung OK Abbrechen	Lokal Lokal Lokal Lokal Lokal	

Damit ist der CEPCES einsatzbereit.

Testphase

Bevor ich den Service testen kann, muss ich meiner Windows Zertifizierungsstelle noch weitere Zertifikatvorlagen zuweisen:

🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-Zertifizierungsstelle-CA1\Zertifikatvorlagen]					
Datei Aktion Ansicht ?					
🗢 🔿 🖻 🖉					
 Zertifizierungsstelle (Lokal) WS-ITS-Zertifizierungsstelle-CA1 Gesperte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehigeschlagene Anforderungen 	Name Beabsichtigter Zweck WS-ITS-OnlineResponder-V1 OCSP-Signatur				
	Verwalten				
	Neu Auszusteilende Zertifikatvorlage Aktualisieren Liste exportieren Ansicht > Symbole anordnen > Am Raster ausrichten + Hilfe +				

Für einen Testlauf nehme ich nur meine Webserver-Vorlage dazu. Diese kann kein AutoEnrollment und ich vermeide somit ungewollte Zertifikate, bevor meine Tests abgeschlossen sind:



Jetzt sind 2 Vorlagen aktiv:

WS IT-Solutions

🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-; Datei Aktion Ansicht ?	🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-Zertifizierungsstelle-CA1\Zertifikatvorlagen] Datei Aktion Ansicht ?					
🗢 🔿 🖄 🙆 🕞 👔						
 Zertifizierungsstelle (Lokal) WS-ITS-Zertifizierungsstelle-CA1 Gesperte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Fehlgeschlagene Anforderungen Zertifikatvorlagen 	Name WS-ITS-Webserver-V2 WS-ITS-OnlineResponder-V1	Beabsichtigter Zweck Serverauthentifizierung OCSP-Signatur				

Es wird Zeit für einen Testlauf. Ich starte eine certlm.msc und frage ein neues Zertifikat an:

ᡖ certlm - [Zertifikate - Lokaler Cor	mputer\	Eigene Zertifikate\Zertifikate]						-		×
Datei Aktion Ansicht ?										
🗢 🤿 🖄 📅 🛅 🙆 🔂	?									
Zertifikate - Lokaler Computer Eigene Zertifikate Zertifikate Zertifikate Yertrauenswürdige Stammzer Zwischenzertifizierungssteller	Ausge ଦ୍ୱୋWS ଦ୍ୱୋWS	estellt für ^ S-ITS-Zertifizierungsstelle-CA1 S-ITS-Zertifizierungsstelle-CA1 S-ITS-Zertifizierungsstelle-CA1	Ausg WS-I WS-I WS-I	estellt von TS-Zertifizierungsstelle-CA1 TS-Zertifizierungsstelle-CA1 TS-Zertifizierungsstelle-CA1	Ablaufdatum 12.12.2025 15.10.2021 16.08.2018	Beabsichtigte Zwec <alle> <alle> <alle></alle></alle></alle>	Anzeigename <keine> <keine> <keine></keine></keine></keine>	Status	Zertifil	atvorlag
> Vertrauenswürdige Herausgel Nicht vertrauenswürdige Zert		Alle Aufgaben	>	Neues Zertifikat anforde	ern					
 Drittanbieter-Stammzertifizie 		Aktualisieren		Importieren						
Vertrauenswürdige Personen Clientauthentifizierungsausst		Liste exportieren		Erweiterte Vorgänge	>					
Stammelemente der Vorabve		Ansicht	>							
Stämme testen Enderstein Enderst		S <u>y</u> mbole anordnen Am Rast <u>e</u> r ausrichten	>							
 Vertrauenswürdige Geräte Webhosting 		<u>H</u> ilfe								

Die Management-Konsole befragt das Active Directory, welche Zertifizierungsstellen existieren. Da wird dann mein CEP mit seiner URL genannt:

🚪 certlm - [Zertifikate - Lokaler Con	npute	er\Eigene Zertifikate\Zertifikate]				-			\times
Datei Aktion Ansicht ?									
	Aus 2 2 2 2 V 2 2 V	 Zertifikatregistrierung Zertifikatregistrierungsrichtlinie auswähl Mithilfe der Zertifikatregistrierungsrichtlinie können 2 Zertifikatvorlagen registriert werden. Die Zertifikatreg konfiguriert. Vom Administrator konfiguriert WS IT-Solutions Zertifikatverteilung Derichtenserbistriert befrigt 	Eigenschaften für Zertifikatregistrie Name: WS IT-Solutions Zertifikatverteilung Registrierungsrichtlinien-ID: (DB9320E4-A7EF-441A-A232-E0D) Registrierungsrichtlinienserver: Server-URI https://ws-ca1.ws.its/ADPolicyProvid	rrungs-Rich 3955ED1E9 Priorität Standard	tilinienserver Authentifizierungstyp Windows-integriert	×	S	Zertifika	tvorlag
Stämme testen Bemotedeskton		Von Ihnen konfiguriert							
Smartcard vertrauenswürdige ⁽¹⁾ Vertrauenswürdige Geräte ⁽²⁾ Webhosting		von millen konngunett	Registrierungskonfiguration		Entfemen				

Der CEP listet mir nun die möglichen Zertifikatvorlagen auf. Ich wähle das Template für ein Webserver-Zertifikat. Da muss ich eine Angabe zum Antragstellernahmen vornehmen. Ich erstelle ein Test-Zertikat:



Die Registrierung läuft und ist wenige Sekunden später abgeschlossen:

WS IT-Solutions

acertim - [Zertifikate - Lokaler Comp Datei Aktion Ansicht ? acertim - [Zertifikate - Lokaler Comp Datei Aktion Ansicht ? acertim - [Zertifikate - Lokaler Comp Datei Aktion Ansicht ? acertim - [Zertifikate - Lokaler Comp Aktion Ansicht Acertim - [Zertifikate - Lokaler Comp Aktion Ansicht Aktion Ansicht Acertim - [Zertifikate - Lokaler Comp Acertim - [Zertifikate - [Zertifikate - Lokaler Comp Acertim - [Zertifikate	puter\E	÷ 🐉 :	Zertifikatexport-Assistent		×			_		×
Zertifikate - Lokaler Computer	Ausges		Fertigstellen des Assist	enten		Zwec	Anzeigename	Status	Zertifikatv	/orlag
Zertifikate	🙀 test		· j			tifizier	<keine></keine>		WS-ITS-W	Vebse
Vertrauenswürdige Stammzer Organisationsvertrauen Zwischenzertifizierungssteller Vertrauenswürdige Herausgel Nicht vertrauenswürdige Zert Drittanbieter-Stammzertifizie Vertrauenswürdige Personen Clientauthentifizierungsausst Stämme testen Remdedesktop Smantcard vertrauenswürdige Vertrauenswürdige Geräte Webhosting Windows Live ID Token Issuer	도 WS- 일 WS- 일 WS-		Der Zertifikatexport-Assistent wurde Sie haben folgende Einstellungen au Dateiname Exportschlüssel Alle Zertifikate im Zertifizierungspf Dateiformat	erfolgreich abgeschlossen. sgewählt: C:\Users\stephan-T1\Desktop\test Nein Zertifikatexport-Assistent Der Exportvorgang wurde erfolgreich abgesch	OK	X	<keine> <keine> <keine> <keine></keine></keine></keine></keine>		WS-ITS-W	/ebse
				Fertig stellen Abbrech	hen					

Danach kontrolliere ich die CDP und AIA-Informationen, die beim Ausstellen von der Zertifizierungsstelle übergeben werden. Das neue Zertifikat ist nur noch über eine Sperrliste über http verifizierbar:

WS IT-Solutions

WSHowTo – Migration einer Windows PKI (WS-CA1) 2020-11-28 Migration auf Windows Server 2019

General Computer\Eigene Zertifikate - Lokaler Computer\Eigene Zertifikate - Lokaler Computer\Eigene Zertificate Datei Aktion Ansicht ? Image: Second Computer (Second Computer) Image: Second Computer) Image: Second Computer) <t< th=""><th>Zertifikat Allgemein Details Zertifizierungspfad</th><th>×</th><th></th><th></th><th>_</th><th></th></t<>	Zertifikat Allgemein Details Zertifizierungspfad	×			_	
Image: Standbox Ausgestellt für Image: Standbox Standbox Image: St	Feld Wert Zertifikatvorlageninformatio… Vorlage=WS-TTS-Webserver-V Erweiterte Schlüsselverwen… Serverauthentifizierung (1.3.6 Schlüsselkennung des Anta Stellenschlüsselvermatikatrichtil Schlüsselkennung des Anta Schlüsselkennung des Anta Schlüsselkennung Schlüssel. Spernisten-Verteilungspunkte Schlüsselverwendungsrichten Verteilungspunkt Schlüsselverwendung Schlüsselverwendung Schlüsselverwendung<td></td><td>eabsichtigte Zwec erverauthentifizier arverauthentifizier Alle> Alle> Alle></td><td>Anzeigename <keine> <keine> <keine> <keine></keine></keine></keine></keine></td><td>Status</td><td>Zertifikatvorlag WS-ITS-Webse WS-ITS-Webse</td>		eabsichtigte Zwec erverauthentifizier arverauthentifizier Alle> Alle> Alle>	Anzeigename <keine> <keine> <keine> <keine></keine></keine></keine></keine>	Status	Zertifikatvorlag WS-ITS-Webse WS-ITS-Webse
	0	к				

In den Stelleninformationen finde ich 2 Einträge: einer zeigt, wo ein Client das Zertifizierungsstellen-Zertifikat organisieren kann. Und der andere Link gibt die Position meines Online-Responders an:

🧧 certlm - [Zertifikate - Lokaler Computer\Eigene Zertif	💂 Zertifikat	× ×
Image: Certim - [Zertifikate - Lokaler Computer\Eigene Zertifi Datei Aktion Ansicht ? Image: Certifikate Image: Certifikate Image: Certifikate Image: Certifikate <td>Allgemein Details Zertifizierungspfad Anzeigen: <alle> Feld QZertifikatvorlageninformatio Vorlage=WS-TTS-Webserver-V GErweiterte Schlüsselverwen Serverauthentifizierung (1.3.6</alle></td> <td>eabsichtigte Zwec Anzeigename Status Zertifikatvorlag erverauthentifizier «Keine> WS-ITS-Websr erverauthentifizier «Keine> WS-ITS-Websr Alle> Keine> WS-ITS-Websr</td>	Allgemein Details Zertifizierungspfad Anzeigen: <alle> Feld QZertifikatvorlageninformatio Vorlage=WS-TTS-Webserver-V GErweiterte Schlüsselverwen Serverauthentifizierung (1.3.6</alle>	eabsichtigte Zwec Anzeigename Status Zertifikatvorlag erverauthentifizier «Keine> WS-ITS-Websr erverauthentifizier «Keine> WS-ITS-Websr Alle> Keine> WS-ITS-Websr
 Organisationsvertrauen Zwischenzertifizierungssteller Vertrauenswürdige Herausgel Nicht vertrauenswürdige Zersonen Drittanbieter-Stammzertifizierungsausst Stammelemente der Vorabve Stämme testen Remotedesktop 	Anwendungsrichtlinien [1]Anwendungsrechtikatrichti Schlüsselkennung Schlüssel-D=Sflüezelstein Schlüssel-D=Sflüezelstein Schlüsselkennung Sperristen-Verteilungspunkte [1]Sperristen-Verteilungspunk Sperristen-Verteilungspunkte [1]Stelleninformation=zugriff Schlüsselverwend und Diotale Sinaatur, Schlüsselelen Alternativer Name: URL=http://ca.ws-its.de/certs/WS-TTS-Zertifizierungsstelle- (2)Stelleninformation=zugriff Zugriffsmethode=Onlinestatusprotokol des Zertifikats (1 2 5 4 5 7 2 4 9)	Alle> <keine> Alle> <keine></keine></keine>
 Smartcard vertrauenswürdige Vertrauenswürdige Geräte Webhosting Windows Live ID Token Issuei 	Alternätiver Name: URL=http://ca.ws-its.de/ocsp Eigenschaften bearbeiten In Datei kopieren	

Die Ausstellung über CEPCES funktioniert also. Ebenso werden die Erweiterungsinformationen korrekt ausgegeben. Dann bleibt nun noch die Kontrolle des Online-Responders. Diese Funktion kann mit certutil grafisch verprobt werden. Dazu exportiere ich das eben ausgestellte Test-Zertifikat in eine cer-Datei und rufe certutil mit dem Parameter URL auf. In der grafischen Oberfläche kann ich nun die einzelnen Stelleninformationen und Sperrlistenoptionen prüfen. Ich beginne mit dem Download des Zertifizierungsstellen-Zertifikates. Das funktioniert wie erwartet:



test.cer		
🖾 C:\Windows\system32\cmd.exe - certutil -url test.cer	_	×
C:\Users\stephan-T1\Desktop>certutil -url test.cer		Ê
URL-Abrufprogramm X		
Status Typ URL Abrufzeit Fingerabdruck Überprüft Zertifikat (0) [0.0] http://ca.ws-its.de/certs/WS-IT 0 ff2e97adff6		
Zeitlimit (Sek.) 15 Hinweis: Heruntergeladene Sperifister und Zertfikate werden nur bis zu einem gewissen Maß überprüft: Die Sperifiste bzw. das LDAP-Verkehr signieren Zertfikat ist möglicherweise nicht ördnungsgemäß signiert oder verfügt nicht übergemäß signiert oder verfügt nicht		
Zertfikatantragstel ordnungsgemäße Überprüfung. test Auswählen Beenden Abrufen		
UKL fur Download		

Auch der Download der klassischen Sperrlisten über http funktioniert einwandfrei:

test.cer		
C:\Windows\system32\cmd.exe - certutil -url test.cer	-	× ^
URL-Abrufprogramm X Status Typ URL Abrufzeit Fingerabdruck Überprüft Basissperfis [0.0] http://ca.ws-its.de/crt/WS-ITS 0 e88e0a5a3 Überprüft Deltasperfis [0.0.0] http://ca.ws-its.de/crt/WS-ITS 0 3f6765d72b		
Zettlimit (Sek.) 15 Hinweis: Heruntergeladene Sperilisten und Zenffikate werden nur bis zu einem gewissen Maß überprüft. Die Speriliste bzw. dass Aburfen LDAP-Verkehr signieren Zentfikati st möglichenweise nicht ordnungsgemäß signiert oder verfügt nicht über entsprechende Erweiterungen für eine ordnungsgemäße Überprüfung. Aburfen C Zentfikate (vom AIA) Zettfikatantragstel Auswählen Beenden C OCSP (von AIA) URL für Download		

Und auch der Online Responder reagiert wie gewünscht:



test.cer					
C:\Windows\system32\cmd.exe - certutil -url test.cer			_	-	×
C:\Users\stephan-T1\Desktop>certutil -ur	rl test.cer				Â
URL-Abrufprogramm			×		
Status Typ Überprüft OCSP	URL [0.0] http://ca.ws-its.de/ocsp	Abrufzeit Fingerabi 0 67242b8	druck 7d		
Zeitlimit (Sek.) 15 LDAP-Verkehr signieren	Hinweis: Heruntergeladene Sperilisten und Zertfikate werden nur bis zu einem gewisse Maß überprüft. Die Speriliste bzw. das Zertfikat ist möglicherweise nicht ordnungsgemäß signiert oder verfügt nicht über entsprechende Erweiterungen für eine ordnurgemäße Überprüftung.	Abrufen C Zertifikate (vom A C Sperfisten (vom C C OCSP (von AIA)	IA) DP)		
Zertifikatantragstel lest URL für Download	Auswählen	Abrufen			

Aber ich möchte auch das "Echtzeit"-Sperrverhalten testen. Daher sperre ich in der Zertifizierungsstelle das Test-Zertifikat:

🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS-IT	S-Zertifizierungsstelle-(CA1\Ausgestellte Zertifi	kate]				-		×
Datei Aktion Ansicht ?									
🗢 🔿 🖄 🖬 🖬 🔛									
Zertifizierungsstelle (Lokal)	Anforderungs-ID	Antragstellername	Ausgestellt: Allge	meiner Name	Zertifikat	vorlage	Anfang	sdatum	n des ^
VS-ITS-Zertifizierungsstelle-CA1	886	WS\WS-CA1\$	test		WS-ITS-	Webserver-V2 (1.3.6.1.4.1.311.21.8.1	12.12.20	20 16:2	29
Gesperite Zertifikate	E 885	WS\WS-CA1\$	WS-CA1.ws.i	Öffnen		OnlineResponder-V1 (1.3.6.1.4.1.311	12.12.20	20 16:0)9
Ausgesteine Zertinkate	1 884	WS\WS-CA1\$	WS-ITS-Zerti WS-ITS-Zerti	Alle Aufgaben	>	Attribute/Erweiterungen anzeige	n	5:3 5:2	32 27
Fehlgeschlagene Anforderungen Zertifikatvorlagen	882	WS\WS-CA1\$	WS-ITS-Zerti	Aktualisieren		Binärdaten exportieren		5:2	27
	l 🔄 880	WS\WS-CA1\$	WS-ITS-Zerti	Hilfe		Zertifikat sperren		8:0	J5
	🔄 879 WS\W	WS\WS-CA1\$ WS-IT	WS-ITS-Zerti			fende Zertifizierungsstelle (CrossCA)	15.10.20	10 18:0	J5
1	877	WS\stephan-T1	Walther, Stephan	- T1	WS-ITS-E	Benutzer-V2 (1.3.6.1.4.1.311.21.8.135	04.12.20	20 07:1	10

Üblicherweise wird hierfür eine Begründung mit angegeben:

🚡 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-	Zertifizierungsstelle-C	A1\Ausgestellte Zertifik	ate]		- 🗆 ×
Datei Aktion Ansicht ?					
🗢 🔿 🖄 🖬 🖬 🖬					
Zertifizierungsstelle (Lokal)	Anforderungs-ID	Antragstellername	Ausgestellt: Allgemeiner Name	Zertifikatvorlage	Anfangsdatum des ^
VS-ITS-Zertifizierungsstelle-CA1	886	WS\WS-CA1\$	test	WS-ITS-Webserver-V2 (1.3.6.1.4.1.311.21.8.1	12.12.2020 16:29
Gesperrte Zertifikate	la 885	Zertifikatsperrung	×	WS-ITS-OnlineResponder-V1 (1.3.6.1.4.1.311	12.12.2020 16:09
Ausgestellte Zertifikate	584	Sind Sie sicher, dass Sie die ausgewählten Zertifikate sperren möchten?		Zertifizierungsstellenaustausch (CAExchange)	12.12.2020 15:32
Schlasschlagens Anforderungen	583			Übergreifende Zertifizierungsstelle (CrossCA)	12.12.2020 15:27
Zertifikatvorlagen	582			Übergreifende Zertifizierungsstelle (CrossCA)	12.12.2020 15:27
Zeninkatvonagen	I 880	Geben Sie einen Grund	, ein Datum und eine Uhrzeit an.	Übergreifende Zertifizierungsstelle (CrossCA)	15.10.2016 18:05
	579	Grund:		Übergreifende Zertifizierungsstelle (CrossCA)	15.10.2016 18:05
	577	Abgelost	~	WS-ITS-Benutzer-V2 (1.3.6.1.4.1.311.21.8.135	04.12.2020 07:10
	576	Datum und Uhrzeit:		WS-ITS-Benutzer-V2 (1.3.6.1.4.1.311.21.8.135	29.11.2020 10:31
	1 875	12.12.2020	16:44	Zertifizierungsstellenaustausch (CAExchange)	28.11.2020 09:29
	874			WS-ITS-Benutzer-V2 (1.3.6.1.4.1.311.21.8.135	28.11.2020 09:22
	873		Ja Nein	WS-ITS-Computer-V2 (1.3.6.1.4.1.311.21.8.13	25.11.2020 14:08
	872			WS-ITS-Computer-V2 (1.3.6.1.4.1.311.21.8.13	25.11.2020 12:53

Nach dieser Aktion muss die Sperrliste außerhalb ihrer automatischen Veröffentlichung manuell erstellt werden. Das geht mit der cmd recht schnell:

WS IT-Solutions



Beim Einsatz eines Online Responders hängt es nun vom Aktualisierungsinterval ab. Ich hatte 5 Minuten angegeben. Die könnte ich nun noch abwarten. Aber ich kann es mit der Management Konsole auch beschleunigen:

😰 ocsp - [Online-Respond	er: WS-CA1.ws.its]					_		×
Datei Aktion Ansicht	?							
♦ ♦								
🗐 Online-Responder: WS-C	A1.ws.its	ation	^	Aktio	nen			
Sperrkonfiguration	Verwenden Sie dieses Snap-In zum K	onfigurieren und Verwalten von Zertifikatsperrrespondern.		Onlin	e-Responder	: WS-C	A1.ws.its	•
WS-CA1.ws.it	Arraymitglied hinzufügen	5	Respondereigenschaften			iften		
	Sperrdaten aktualisieren			Responder neu zuweisen				
	Mitglieder mit Arraycontroller synchronisieren		•	A	nsicht			•
	Aktualisieren	Responder unterstützen Sie bei der Konfiguration und Certificate Status-Protokoll) mit einer oder mehreren	^	Q A	ktualisieren			
	Hilfe	forshen:		🛛 🛛 Hilfe				
	- Verwalten von Zertifikatsnerrkonfigurat	ionen für ein Online-Resnonderarrav						

Ein Sperrlistentest mit certutil zeigt, dass die klassische Sperrlistenfunktion das Zertifikat noch nicht als zurückgezogen deklariert, denn mein Client hat sich beim ersten Test die Datei über http heruntergeladen und die Datei im Cache ist noch gültig. Er wird sich also die neue Version noch nicht herunterladen:

test.	er	
C:\Windows\system32\cmd.exe - certutil -url tes C:\Users\stephan-T1\Desktop>certutil URL-Abrufprogramm Status Typ Oberprüft Basissp Oberprüft Deltaspr	.cer -url test.cer URL Abrufzeit Fingerabdruck rilis [0.0] http://ca.ws-its.de/crl/WS-ITS 0 07465c5b07 rilis [0.0.0] http://ca.ws-its.de/crl/WS-ITS 0 2c7c5a7d77	×
Zeitlimit (Sek.) 15 LDAP-Verkehr sign Zertfikatantragstel test URL für Download	Hinweis: Heruntergeladene Speriisten und Zertfikate werden nur bis zu einem gewissen Maß überprüft. Die Speriiste bzw. das ordnungsgemäß signiet oder verfügt nicht über entsprechende Erweiterungen für eine ordnungsgemäße Überprüfung. Abrufen Auswählen Beenden	~

Aber der Online Responder hat diese neue Sperrliste bereits verarbeitet und reagiert dementsprechend mit einem Sperrhinweis. Damit ist diese Sperrfunktion wesentlich schneller und agiler als die Verwendung der klassischen Sperrlisten:



	test.cer					
C:\Windows\system32\cmd.exe	- certutil -url test.cer				 -	
C:\Users\stephan-T1\Deskt	top>certutil -ur L-Abrufprogramm	l test.cer		×		
S G	tatus Typ espent OCSP	URL [0.0] http://ca.ws-its.de/ocsp	Abrufzeit 0	Fingerabdruck fe2502ca44		
Zei Zei Zei Zei tes	tlimit (Sek.) 15 LDAP-Verkehr signieren ertifikatantragstel st	Hinweis: Heruntergeladene Spertisten und Zertifikate werden nur bis zu einem gewisse Maß überprüft. Die Spertiste bzw. das Zertifikat ist möglicherweise nicht ordnungsgemäß signiert oder verfügt für eine ordnungsgemäße Überprüfung. Auswählen	Abrufen — C Zertifik C Sperfis OCSP	ate (vom AIA) sten (vom CDP) (von AIA)		~
UR	RL für Download					

Meine Zertifizierungsstelle hat alle Tests bestanden. Es kann also mit der Aktivierung der Standardfunktionen weiter gehen.

Aktivierung der PKI

Meine Computer und Benutzer werden über Gruppenrichtlinien angewiesen, die PKI regelmäßig zu besuchen, um dort nach Zertifikatvorlagen mit Auto Enrollment zu suchen. Solange meine Zertifizierungsstelle also keine passenden auszustellende Vorlagen hat, passiert nichts. Das kann ich nach meinen erfolgreichen Tests nun ändern. Ich nehme weitere Vorlagen zur Ausstellung dazu:

🙀 certsrv - [Zertifizierungsstelle (Lokal)\WS-ITS-	Zertifizierun	gsstelle-CA1\Zertifikatvorlagen]		-	×						
Datei Aktion Ansicht ?												
🗢 🔿 🙇 🙆 📑 👔												
✓ Jertifizierungsstelle (Lokal) ✓ Jews-ITS-Zertifizierungsstelle-CA1 Gesperte Zertifikate Ausgestellte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderungen	Name WS-ITS WS-ITS	-Webserver-V2 -OnlineResponder-V1	Beab Serve OCS	sichtigter Zweck erauthentifizierung P-Signatur								
Zertifikatvorlagen		Verwalten										
1								Neu	>	Auszustellende Zertifikatvorlage		
		Aktualisieren Liste exportieren										
		Ansicht	>									
		Symbole anordnen Am Raster ausrichten	>									
		Hilfe										

Mein Vorlagenkatalog ist recht überschaubar:

📮 certsrv - [Zertifizierungsstelle (Lokal)\\	VS-ITS-Zertifizierungsstelle-CA1\Zertifika	tvorlagen]		-	×
Datei Aktion Ansicht ?					
🗢 🔿 🙇 🙆 🛃					
Zertifizierungsstelle (Lokal) V 🛃 WS-ITS-Zertifizierungsstelle-CA1	Zertifikatvorlagen aktivieren		×		
 Gesperrte Zertifikate Ausgestellte Zertifikate Ausstehende Anforderungen Fehlgeschlagene Anforderunge Zertifikatvorlagen 	Wählen Sie eine Zertfikatvorlage aus, die Hinweis: Wird eine kürzlich erstellte Zertfik warten, bis die Informationen zu dieser Vor Möglicherweise sind für die Zertfizierungss Weitere Informationen finden Sie unte	für diese Zertifizierungsstelle aktiviert werden soll. atvorlage nicht in dieser Liste angezeigt, müssen Sie möglicherweise age auf alle Domänencontroller reoliziert wurden. telle nicht alle Zertifikatvorlagen Ihrer Organisation verfügbar. r <u>Konzepte für Zertifikatvorlagen</u> .			
	Name	Beabsichtigter Zweck	^		
	WS-ITS-Benutzer-V2	Clientauthentifizierung			
	R WS-ITS-Bitlocker	BitLocker Network Unlock			
	R WS-ITS-CodeSignatur	Codesignatur			
	WS-ITS-CodeSignatur-V2	Codesignatur			
	R WS-ITS-Computer	Serverauthentifizierung, Clientauthentifizierung			
	WS-ITS-Computer-V2	Clientauthentifizierung			
	Regional WS-ITS-DomainController	Serverauthentifizierung, Clientauthentifizierung			
	WS-ITS-DomainController-V2	KDC-Authentifizierung, Smartcard-Anmeldung, Serverauth			
	R WS-ITS-SmartCard	Smartcard-Anmeldung, Clientauthentifizierung	~		
	<				

Damit kann meine PKI ihre Arbeit aufnehmen.

Nacharbeiten

NS IT-Solutions

Konfiguration der Datensicherung

Es folgen die üblichen Standardarbeiten. Eine wichtige ist die Konfiguration der Datensicherung. Die Zertifizierungsstelle werde ich wieder mit der Windows Serversicherung sichern. Dafür registriere ich wieder meine Standardaufgabe in der Aufgabenplanung:

🕑 Aufgabenplanung						– 🗆 X
Datei Aktion Ansicht	?					
🗢 🔿 🖄 🖬 🛽 🗖						
Aufgabenplanung (Lok	al) Name Status Tri	gger				Aktionen
> 🛃 Aufgabenplanu	Einfache Aufgabe erstellen	Tag um 00:20 Uhr				Aufgabenplanungsbibliothek 🔺
	Aufgabe erstellen	Systemstart - Nach Auslösu	ung alle 10 Minuten fü	r die Dauer von 1 Stunde w	viederholen.	Einfache Aufgabe erstellen
	Aufgabe importieren					🐌 Aufgabe erstellen
	Alle aktiven Aufgaben anzeigen					Aufgabe importieren
	Verlauf für alle Aufgaben deaktivieren					Alle aktiven Aufgaben anzeigen
	Neuer Ordner					Verlauf für alle Aufgaben deaktivieren
	Ansicht	>				Meuer Ordner
	Aktualisieren				>	Ansicht •
	Aktobiliseten	ungen Einstellungen Ver	rlauf			Aktualisieren
	Hilfe	Jp			^	Hilfe
	Sneicherort:					-
Aufgabenplanung						- 🗆 ×
🕑 Öffnen					×	
$\leftarrow \rightarrow \checkmark \land \square $	Dieser PC > Freigaben (M:) > AdminArea	> Services > DPM > BMR	 ✓ ⁽²⁾ "B! 	/R" durchsuchen	Q	
				_		Aktionen
Organisieren 🔻 Ne	euer Ordner					Aufgabenplanungsbibliothek 🔺
Netzwerk	^ Name	Änderungsdatum	Тур	Größe	n.	Einfache Aufgabe erstellen
Services	SProgramm	09.06.2020 07:24	Verknüpfung	2 KB		🐌 Aufgabe erstellen
Active Dire	ServerSicherung.xml	11.08.2019 14:33	XML-Dokument	4 KB		Aufgabe importieren
ADFS						Alle aktiven Aufgaben anzeigen
Azure						👔 Verlauf für alle Aufgaben deaktivieren
BMR						Meuer Ordner
DHCP					>	Ansicht •
DNS						Aktualisieren
DPM					~	Hilfe
Agent-In						

Der Account ist wieder nur als Dummy eingetragen:



Aufgabenplanung		- 🗆 X
Datei Aktion Ansicht ?		
🗢 🔿 🔁 🖬 🖬 🖬		
Aufgabenplanung (Lokal) Name	1	nen
> Aufgabenplanungsbibliot B PSTranscript-	() Aufgabe erstellen X	abenplanungsbibliothek 🔺
🕒 Restart-NLA	Allgemein Trigger Aktionen Bedingungen Einstellungen	Einfache Aufgabe erstellen
	Name: ServerSicherung	Aufgabe erstellen
	Speicherort	Aufgabe importieren
	Autor: WS\stephan-ad	Alle aktiven Aufgaben anzeigen
	Beschreibung:	Verlauf für alle Aufgaben deaktivieren
		Neuer Ordner
		Ansicht 🕨
Allgemein Trig		Aktualisieren
Name:	Sicherheitsoptionen	Hilfe
Speicherort:	Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden:	ewähltes Element
Autor:	WS\stephan-T3 Benutzer oder Gruppe ändern	Ausführen
Beschreibung:	 Nur ausführen, wenn der Benutzer angemeldet ist 	Beenden
	Unabhängig von der Benutzeranmeldung ausführen	Deaktivieren
	Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu.	Exportieren
	Mit höchsten Privilegien ausführen	Eigenschaften
Sicherheitsopt	Ausgeblendet Konfigurieren für: Windows® 7, Windows Server''' 2008 R2	Löschen
Beim Ausführ		Hilfe
NT-AUTORIT	OK Abbrechen	

Über mein gMSA-Script kann ich nun vom Domain Controller aus den Sicherungsaccount durch einen Group Managed Service Account ersetzen:

🛥 gMSA-Admin			—	\times
vorhandene gMSA:	zugehörige Ser	ver:	zugehörige Gruppen:	
gMSA-Backup (Task User für BMR) gMSA-Monitor (Task User für Monitoring) gMSA-SQLDPM (Service SQL auf WS-f erstelle gMSA lösche gMSA Einsatz als: Task	WS-DC1.ws.its WS-PS1.ws.its WS-FS1.ws.its WS-FX1.ws.its WS-CA1.ws.its WS-MX1.ws.its WS-MX2.ws.its WS-MX2.ws.its WS-PD2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DPM.ws.its WS-MX4.cws.its WS-MX4.cws.its WS-MX4.cws.its WS-MX1.ws.its WS-MX1.ws.its WS-MX1.ws.its WS-MX1.ws.its WS-MX1.ws.its WS-MX1.ws.its WS-HY1.ws.its WS-HY1.ws.its WS-HY1.ws.its WS-HY2.ws.it WS-HY2.ws.it WS-HY2.ws.it WS-HY2.ws.it WS-HY2.ws.its WS-	(online) ts ts ts ts Erfolg X Der Task wurde umgestellt!	direkte Gruppen: GG-SEC-Server-Montoring-Admins GG-SEC-Server-Standard-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-MX-Admins GG-SEC-Server-HyperV-Admins GG-Admin-Backup GG-SEC-Server-File-Admins Sicherungs-Operatoren indirekte Gruppen (durch Verschachtelung): LD-Admin-Backup LD-AD-AdminArea-R LD-SEC-Clients-JB-ADP LD-SEC-Clients-JB-ADP LD-SEC-Clients-JB-ADP LD-SEC-Clients-JB-ADP LD-SEC-Clients-JB-AMINS LD-SEC-Clients-JB-Admins SC-Server-HyperV-VWnRM LD-SEC-Server-HyperV-Vogin LD-SEC-Server-HyperV-Admins SA weitere Gruppe entferne Gruppe	~
Server	TaskName	Account	Pfad	^
WS-CA1	PSTranscript-CleanUp	NT-AUTORITÄT\SYSTEM	N	
WS-CA1	Restart-NLA	NT-AUTORITÄT\SYSTEM	N	
WS-CA1	ServerSicherung	ws\gMSA-Backup\$	N	
WS-CA1	Server Initial Configuration Task	NT-AUTORITÄT\SYSTEM	\Microsoft\Windows\	
WS-CA1	.NET Framework NGEN v4.0.30319	NT-AUTORITÄT\SYSTEM	\Microsoft\Windows\.NET Framework\	
WS-CA1	.NET Framework NGEN v4.0.30319 64	NT-AUTORITÄT\SYSTEM	\Microsoft\Windows\.NET Framework\	
WS-CA1	.NET Framework NGEN v4.0.30319 6	NT-AUTORITÄT\SYSTEM	\Microsoft\Windows\.NET Framework\	
WS-CA1	.NET Framework NGEN v4.0.30319 C	NT-AUTORITÄT\SYSTEM	\Microsoft\Windows\.NET Framework\	\checkmark
lese alle Server setze gMSA ein bereit]		·	

Damit ist alles erledigt. Die Sicherungsdefinition liegt ja zentral in meiner Konfiguratiosdatei. Das genügt mir.

Monitoring

Weiter geht es mit dem Monitoring. Die aktuellen Sensoren zeigen meinen Base-Sensor im Fehlerstatus. Das liegt am Fehlen der alten Systemfestplatte, die über ihre GUID referenziert wurde. Ich lösche diesen alten Sensor im Webportal:

WS IT-Solutions

WSHowTo – Migration einer Windows PKI (WS-CA1) 2020-11-28 Migration auf Windows Server 2019

08	Startseite	Geräte E	Bibliotheken	Sensoren	Alarme	Maps 8	Berichte Pro	otokoll Tickets	s Konfiguration	
#	Geräte WS-ITS	Server 💌 🕅	WS-CA1 🔻							
(Gerät <mark>WS-C</mark>	A1 P ***								
	🔿 Übersi	icht 2	Tage	30 Tage	365 Tage	A Alarn	ne 🛛 Sy	ysteminformationen	Protokoll	🌣 Einstellungen
	Wenn S	ie hier Sensortacho	s sehen möchter	n, ändern Sie die Priori	ität von einem	oder mehreren Senso	oren zu 🗯	****		
	Pos. 🗸	Sensor 🗢				Status 🗢	Nachricht			Graph
	Pos. ▼	Sensor 🗢	1	Sensormen	ü	Status 🗢 Fehler (Bestätiat)	Nachricht	1.12.2020 21:27:50 (UTC)	von Stephan bis 12.12.2020 2	Graph сяџ , р,56 %
	Pos. ▼ ⊕ 1. ⊕ 2.	Sensor 🗘 Base WS-CA		Sensormen Jetzt abfragen Details	ü	Status 🌩 Fehler (Bestätigt) OK	Nachricht [[Bestätigt um 1 PKI Services are	1.12.2020 21:27:50 (UTC) running	von Stephan bis 12.12.2020 2	Graph CRU 0.56 % Services PKI 7#
	Pos. ▼	Sensor Sensor Services PKI		Sensormen 9 Jetzt abfragen 1 Details 9 Bearbeiten • Alarm bestätigen	ŭ >	Status 🖗 Fehler (Bestätigt) OK	Nachricht [[Bestätigt um 1 PKI Services are	1.12.2020 21:27:50 (UTC) running	von Stephan bis 12.12.2020 2	Graph
	Pos. ▼	Sensor Sensor Services PKI		Sensormen 5 Jetzt abfragen 2 Details 8 Bearbeiten 4 Alarm bestätigen 1 Löschen 4 Klonen	ŭ 	Status 🗢 Fehler (Bestätigt) OK	Nachricht [Bestätigt um 1 PKI Services are << < 1 bis 2 von 2 >	1.12.2020 21:27:50 (UTC) running	von Stephan bis 12.12.2020 2	Graph CRU 556 % Services PKI 7 #

Danach kann ich ihn neu erstellen. Der Sensor ist ein eigens programmierter. Er gehört nicht zum Standard vom PRTG:

🔿 Startseite	Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	Protokoll	Tickets	Konfiguration	Neue Protokolleinträ
Geräte WS-ITS	S 💌 Server	 WS-CA1 Sen 	sor hinzufügen (Sch	hritt 2 von 2)						
	Sensor	ninzufügen z	um Gerät WS	S-CA1 Iws-c	a1 ws its]					
					u					
	< Abbrech	en								
	Allaen	neine Sensor	einstellunger	1						
					N	lame des Sensors	Base WS-CA1			
					Üb	ergeordnete Tags	0			
						Tags	• xmlexesenso	r 🗙 🖸		
						Priorität	0 ★★★☆☆			
	Senso	reinstellunge	n				Die ausfü Das Arbe Arbeitsve	hrbare Datei w itsverzeichnis rzeichnisse ve	vird auf dem Rechner ausgeführt, auf dem die übergeordnete Probe installiert ist, nicht auf für EXE-Dateien ist das Verzeichnis der Probevbs-, .ps1- oder andere Skriptdateien können rwenden.	lem übergeordneten G andere
						Programm/Skript	WSSensor-Se	erverBaseline.	ps1	
						Parameter	• "WS-CA1"			
						Umgebung	Standardu	imgebung		
							O Platzhalte	r als Umgebur	ngsvariablen verwenden	
					s	Sicherheitskontext	Icherheit	skontext des I	PRTG Probe-Dienstes verwenden	
							O Die Zugan	gsdaten für W	findows des übergeordneten Geräts verwenden	
						Name des Mutex	0			

Nach wenigen Sekunden sind die Counter im Sensor geladen:

0	Startseite	e Geräte	Bibliotheken	Sensoren	Alarme	Maps	Berichte	Protokoll	Tickets	Konfiguration	
*	Geräte	WS-ITS 🔻 Serv	er 🔻 WS-CA1 🔻	Base WS-CA1 🔻							
~	Sensor ок	Base WS-CA	\1 ^P ★★★☆☆								
	0	Übersicht	(••) Livedaten	2 Tage	3	30 Tage	365 Tage	🖿 Hist	orische Daten	Protokoll	🌣 Einstellungen
	CPU			Backup-Alter	· '	NIC Ethernet empfangen	NIC Etherne	et senden	RAM frei	RAM Seitenfehler	Vol. System frei
				-1 h		0 MB/s	o ∓ 0 MB/s	0.1	43 %	16,02 f/s	89%
				Vol. System lesen		Vol. System schreiben	Vol. System	n Warteschlange			
		- \	/ 🗸	0 kB/s	0.1	0 kB/s	0#	0.1			
	1,71 %	0	% 99,75 %	<u>+ +</u>							

<u>Updates</u>

Im WSUS verschiebe ich den neuen Server noch in den passenden Update-Container. Den Rest erledigen meine Gruppenrichtlinien:



📷 Update Services					- 🗆 X	
📷 Datei Aktion Ansicht Fenster	?				- 8	×
🗢 🔿 🙍 📊 🛿 🗊						
🃷 Update Services	Update-Sofort (9 Computers vo	n 9 angezeigt, 29 insgesamt)			
✓ im WS-CM > im Updates	Status: Alle	🝷 📿 Aktualisieren				
🗸 💱 Computer	i) Name	IP-Adresse	Betriebssystem	Prozentsatz "Installiert/N	Letzter Statusbericht	^
V Nicht and Computer	\Lambda ws-ca1.ws.its	192.168.100.6	Windows Server 2019 Datac	99%	12.12.2020 14:37	
Clients	▲ ws-dc2.ws.its	192.168.100.2	Windows Server 2019 Datac	99%	12.12.2020 13:04	
V Server	▲ ws-fs1.ws.its	192.168.100.11	Windows Server 2019 Datac	99%	12.12.2020 16:10	
💕 Update-Sofort	▲ ws-hv1.ws.its	192.168.100.9	Windows Server 2019 Datac	99%	12.12.2020 16:24	
💱 Update-Verzoeger	\Lambda ws-mm	192.168.110.104	Windows Server 2019 Datac	99%	12.12.2020 14:50	
Downstreamserver	\Lambda ws-mx1.ws.its	192.168.100.3	Windows Server 2019 Datac	99%	12.12.2020 16:30	
Berichte	▲ ws-print1.ws.its	192.168.100.14	Windows Server 2019 Datac	99%	12.12.2020 14:31	
Dptionen	\Lambda ws-rds2.ws.its	192.168.110.21	Windows Server 2016 Datac	99%	12.12.2020 14:18	
	ws-ca1.ws.its					•
< >>	Status Updates mit Fehler Erforderliche Upda Installierte/nicht zu Updates ohne Stat	m: 0 tes: 1 trreffende Updates: 704 us: 0	Gruppenmitgliedschaft: All Betriebssystem: Wii Betriebssystemsprache: de- Service Pack: Kei IP-Adresse: 192	e Computer, Update-Sofort ndows Server 2019 Datacenter DE ne 1.168.100.6		<
	,					

Bereinigungen

Im Hyper-V steht noch der alte VM-Eintrag. Diese VM kann ich nun löschen:

Image: Hyper-V-Manager Datei Aktion Ansicht ? Image: Hyper-V-Manager ? <							
Hyper-V-Manager WS-HV1.WS.ITS WS-HV2.WS.ITS WS-HV3.WS.ITS	Virtuelle Computer Name WS-ACAD	Phase Wird ausgeführt	CPU-Auslast 0 %	Zugewiesener Spei 2048 MB	Betriebszeit 7.05:15:43	Status	Konfiguratio 8.0
	WS-CA1-at WS-CL6 WS-CL8 WS-DC2 WS-DPM WS-FS2 WS-MON	Verbinden Verbinden Einstellungen. Konfiguration Starten	0 % sversion upgrade	2008 MB	4.04:07:47 23.13:38:04 24.13:45:59 23.10:46:18 18.12:39:01 16.12:36:41 4.08:34:37		9.0 8.0 9.0 9.0 9.0 9.0 9.0 8.0
	WS-WX2 WS-PFS1b WS-RDS2 WS-Reuer-alt WS-WAC	Prüfpunkt Verschieben Exportieren Umbenennen. Löschen Replikation ak Hilfe	 tivieren		18.12:46:28 41.04:02:23 24.12:55:41 24.12:29:01		9.0 8.0 8.0 9.0

Die dazugehörige Festplattendatei muss manuell bereinigt werden:

Verwatten WS-CA1 Date: Statt Freigeben Ansicht Datenträgerimagetools Image: Statt Freigeben Anderungsdatum Typ Größe Virtual Hard Disks 28.11.2020 10:17 Dateiordner Virtual Hard Disks 28.11.2020 08:19 Festplatten-Image 27.889.664 Image: Virtual Hard Disks 28.11.2020 08:19 Freigaben (M:) Image: Virtual Hard Disks Im									
Date Start Freigeben Ansicht Datenträgerimagetools ← →	_ 🖉 _ =	Verw	valten	WS-	-CA1				
← → · ↑ ▲ > Dieser PC → Tier-Silver (W:) → Hyper-V → WS-CA1 * Schnellzugriff Name ^ Anderungsdatum Typ Größe Desktop Virtual Hard Disks 28.11.2020 10:17 Dateiordner Walther, Stephan - T1 Wirtual Hard Disks 08.12.2020 08:19 Festplatten-Image 27.889.664 Dieser PC *: System (C:) DATEN (D:) Freigaben (M:) Tier-Gold (V:) Tier-Silver (W:) Base	Datei Start Freigeben Ansicht Dat	enträge	rimagetools						
Image Anderungsdatum Typ Größe □ Desktop ↓ Vitual Hard Disk 28.11.2020 10:17 Dateiordner ▲ Walther, Stephan - T1 → 08.12.2020 08:19 Festplatten-Image 27.889.664 ■ HDD0.vhdx 08.12.2020 08:19 Festplatten-Image 27.889.664 ■ HDD0.vhdx 08.12.2020 08:19 Festplatten-Image 27.889.664 ■ HDD0.vhdx 08.12.2020 08:19 Festplatten-Image 27.889.664 ■ Dieser PC ● Freigabe ● ● ■ DATEN (D:) ● Senden an > > ■ Tier-Gold (V:) Ausschneiden × > > ■ Base Verknüpfung erstellen > WS-CL6 Umbenennen Eigenschaften > ■ Tier-Bronze (X:) ● ● Eigenschaften > >	\leftarrow \rightarrow \checkmark \uparrow \blacksquare \rightarrow Dieser PC \rightarrow Tier-Silver (W:) > Hy	yper-V > WS-0	CA1					
■ Desktop Virtual Hard Disks 28.11.2020 10:17 Dateiordner ■ HDD0.vhdx 08.12.2020 08:19 Festplatten-Image 27.889.664 ■ Dieser PC ● Bereitstellen ● ● ■ DATEN (D:) ● Freigabe ● Øffnen mit Vorgängerversionen wiederherstellen ● ■ Tier-Gold (V:) ● Base ✓ Ausschneiden ● ● ■ Hyper-V ● Verknüpfung erstellen ● </td <th>📌 Schnellzugriff</th> <td>Na</td> <td>ame</td> <td></td> <td>^</td> <td>Änderungsdatum</td> <td>Тур</td> <td>0</td> <td>Größe</td>	📌 Schnellzugriff	Na	ame		^	Änderungsdatum	Тур	0	Größe
Image: Big black	Deskton		Virtual Hard D	lisks		28.11.2020 10:17	Dat	teiordner	
Wather, Stephan - 11	Welling Charles T1	-	HDD0.vhdx			08.12.2020 08:19	Fes	tplatten-Image	27.889.664
□ Dieser PC IP Freigabe ○ System (C:) Offnen mit □ DATEN (D:) Vorgängerversionen wiederherstellen ○ Freigabe (M:) Senden an □ Tier-Gold (V:) Ausschneiden □ Base Kopieren □ Hyper-V Uerknüpfung erstellen □ WS-CL6 Umbenennen □ Tier-Bronze (X:) Eigenschaften	waitner, stepnan - 11				Bereitstellen				
System (C:) Öffnen mit DATEN (D:) Vorgängerversionen wiederherstellen Freigaben (M:) Senden an Tier-Gold (V:) Ausschneiden Base Kopieren Hyper-V Verknüpfung erstellen WS-CL6 Umbenennen Tier-Bronze (X:) Eigenschaften	Uieser PC			È	Freigabe				
DATEN (D:) Vorgängerversionen wiederherstellen Freigaben (M:) Senden an Tier-Gold (V:) Ausschneiden Base Kopieren Hyper-V Verknüpfung erstellen WS-CA1 Umbenennen WS-CL6 Eigenschaften	🏪 System (C:)				Öffnen mit				
 Freigaben (M:) Tier-Gold (V:) Tier-Silver (W:) Base Hyper-V WS-CA1 WS-CL6 Tier-Bronze (X:) Eigenschaften 	DATEN (D:)				Vorgängerversionen wie	derherstellen			
Tier-Gold (V:) Ausschneiden Tier-Silver (W:) Ausschneiden Base Kopieren Hyper-V Verknüpfung erstellen WS-CL6 Umbenennen Tier-Bronze (X:) Eigenschaften	🛖 Freigaben (M:)				Senden an		>		
Tier-Silver (W:) Ausschneiden Base Kopieren Hyper-V Verknüpfung erstellen WS-CA1 Löschen WS-CL6 Umbenennen Tier-Bronze (X:) Eigenschaften	Tier-Gold (V:)				Schuch un		_		
Base Kopieren Hyper-V Verknüpfung erstellen WS-CA1 Löschen WS-CL6 Umbenennen Tier-Bronze (X:) Eigenschaften	Tier-Silver (W:)				Ausschneiden				
Hyper-V Verknüpfung erstellen WS-CA1 Löschen WS-CL6 Umbenennen Tier-Bronze (X:) Eigenschaften	Base				Kopieren				
Löschen WS-CL6 Tier-Bronze (X:) Löschen Umbenennen Eigenschaften	Hyper-V				Verknüpfung erstellen				
WS-CL6 Umbenennen Tier-Bronze (X:) Eigenschaften	WS-CA1	1 - E			Löschen				
Tier-Bronze (X:)					Umbenennen				
	Tim Brown (V)				Eigenschaften		_		
				_	-]	

Problem Smartcard Logon

Ich verwende auf einem System eine Smartcard für die Anmeldung. Weil ich heute zufällig vor Ort bin, tausche ich das Zertifikat gleich manuell aus. Aber nach dem Austausch hängt die Anmeldung mit der neuen Smartcard mit dieser Fehlermeldung:



Da hat etwas bei der Neuausstellung des Zertifizierungsstellen-Zertifikates nicht geklappt. Für eine Smartcard-Anmeldung muss der Domain Controller dem Aussteller des Smartcard-Zertifikates vertrauen. Das ist üblicherweise vollautomatisch und wird unsichtbar im Hintergrund konfiguriert. Ich nutze aber ein angepasstes Administrationsmodell. Und bei dem hatte ich ja auch schon Probleme bei der CRL-Veröffentlichung im Active Directory. Offenbar wurde hier noch etwas im AD vergessen...

Ich führe das Problem also auf mein administratives Tier-Management zurück, in dem ich eben nicht alles als Domain Admin oder Enterprise Admin durchführe.

Aber ich kenne die notwendigen Schritte: Meine Domain Controller müssen das neue Zertifizierungsstellen-Zertifikat als NTAuth-Zertifikat konfiguriert bekommen. Um das zu konfigurieren, berechtige ich meinen T3-Admin als PKI-Admin und als Enterprise Admin:

🛥 PAM-AdminG	UI - verbunden mit	WS-DC1.ws.it	s (Version V2.00)						
Zeitraum: Ziel-DC:	1 Stunde	~		Z		Die automatische AD-Replikation	n ist a	ıktiv.	
Security-Tiers:		Admins:			mögliche Gruppen:			aktive Mitgliedschaften:	
	x			x			x		
alle Tier0 - DomainAdm Tier1 - ServerAdmin Tier2 - ClientAdmini Tier3 - ServiceAdm	inistration histration stration in	stephan-T3			GG-Admin-AD-GPO GG-Admin-ATA GG-Admin-ATA GG-Admin-Backup GG-Admin-DHCP GG-Admin-DHCP GG-Admin-HVperV- GG-Admin-HVperV- GG-Admin-HVperV-SC GG-Admin-LAPS-Slerv GG-Admin-MX-Storano GG-Admin-MX-Storano	rage ts er	^	Gültigkeit 2020-12-15 20:31:09 2020-12-15 20:31:09 2020-12-15 20:31:09 2020-12-15 20:31:09 2020-12-15 21:05:28	Gruppe Domänen-Admins GG-Admin-PKI Organisations-Admins GG-SEC-Server-Standard-Admins

Mit diesen Rechten ausgestattet starte ich eine PKIVIEW-Konsole. Hier kann man nicht nur die PKI überprüfen, sondern auch Anpassungen im AD-Kontext vornehmen:

🔿 🔿 🖄	▶ ?				
Unternehmen	Vorlagen verwalten		Status	Ablaufdatum	Ort
🙀 WS-ITS-Ze	AD-Container verwalten	ellenzertifikat	ОК	12.12.2025 15:37	
	Ontionen	#1	ОК	12.12.2025 15:37	http://ca.ws-its.de/certs/WS-ITS-Zertifizierungsstelle-CA1(2).crt
	optionen	perrlisten	ОК	20.12.2020 04:56	http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2).crl
	Aktualisieren	erort #1	ОК	17.12.2020 04:56	http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2)+.crl
	Hilfe	rt #1	ОК		http://ca.ws-its.de/ocsp

Für eine Smartcard-Anmeldung werden vertrauenswürdige NTAuthCertificates verwendet. Und genau hier liegt das Problem: Das neue Zertifizierungsstellen-Zertifikat fehlt in der Auflistung! Gelistet ist nur das alte:

🚔 pkiview - [Unternehmens-PKI\WS-IT	S-Zertifizierungsstelle-CA1 (V2.2)]			
Datei Aktion Ansicht ?				
Unternehmens-PKI	Name Zertifizierungsstellenzertifikat AIA-Speicherort #1 Speicherort für Sperlisten DeltaCRL-Speicherort #1 OCSP-Speicherort #1 AD-Container verwalte Zertifizierungsstell NTAuthCertificates Name SWS-ITS-Zertifizien	Status OK OK OK OK encontainer AIA-Contain	Ablaufdatum 12.12.2025 15:37 12.12.2025 15:37 20.12.2020 04:56 17.12.2020 04:56 Registrierum er CDP-Containe	Ort http://ca.ws-its.de/certs/WS-ITS-Zertifizierungsstelle-CA1(2).crt http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2).crl http://ca.ws-its.de/crl/WS-ITS-Zertifizierungsstelle-CA1(2)+.crl http://ca.ws-its.de/ocsp
			Zertifikat Allgemein Details Z Zertifika Dieses Zertifika Alle ausge Alle Anwern	X tertifizierungspfad tisinformationen at ist für folgende Zwecke beabsichtigt: gebenen Richtlinien ndungsrichtlinien
	Hinzufügen	intfermen	Ausgestell Ausgestell Gültig a <mark>b</mark>	It für: WS-ITS-Zertifizierungsstelle-CA1 It von: WS-ITS-Zertifizierungsstelle-CA1 15, 10, 2016 bis 15, 10, 2021 Zertifikat installieren Ausstellererklärung
< >				OK

Über den Schalter "Hinzufügen" kann ich nun das neue Zertifikat zuweisen:



Entfemen

Ausgestellt von: WS-ITS-Zertifizierungsstelle-CA1

Zertifikat installieren...

OK

Gültig ab 12, 12, 2020 bis 12, 12, 2025

Hinzufügen.

Dennoch wird die Anmeldung mit einer Smartcard erst funktionieren, wenn der prüfende Domain Controller über diese Veränderung informiert wurde. Denn jeder DC wird in seiner Registry die Zertifikate cachen. Bei mir ist es einfach, denn der Client mit der Smardcard steht in meiner Außenstelle und dort gibt es nur einen Domain Controller. In der Registry finde ich nur einen Zertifikateintrag für das alte Zertifizierungsstellen-Zertifikat:





Mit einem simplen gpupdate kann ich den Domain Controller dazu bringen, die Daten neu zu laden. Das hat nichts mit Gruppenrichtlinien zu tun. Aber der erzwungene Kontakt zu einem Domain Controller aktualisiert eben auch diese Daten. Und auch Domain Controller verhalten sich hier eben wie alle anderen Server und Clients. Nach dem gpupdate wird auch das neue Zertifikat lokal gelistet:



Nachdem der Domain Controller das neue Zertifizierungsstellen-Zertifikat gespeichert hat, akzeptiert er auch die Smartcard-Anmeldung vom Client:





Damit wäre auch dieses Problem behoben.

Problem Snort

Das nächste Problem lässt nicht lange auf sich warten. Mein Advanced Threat Analytics (ATA) meldet mir per Mail, dass es meinen WS-DC3 nicht mehr erreichen kann. Das sieht erst einmal nicht nach einem zertifikatbasierten Problem aus:



Aber direkt danach erhalte ich eine weitere Mail von meinem Monitor-Server. Dort läuft ein PowerShell-Script, dass die Logfiles im dort installierten SYSLOG analysiert. Im SYSLOG protokolliert meine Firewall und mein IPS diverse Meldungen. Und eine davon zeigt meinen WS-DC3:

neue IF	S-Alerts										
count	TotalCount	SourceIP	DestinationIP	SourcePort	DestPort	FirstSeen	LastSeen	Classification	AlertMessages	SourceName	DestinationName
2	4	167.248.133.24, 167.248.133.37	172.19.120.120	56194, 61407	443	11:43:06	11:43:06	Misc Attack	ET DROP Dshield Block Listed Source group 1	scanner- 08.ch1.censys- scanner.com	HAProxy.dmz.ws.i
1	3	192.168.101.1	192.168.100.6	64854	80	11:53:58	11:53:58	Unknown Traffic	(http_inspect) INVALID CONTENT- LENGTH OR CHUNK SIZE	WS-DC3.ws.its	WS-CA1.ws.its

Das sehe ich mir im IPS genauer an. Mein IPS ist ein Snort, dass in meiner PFSense mitläuft und den erlaubten Traffic regelbasiert analysiert und ggf. die Verbindungen blockiert. Da mein WS-DC3 in meinem Außenstandort läuft und daher



über ein VPN angebunden ist, muss die Kommunikation durch den "äußeren Filter". Hier sind die blockierten Hosts sichtbar. Das sind alles System im Außenstandort:

	ENSE System	▼ Interfaces ▼ Firewall ▼	Services -	VPN -	Status 👻	Diagnostics 👻	Help -			۵
Ser	rvices / Snort	/ Blocked Hosts								0
Sno	rt Interfaces Glo	oal Settings Updates Alert	s Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Blo	cked Hosts and L	og View Settings								
	Blocked Hosts	L Download All blocked hosts will be saved			All blo	c <mark>lear</mark> ocked hosts will b	e removed			
R	efresh and Log View	Save Save auto-refresh and view setting:	⊠ Ref s Defaul	f resh It is ON		500 Numbe Default	r of blocked ent is 500	ries to view.	•	
Las #	t 500 Hosts Block	ced by Snort Alert Descriptions and Event T	ïmes						Remove	
1	192.168.101.1 Q	(http_inspect) INVALID CONTE ET CHAT MSN status change	ENT-LENGTH OR CH 2020-12-08 21:50	HUNK SIZE 20):18	020-12-17 11:53	3:57			×	
2	192.168.101.2 Q	(http_inspect) INVALID CONTE	ENT-LENGTH OR C	HUNK SIZE 20	020-12-17 12:03	3:48			×	
3	192.168.101.3 Q	(http_inspect) INVALID CONTE (http_inspect) UNKNOWN ME ET CHAT MSN status change	ENT-LENGTH OR CH THOD – 2020-11-2 – 2020-11-23 03:09	HUNK SIZE 20 1 07:30:01 9:27	020-12-17 12:0	5:11			×	
		3 h	ost IP addresses a	re currently beir	ng blocked by S	Snort.				

In den Alerts kann ich die Ursache finden. Es war eine Kommunikation zwischen den blockierten Hosts und meiner neuen Zertifizierungsstelle. Besonders interessant ist dabei der Port 80:

		System -	Interfac	ces 👻 🛛 Fire	ewall -	Services 🕶	VPN -	Status	▪ Di	agnostics -	Help 🗸			•
Servic	es/	Snort /	Alerts											0
Snort Int	erfaces	Glob	al Settings	Updates	Alerts	Blocked	Pass L	.ists Su	ppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Alert Lo	og Viev	w Settin	gs											
Inter	rface to I	nspect	DMZ_120_ Choose inte	_EXTERN (h <mark>~</mark> rface	Auto	o-refresh view	р А	250 Alert lines to d	lisplay.	🖺 Sav	re			
AI	ert Log /	Actions	📩 Downloa	d <u>ញ</u> Clear										
Alert Lo	og Viev	w Filter												•
Last 25	50 Aler	t Log En	tries											
Date	Pri	Proto	Class		Source IP	SPc	ort Dest	ination IP	DPort	SID	Description			
2020-12-1 12:05:11	73	TCP	Unknown	Traffic	192.168. Q 🕀 🗴	101.3 52: •	202 192 Q	.168.100.6 ⊕	80	120:8 🕀 🗙	(http_inspect CHUNK SIZE) INVALID CONTE	NT-LENGTH	OR
2020-12-1 12:03:48	73	TCP	Unknown	Traffic	192.168. Q 🕀 🛪	101.2 64	825 192 Q	.168.100.6 ⊕	80	120:8 🕀 🗙	(http_inspect CHUNK SIZE) INVALID CONTE	NT-LENGTH	OR
2020-12-1 11:53:57	73	TCP	Unknown	Traffic	192.168. Q 🕀 🛪	101.1 64	854 192 Q	168.100.6 ⊕	80	120:8 🕀 🗙	(http_inspect CHUNK SIZE) INVALID CONTE	NT-LENGTH	OR

Auf diesem Port läuft mein neuer OCSP. Ebenso kann hier aber auch der Sperrlisten-Download drüber laufen! Anscheinend werden die Verbindungen falsch bewertet. Daher erstelle ich eine neue Ausnahme:

	e. ^{on}	System -	Interfaces 🕶	Firewall + Servic	es 🕶 👌	/PN + Status	i • Di	agnostics -	Help -			0
Service	s/	Snort /	Alerts								()	8
Snort Inter	faces	Globa	l Settings Update	es Alerts Blo	cked	Pass Lists S	uppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
Alert Log	j Viev	v Setting	S									
Interfa	ice to li	nspect	DMZ_120_EXTERN (Choose interface	h Auto-refres	h view	250 Alert lines to	display.	🖹 S	ave			
Aler	t Log A	ctions	📩 Download 📋 Cle	ar								
Alert Log	y Viev	v Filter									(D
Last 250	Alert	t Log Ent	ries									
Date	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	SID	Description			
2020-12-17 12:05:11	3	TCP	Unknown Traffic	192.168.101.3 Q 🕀 🗙	52202	192.168.100.6 Q 🕀	80	120:8 🕀 🗶	(http_inspect) CHUNK SIZE	INVALID CONTE	NT-LENGTH O	R
2020-12-17	3	TCP	Unknown Traffic	192.168.101.2	64825	192. Add this al	ert to the Sup	press List and tr	ack by_dst IP pect)	INVALID CONTE	NT-LENGTH O	R
12:03:48				Q 🕀 🗙		Q 🕀		± ×	CHUNK SIZE			
2020-12-17 11:53:57	3	TCP	Unknown Traffic	192.168.101.1 Q 🕀 🗙	64854	192.168.100.6 Q ⊞	80	120:8 🕀 🗶	(http_inspect) CHUNK SIZE	INVALID CONTE	NT-LENGTH O	R

Danach entferne ich noch die geblockten Hosts und die Verbindungen funktionieren wieder. An diesem Live-Beispiel kann man sehen, wie ein aktives und intelligentes Monitoring beim Lösen von Problemen helfen kann.

<u>Zusammenfassung</u>

VS IT-Solutions

Auch diese Migration verlief nicht ohne Probleme. Einige wären vermeidbar gewesen. Dennoch ist jede Problemlösung ein Lieferant für wertvolles Wissen.

Nachdem dieser Server nun mit meinem Ziel-Betriebssystem läuft, bereite ich mich auf den nächsten vor. Viele sind ja nicht mehr über...