

Zertifikatssperrliste(n) in Active Directory veröffentlichen



# Zertifikatssperrliste(n) in Active Directory veröffentlichen

#### Inhalt

Zertifikatssperrliste(n) in Active Directory veröffentlichen	2
Erweiterung in der Zertifizierungsstelle konfigurieren	3
DNS Host Eintrag konfigurieren	4
Managed Service Account im AD anlegen	5
Virtuelles Verzeichnis im IIS konfigurieren	5
Zertifikatssperrliste veröffentlichen	8
Zertifikatssperrliste im Browser überprüfen	9

1

# Zertifikatssperrliste(n) in Active Directory veröffentlichen

Hier in diesen Howto möchte ich euch zeigen, wie man die Zertifikatssperrliste(n) in Active Directory veröffentlicht. Das ganze wurde wieder in einer Virtuellen Umgebung mit Oracle - VirtualBox nachgestellt.

Die erste Frage die sich stellt ist was ist eigentliche eine Zertifikatssperrliste?

- Eine Zertifikatsperrliste (certificate revocation list, CRL) ist eine Liste, die die Ungültigkeit von Zertifikaten beschreibt. Sie ermöglicht es, festzustellen, ob ein Zertifikat gesperrt oder widerrufen wurde und warum.
- Zertifikate werden gesperrt oder widerrufen, wenn deren zugehöriger Schlüssel z. B. nicht mehr sicher ist, weil sie in die falsche Hände geraten sind oder kompromittiert wurden in solchen Fällen muss das Zertifikat noch vor dem eigentlichen Ablaufdatum gesperrt werden.

Eine **CDP (CRL Distribution Point)** = Zertifikatsperrlisten-Verteilungspunkt ist eine Verzeichnisfreigabe in dem man die Zertifikatsperrliste(n) einer Firma findet und öffentlich für das Netzwerk zugänglich macht.

Die Standardangaben einer sogenannten CDP (CRL Distribution Point) sind wie folgt:

- Lokaler Pfad Zertifikatsserver C:\Windows\system32\CertSrv\CertEnroll\<CDP variables>
- LDAP Idap://CN=<CDP CA Name>,CN=<CDP server><other CDP variables>
- HTTP/HTTPS http://<CA server name>\CertEnroll\<CDP variables>
- Dateipfad file://<CDP variables>
- Dateifreigabe \\<server name>\<share>\<CDP variables>

Da nicht alle Firmen Benutzer auf das Hauptverzeichnis vom Domänencontroller zugreifen sollen, werden die Zertifikatssperrliste(n) in eine neue Freigabe um konfiguriert.



# Erweiterung in der Zertifizierungsstelle konfigurieren

Als erstes wird die Verwaltungskonsole der Zertifizierungsstelle geöffnet, mit der rechten Maustaste klickt man auf den Servernamen und ruft die Eigenschaften auf.

Eigenschaften von HTDOM-CA 🛛 ? 🗙						
Speicherung	Zertifikatver	waltungen	Regist	trierungs-Agents		
Überwachung	Wieder	herstellungs-Ag	jents	Sicherheit		
Allgemein Ric	htlinienmodul	Beendigung	smodul	Erweiterungen		
Erweiterung auswa	ählen:					
Sperrlisten-Verteil	ungspunkt			~		
Geben Sie Standorte an, von denen Benutzer eine Zertifikatsperfiste erhalten können. http:// <serverdnsname>/CertEnroll/<caname><crlnamesuffix><d< td=""></d<></crlnamesuffix></caname></serverdnsname>						
http://ads01.htdo	m.local/CertEn	roll/ <caname></caname>	<crlnan< td=""><td>neSuffix&gt;<del <sub="">≡</del></td></crlnan<>	neSuffix> <del <sub="">≡</del>		
\\ads01.htdom.lo	cal/CertCRDLis	t\$\ <caname><c< td=""><td><crlnames< td=""><td>eSuffix&gt;<delt td="" ~<=""></delt></td></crlnames<></td></c<></caname>	<crlnames< td=""><td>eSuffix&gt;<delt td="" ~<=""></delt></td></crlnames<>	eSuffix> <delt td="" ~<=""></delt>		
< 111		-		>		
Hinzufügen Entfemen Sperilisten an diesem Ort veröffentlichen						
In alle Sperifisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll						
☑ In Sperilisten einbeziehen. Wird z. Suche von Deltasperilisten verwendet						
✓ In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen						
Deltasperrlister	an diesem Ort	veröffentlichen				
In die IDP-Erw	eiterung ausges	tellter CRLs eir	beziehen			
(	ОК АЫ	brechen	bernehme	en Hilfe		

In der Erweiterung wählt man die **Sperrlisten-Verteilungspunkt** aus und fügt insgesamt zwei neue Einträge hinzu.

Erster Eintrag enthält die URL die man später über den Browser aufrufen kann.

#### http://crl.server.domain.local/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

- In Sperrliste einbeziehen. Wird z. suchen von Deltasperrlisten verwendet
- In CDP-Erweiterungen des ausgestellten Zertifikats einbeziehen



	Eigenso	hafte	n von H	TDOM-CA	A L	?	x
Speicherung	) Zerti	fikatven	waltungen	Regist	rierung	s-Ager	nts
Überwachu	ing	Wieder	herstellungs	-Agents	Sic	cherhe	eit
Allgemein	Richtlinienm	odul	Beendig	ungsmodul	Erwe	eiterun	gen
Erweiterung a	uswählen:						
Sperfisten-V	erteilungspun	kt					~
Geben Sie Standorte an, von denen Benutzer eine Zertifikatsperfiste erhalten können. http:// <serverdnsname>/CertEnroll/<caname><crlnamesuffix><de file://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><de http://ads01.htdom.local/CertEnroll/<caname><crlnamesuffix>CDet http://cd.ads01.htdom.local/CertEnroll/<caname><crlnamesuffix>CDetaO \vads01.htdom.local/CertCrDList\$\<caname><crlnamesuffix>CDetaV vads01.htdom.local/CertCRDList\$\<caname><crlnamesuffix>CDetaV vads01.htdom.local/CertCRDList\$\<caname><crlnamesuffix>CDetaV vads01.htdom.local/CertCRDList\$\<caname><crlnamesuffix><detav< td=""></detav<></crlnamesuffix></caname></crlnamesuffix></caname></crlnamesuffix></caname></crlnamesuffix></caname></crlnamesuffix></caname></crlnamesuffix></caname></de </crlnamesuffix></caname></serverdnsname></de </crlnamesuffix></caname></serverdnsname>							
Hinzufügen Entfemen  Spertisten an diesem Ort veröffentlichen  In alle Spertisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll							
In Sperilisten einbeziehen. Wird z. Suche von Deltasperilisten verwendet							
In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen							
Deltasperfisten an diesem Ort veröffentlichen							
In die IDP	-Erweiterung	ausgest	ellter CRLs	einbeziehen			
	ОК	Abb	prechen	Übernehme	n	Hilf	e

Zweiter Eintrag beinhaltet die Serverfreigabe die im Anschluss angelegt wird.

#### \\server.domain.local\<Freigabe\$>\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

- Sperrlisten an diesen Ort veröffentlichen
- Deltasperrlisten an diesen Ort veröffentlichen

## **DNS Host Eintrag konfigurieren**

Damit wir die URL später im Browser aufrufen können legen wir einen neuen A/AAAA Host Eintrag im DNS Server an

In diesem Beispiel - crl - IP-Adresse Zertifikatserver

Neuer Host X
Name (bei Nichtangabe wird übergeordneter Domänenname verwendet):
cl
Vollqualifizierter Domänenname:
crl.htdom.local.
IP-Adresse:
192.168.178.101
Verknüpften PTR-Eintrag erstellen
Authentifizierte Benutzer können DNS-Einträge mit demselben Besitzernamen aktualisieren
Gültigkeitsdauer (TTL):
0 :1 :0 :0 (TTTTT:HH.MM.SS)
Host hinzufügen Abbrechen

## Managed Service Account im AD anlegen

Im Active Directory wird ein neuer Managed Service Account anlegen, der später Vollzugriff auf das Virtuelle Verzeichnis im IIS bekommt.

Datei Aktion Ansicht ?			
🗢 🄿 📶 🦸 📋 🗙 🗟 🗟	🛛 🖬 🗏 🐮 🝸	<u>e</u> (*	
Active Directory-Benutzer und -Computer [A	Name	Тур	Beschreibung
b Gespeicherte Abfragen	👗 CertCRDList	Benutzer	CRD List PKI User - HTDOM-CA and IIS Virtual Directory
⊿ 🚔 htdom.local	🔏 KeyRecoveryAgent	Benutzer	KeyRecoveryAgent for PKI - HTDOM-CA
▶ 1 LHTDOM			
Builtin			
Computers			
Domain Controllers			
ForeignSecurityPrincipals			
LostAndFound			
Managed Service Accounts			
	1		

## Virtuelles Verzeichnis im IIS konfigurieren

Im IIS-Servermanager legen wir für die Default Web Site ein neues Virtuelles Verzeichnis an



Das Virtuelle Verzeichnis bekommt einen Aliasname **CRLD** und im Physikalischen Pfad **C:\Windows\system32** wird ein neuer Ordner mit dem Namen **CertCRDList** angelegt. Der Ordner kann theoretisch angelegt werden wo man möchte.



Virtuelles Verzeichnis bearbeiten ? ×
Sitename: Default Web Site Pfad: /
Alias: CRLD Beispiel: Bilder Physischer Pfad: C:\Windows\System32\CertCRDList verbinden als "htdom\CertCRDList" Verbinden als Einstellungen testen
Verbinden als ? X
Pfadanmeldeinformationen:
Bestimmter Benutzer:     htdom\CertCRDList     Festlegen     Anwendungsbenutzer (Pass-Through-Authentifizierung)
OK Abbrechen

Bei Verbinden als... konfigurieren wir nun den neu erstellten Managed Service Account.

Bitte noch nicht auf **Einstellung testen**... klicken, hier würde man eine Fehlermeldung angezeigt bekommen, da der Managed Service Account noch <u>nicht</u> auf das Verzeichnis berechtigt ist.



Im nächsten Schritt berechtigen wir jetzt das Virtuelle Verzeichnis für die Veröffentlichung der Zertifikatssperrliste(n), hierzu klickt man auf das Virtuelle Verzeichnis und bearbeite die Berechtigungen.



Eigenschaften von	CertCRDLi	st	x
Erweiterte Fr	eigabe		x
✓ Diesen Ordner freigeben			
Einstellungen			
Freigabename:			
CertCRDList\$		~	
Hinzufügen Entfer	nen		
Zugelassene Benutzeranzahl eins auf:	thränken	16777 🔹	
Kommentare:			
🐌 🛛 Berechtigungen für	"CertCRDL	ist\$"	×
Freigabeberechtigungen			
Gruppen- oder Benutzemamen:			
leder			
& ADS01\$ (HTDOM\ADS01\$)			
👗 CertCRDList (CertCRDList@htd	om.local)		
H	inzufügen	Entferner	ı
Berechtigungen für "CertCRDList"			_
	Zulassen	Verweige	<u>m</u>
Vollzugriff			
Andem	~		
Lecon	~		

Das Verzeichnis wird nun Freigegeben mit dem Namen CertCRDList\$

Berechtige den Domänencontroller mit Vollzugriff und den Managed Service Account mit Ändern Rechte, Jeder hat lese Zugriff.

Eigenschaften von CertCRDList	x
Allgemein Freigabe Sicherheit Vorgängerversionen Anpasser	1
Berechtigungen für "CertCRDList"	x
Sicherheit	
Objektname: C:\Windows\System32\CertCRDList	
Gruppen- oder Benutzernamen:	
ADS015  Administratoren (HTDOM\Administratoren)  CentCRDList (CertCRDList (CertCRD	
Vollzugriff  Andem  Vollzugriff Andem  Vollzugriff Lesen, Ausführen  Vollzugrift Crdnerinhalt anzeigen  Lesen  V	
OK Abbrechen Übernehm	men

In dem Reiter Sicherheit berechtige ich ebenfalls den Domaincontroller mit Vollzugriff und den Managed Service Account mit Ändern Rechte, alles anderen Einträge bleiben unverändert.



Im Anschluss kann man das Virtuelle Verzeichnis auf den Zugriff testen.

C - I / A I Santa I Sa	istrator)	rbeiten
<ul> <li>▲ Sites</li> <li>▲ Default Web Site</li> <li>▶ ■ Default Web Site</li> <li>▶ ■ aspnet_client</li> <li>▶ ■ CertEnroll</li> <li>▶ ■ CertEnroll</li> <li>▶ ■ CertSiv</li> <li>▶ ■ CRLD</li> </ul>	Virtuelles Verzeichnis bearbeiten     ?     X       Sitename:     Default Web Site     Pfad:     /       Alias:     CRLD     Beispiel: Bilder       Physischer Pfad:         C:\Windows\System32\CertCRDList        Verbinden als     Einstellungen testen	erwalten vis durchsuchen https://durchsuchen vis bearbeiten gen
Bereit Ergel	Verbindung testen           nisse:           en         Einstellung           uthentifizierung         Benutzername (htdom\CertCRDList)           utorisierung         Auf den Pfad kann zugegriffen werden (C:\Windows\Syste	

# Zertifikatssperrliste veröffentlichen

Um nun die Zertifikatssperrliste(n) im neuen Verzeichnis zu veröffentlichen, öffnet man die Verwaltungskonsole der Zertifizierungsstelle, klickt auf Gesperrte Zertifikate  $\rightarrow$  Alle Aufgaben  $\rightarrow$  Veröffentlichen.

🔄 🔄 🗉 🏦 🕨 Netzwe	rk ⊧ ads01	.htdom.local 🕨 Cert(	CRDList\$			
🔆 Favoriten	Name	<b>^</b>		Änderungsdatum	Тур	Größe
📃 Desktop	🐮 H	TDOM-CA.crl		17.02.2015 11:46	Zertifikatsperrliste	1 KE
🗼 Downloads	w	eb.config		17.02.2015 11:38	CONFIG-Datei	1 KE
🖳 Zuletzt besucht						
🗔 certsrv	/ - [Zertifi	izierungsstelle (Lo	kal)\HTDOM-	CA\Gesperrte Zertif	ikate] 📃 🗖	x
Datei Aktion Ansicht ?						
🗢 🄿 🙇 🗐 🕼 👔						
🚋 Zertifizierungsstelle (Lokal)		Anforderungs-ID	Sperrdatum	Effektives Sperrdatum	Grund für die Sperrun	ig Ar
🛛 🍶 HTDOM-CA		5	16.02.2015 2	16.02.2015 22:55	Vorgangsende	HI
Gesnerrte Zertifikate			15 02 26 15 2	16.02.2015 23:05	Vorgangsende	
📔 🛛 Alle Aufgaben	•	Veröffentlichen				н

## Zertifikatssperrliste im Browser überprüfen

CertSrv	- Ċ 🌈 crl.htdom.locəl - /crld/ ×	
crl.htdom.local - /crld/           [To Parent Directory]           17.02.2015         11:46           17.02.2015         11:38		
Zertifikatsperrliste	certsrv - [Zertifizierungsstelle (Lokal)\HTDOM-CA\Ges	perrte Zertifikate]
Allgemein         Sperrliste           Gesperrte Zertifikate:	Datei Aktion Ansicht ?	Anfangsdatum des Zer 16.02.2015 22:41 16.02.2015 22:47

Um das Ganze zu kontrollieren kann man im Webbrowser die URL zu dem Sperrlistenzertifikat aufrufen.

#### http://crl.<domain.de>/crld/<ZertifizierungsStellenName>.crl

Sollte die URL nicht aufgerufen werden können, kann es daran liegen dass die Webseite noch zu den Vertrauenswürdigen Webseiten hinzugefügt werden muss.

## Gruppenrichtlinie für Vertrauenswürdige Webseiten konfigurieren

Dies kann man recht einfach per Gruppenrichtlinie erledigen.

net_Explorer_11_Settings_HTDOM				
rmittelt am: 17.02.2015 18:03:15				Alle ausble
terkonfiguration (Aktiviert)				Ausble
linien				<u>Ausble</u>
ninistrative Vorlagen				Ausble
Richtliniendefinitionen (ADMX-Dateien) wurden beim lok	alen Computer abgerufen.			
Windows-Komponenten/Internet Explorer/Internets	/stemsteuerung/Sicherheitsseite			Ausble
Richtlinie	Einstellung		Kommentar	
Liste der Site zu Zonenzuweisungen	Aktiviert			
Geben Sie die Zonenzuweisungen hier ein				
http://cd.htdpm.local/odd/HTDOM-CA.cd		2		
http://chinicdoin.ideal/chid/111Dointe.ck.ch		2		
https://adsU1.htdom.local/certsrv/default.asp		2		
				Auchie
				Ausble
linien				Ausble
ninistrative Vorlagen				Ausble
Richtliniendefinitionen (ADMX-Dateien) wurden beim lok	alen Computer abgerufen.			
Windows-Komponenten/Internet Explorer/Internets	/stemsteuerung/Sicherheitsseite			Ausble
Richtlinie	Einstellung		Kommentar	
Liste der Site zu Zonenzuweisungen	Aktiviert			
Geben Sie die Zonenzuweisungen hier ein				
Geben Sie die Zonenzuweisungen hier ein.		2		
Geben Sie die Zonenzuweisungen hier ein. http://crl.htdom.local/crld/HTDOM-CA.crl		2		

Download Administrative Templates for Internet Explorer



#### Richtlinie

Computerkonfiguration --> Administrative Vorlagen --> Windows Komponenten --> Internet Explorer --> Internetsystemsteuerung --> Sicherheitsseite --> Liste der Site zu Zonenzuweisung

### http://crl.<domain.de>/crld/<ZertifizierungsStellenName>.crl

Benutzerkonfiguration --> Administrative Vorlagen --> Windows Komponenten --> Internet Explorer --> Internetsystemsteuerung --> Sicherheitsseite --> Liste der Site zu Zonenzuweisung

## http://crl.<domain.de>/crld/<ZertifizierungsStellenName>.crl

So das war es erstmal wieder von mir.

Viele Grüße Helmut Thurnhofer