Certificates rely on certification authorities to maintain an updated list of revoked certificates issued by the public key infrastructure. Certificates are revoked for a number of reasons—not all revocations are for compromised certificates or nefarious reasons. It is essential that when a computer is presented a revoked certificate, that it does not honor the certificate.

The common means to inform computers of revoked certificates is by using a certificate revocation list (CRL). Ensuring that the certificate revocation list gets to all computers can be problematic—if you do not understand how to set up the paths to the certificate revocation list distribution point. This article describes how to set up and publish a certificate revocation list distribution point to ensure that all computers receive an up-to-date certificate revocation list.

Author: Rick Kingslan, Microsoft Senior Technical Writer

Publication date: December 17, 2012, updated Feb. 10, 2014

Product version: Windows Server 2003, Windows Server 2008, Windows Server 2012

The certificate revocation list or CRL is a primary mechanism that ensures the security and health of your PKI. The CRL is a list of all certificates that have been issued by your PKI but have been revoked for one reason or another. There are two types of CRLs:

- The first type is a full CRL; it contains all certificates revoked by the PKI.
- The second type is known as a delta CRL. It contains the list of all revoked certificates since the last time a full CRL was created. If a computer has received a full CRL, it requests a delta CRL, unless a new full CRL is available.

This function of collecting certificate serial numbers (an attribute of the certificate that is guaranteed to be unique within the scope of your PKI), populating a list with the serial numbers, creating the CRL, and then posting the CRL to a **CRL distribution point** is an essential security component.

If a revoked certificate is not identified as compromised or invalid, it creates a significant number of security risks including interception of encrypted data and impersonating another computer or user.

Certificates issued by public CAs have a CDP. Your internal PKI needs one, too. This article shows you the most effective way to create the CDP and ensures that your PKI-issued certificates will have access to this important list of revoked certificates.

What is CDP?

The certificate revocation list distribution point (CDP) is a path represented as one or more attributes on every certificate issued by a PKI.

Configure the CDP settings on the certificate authority

1. On DC1, click **Start**, **Administrative Tools**, and click **Certification Authority**.

2. In the details pane, right-click the name of the CA. For example, **DC1-CA**, then click **Properties**.

3. Click the **Extensions** tab.

4. On the Extensions tab, click **Add**. In Location, type **http://crl.<the domainname>/crld/** For example, **http://crl.dc1.contoso.com/crld/**

5. In Variable name, click **<CaName>**, click Insert; click **<CRLNameSuffix>**, click Insert; click **<DeltaCRLAllowed>**, click Insert.

6. In **Location**, type **.crl** at the end of the Location string and then click **OK**.

7. Select **Include in CRLs.** Clients use this to find Delta CRL locations. And Include in the CDP extension of issued certificates, then click **Apply**. Click **No** in the dialog box asking you to restart the ADCS.

Configure the file share definition:

1. Click **Add**.

2. In **Location**, define the file server and share name. For example, type **\\fs01\crldist$** . (See Note above.)

Note: The file share definition above contains the special character '$' that has the effect of making the file share invisible to simple browsing methods. If you know the name of the server and share, you can connect – given that you have the permissions. But browsing a list of computers and their shared resources will not list the share crldist. Not intended as a security mechanism, but more of a method to hide shares that are special purpose and not meant for users.

3. In **Variable,** click **<CAName>**, click **Insert**; In **Variable**, click **<CRLNameSuffix>**, click **Insert**; In **Variable**, click **<DeltaCRLAllowed>**, click **Insert**.

4. In **Location**, type **.crl** at the end of the Location string and then click **OK**.

5. Select **Publish CRLs to this location** and **Publish Delta CRLs to this Location**, then click **Apply**. Click **Yes** in the dialog box asking you to restart the ADCS.

6. Close the **Certification Authority** console.

Create a DNS record for crl.contoso.com

1. On your DNS Server, click **Start**, click **Administrative Tools**, click **DNS**.

2. In the **DNS Manager console**, expand your DNS server, expand **Forward Lookup Zones**. Right-click your domain name, and click **New Host (A or AAAA)**.

3. In the **New Host** dialog, type **crl** in the **Name (uses parent domain name if blank)**. In **IP address**, type the IP address of the CA server. Click **Add Host**. Click **OK** in the dialog noting that the record was created. Click **Done** in the **New Host** dialog box.

4. Close the DNS Manager console.

Configure the file server for HTTP CRL distribution

1. Install the IIS role on FS01. Accept at the least the defaults, and click **Install**.

2. Verify that the IIS installation was successful and then click **Close**.

3. To create the web-based CDP, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

4. In the console tree, navigate to FS01\Sites\Default Web Site. Right-click **Default Web Site** and click **Add Virtual Directory**.

5. In the **Add Virtual Directory** dialog box, in **Alias**, type *CRLD*. Next to **Physical path**, click the ellipsis "…" button.

6. In the **Browse for Folder** dialog box, click **Local Disk (C:)**, and then click **Make New Folder**.

7. Type *CRLDist*, and then press **ENTER**. Click **OK** in the **Browse for Folder** dialog box.

8. Click **OK** in the **Add Virtual Directory** dialog box.

9. In the middle pane of the console, double-click **Directory Browsing**.

10. In the details pane, click **Enable**.

11. In the console tree, click the CRLD folder.

12. In the middle pane of the console, double-click the **Configuration Editor** icon.

13. Click the down-arrow for the **Section** drop-down list, and then navigate to system.webServer\security\requestFiltering.

14. In the middle pane of the console, double-click the **allowDoubleEscaping** entry to change the value from **False** to **True**.

15. In the details pane, click **Apply**.

16. Close the **Internet Information Services (IIS) Manager** console.

Configure the file server for file share CRL publishing

1. On APP1, click **Start**, and then click **Computer**.

2. Double-click **Local Disk (C:)**.

3. In the details pane of Windows Explorer, right-click the **CRLDist** folder and click **Properties**.

4. In the **CRLDist Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.

5. In the **Advanced Sharing** dialog box, select **Share this folder**.

6. In Share name, add a "$" to the end so that the share name is CRLDist$. Recall that appending the $ hides the share from simple browsing.

7. In the **Advanced Sharing** dialog box, click **Permissions**.

8. In the **Permissions for CRLDist$** dialog box, click **Add**. (See Note above.)

9. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.

10. In the **Object Types** dialog box, select **Computers**, and then click **OK**.

11. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select**, type *DC1*, and then click **Check Names**. Click **OK**.

12. In the **Permissions for CRLDist$** dialog box, select DC1 (CONTOSO\DC1$) from the **Group or user names** list. In the **Permissions for DC1** section, select **Allow for Full control**. Click **OK**.

13. In the **Advanced Sharing** dialog box, click **OK**.

14. In the **CRLDist Properties** dialog box, click the **Security** tab.

15. On the **Security** tab, click **Edit**.

16. In the **Permissions for CRLDist** dialog box, click **Add**.

17. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.

18. In the **Object Types** dialog box, select **Computers**. Click **OK**.

19. In the **Select Users, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select**, type *DC1*, and then click **Check Names**. Click **OK**.

20. In the **Permissions for CRLDist** dialog box, select DC1 (CONTOSO\DC1$) from the **Group or user names** list. In the **Permissions for DC1** section, select **Allow for Full control**. Click **OK**.

21. Click **Close** in the **CRLDist Properties** dialog box.

22. Close the Windows Explorer window.

Wow! That's a Lot of Stuff!

Yes, it is. There is one more thing that we need to do – we need to be sure that the CRLs are actually being published to the file share CDP. You publish the CRLs and delta CRLs to the FS01 file share by doing the following:

1. On DC1, click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.

2. In the console tree, open DC1-CA. Right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**.

3. In the **Publish CRL** dialog box, click **New CRL**, and then click **OK**.

4. Click **Start**, type \\FS01\CRLDist$ and press **ENTER**.

5. In the Windows Explorer window, you should see the DC1-CA (this is the full CRL) and DC1-CA+ (this is the delta CRL) files.

6. Close the Windows Explorer window. Close the Certification Authority console.

What Does This Look Like on the Certificate?

Important: This CDP will only appear on certificates created AFTER the CDP is defined. This means that if you have issued certificates, you will need to re-issue certificates to have the CDP available to those computers. There is no way around this.

We know why the CDP is important, but what does it actually look like? Note the http:// and file:// path and how it relates to the process we've detailed. We've seen variables, but what do those variables contain? We configured the following:

For the Web services on the CA:

http://crl.dc1.contoso.com/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

Note: You should be able to reach this location using a browser, and is an effective troubleshooting measure.

What do the three variables used resolve to?

- CaName: Inserts the DNS Name of the server into the path.
- CRLNameSuffix: Appends a suffix to distinguish the CRL file name.
- DeltaCRLAllowed: Substitutes the delta CRL name suffix for the CRL file name suffix, if appropriate.

Based on what the certificate needs, it will use the populated information to retrieve the CRL or delta CRL using a path like the following, which is derived from the populated CDP according to the rules for the Web services on the CA.

URL=http://crl.contoso.com/crld/DC1-CA.crl

And, just for fun, here is the LDAP CDP:

URL=ldap:///CN=DC1-CA,CN=DC1,CN=CDP,CN=Public%20Key%20Services,

CN=Services,CN=Configuration,contoso,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint

This article contains a lot of information. Don't be intimidated if the CA topic is new to you. Just think of the CDP as a defined path to where all issued certificates look for their CRLs. That's the net of what the CDP is.

Reminders

A CDP only applies to certificates issued AFTER the CDP path is created and published. Certificates created before the path was published will look to the existing CDP path on that certificate.

CDP can be hosted by an LDAP path, HTTP path, file path or file share. Note that there is the local C:\Windows System32 path that was discussed earlier. This is the local store where the CA puts files for its own use – not other computers

https://technet.microsoft.com/en-us/library/cc770413(v=ws.10).aspx