Access Gateway Advanced 4.5

Registry Scan
(Watermark Scan)

Inhaltsverzeichnis

Grundsätzliches

Diese Anleitung richtet sich an alle Administratoren, die bereits mit Produkten von Citrix vertraut sind, oder es werden wollen. Die Anleitung erfordert u. U. das Bearbeiten der Registry, oder das Austauschen von Dateien. Diese Arbeiten sollten nie ohne vorgängige Sicherung der manipulierten Dateien oder der Registry vorgenommen werden. Auch sonst gelten die üblichen Vorsichtsmassnahmen bei Anpassungen und Manipulationen an bestehenden Softwareinstallationen.

Dieses Dokument wurde mit grösster Sorgfalt erstellt und geprüft. Es kann jedoch nicht mit 100%iger Sicherheit ausgeschlossen werden, dass trotzdem Fehlfunktionen auftreten. Eine Haftung für Schäden, die durch die vorliegende Anleitung und deren Implementation entstanden sind, wird hiermit abgelehnt.

Das Problem

Wer das Citrix Access Gateway (CAG) mit Advanced Access Control (AAC) schon eine Weile kennt, speziell die Version 4.2, kennt sicher auch den “Citrix Watermark” End Point Analysis Scan (EPA Scan). Eine Möglichkeit, über einen Registry Key die Zugehörigkeit zu einer bestimmten Sicherheitsgruppe zu definieren. Im Gegensatz zu MAC oder Domain Filtern war dieser Scan eine einfache Möglichkeit, schnell den Sicherheitskontext zu wechseln, um z. B. bei Produktdemonstrationen unterschiedliche Zugriffsszenarien vorführen zu können.

Das Update auf die AAC Version 4.2.5, bzw. auf die Version 4.5 brachte hier massive Änderungen im Bereich EPA Scans mit sich. Als einschneidendste Änderung kann die Verpflichtung zum Signieren aller EPA Scans gelten. Neu sind alle EPA Scans von Citrix bereits signiert. Selbst erstellt EPA Scans funktionieren nun ebenfalls nur noch, wenn sie signiert und damit als vertrauenswürdig gekennzeichnet sind. Diesen Aufwand und die damit verbundenen Kosten scheuen viele Kunden. Für Citrix Partner, die nur eine Demo Site aufbauen wollen, lohnt sich der Aufwand in der Regel ebenfalls nicht. Wer daher kein Geld in Custom Scans z. B. von EPAFactory stecken wollte, musste sich zwangsläufig mit den mitgelieferten EPA Scans arangieren:-(

Hier möchte ich daher einen Weg aufzeigen, wie mit den vorhandenen Möglichkeiten trotzdem ein funktionierender Registry Scan zu erstellen ist. Die meisten EPA Scans machen tatsächlich nichts anderes, als in der Registry des Clients an vorkonfigurierten Stellen vorhandene Werte auszulesen. Daher kann prinzipiell fast jeder EPA Scan als Registry Scan verwendet werden. Als Beispiel verwende ich hier den mitgelieferten “Citrix Scans for Windows Update”. Dieser Scan liest auf dem Clientrechner rekursiv alle Keys unterhalb von:

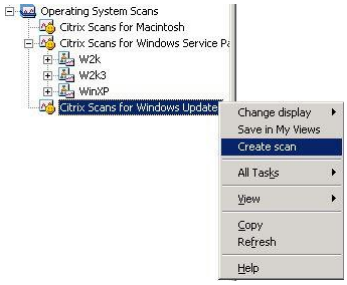
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates

aus und liefert die darin gefundenen KB-Nummern zurück. Zu beachten ist hier, dass Keys direkt unter dem o. g. Key **nicht** zurückgeliefert werden. Man sollte sich daher einen vorhandenen Unterordner auswählen um den Key dort zu erstellen. Mit diesem Wissen lässt sich nun recht einfach ein Registry Scan erstellen. Wem diese Kurzanleitung nicht genügt, findet hier eine detaillierte Beschreibung mit Screenshots.

Die Lösung

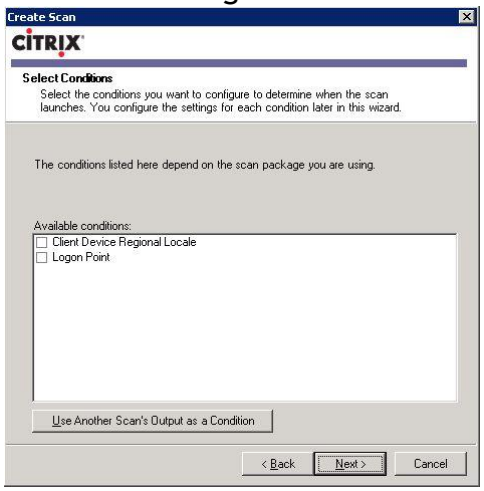
Um einen neuen EPA Scan zu erstellen, genügt es, einen Rechtsklick auf den entsprechenden Knoten in der Application Management Console (AMC) zu machen. Im darauf erscheinenden Kontextmenü wird mit „Create Scan“ der Assistent gestartet. In diesem Beispiel wird der „Citrix Scans for Windows Updates“ verwendet.

EPA Scan erstellen



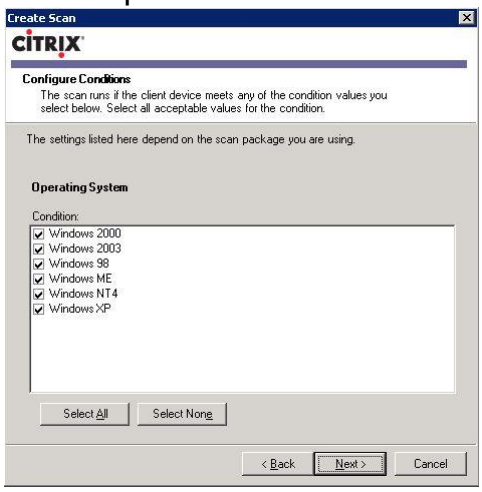
Der Assistent fragt nach einem Namen, der prinzipiell frei gewählt werden kann, aber sinnvollerweise eine „sprechende“ Bezeichnung erhält, hier „Watermark“.

Im nächsten Schritt können weitere Vorbedingungen definiert werden, die hier nicht von Belang sind.

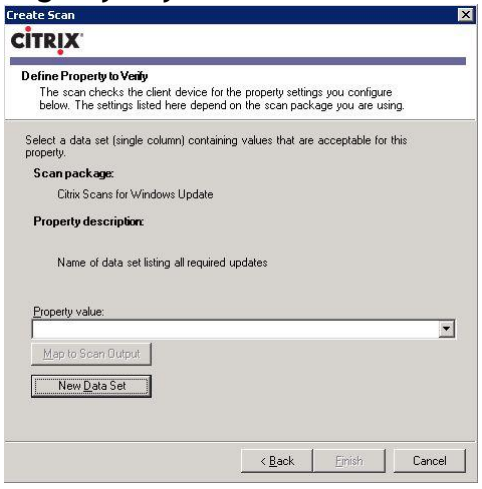


Auch der Name der Regel sollte möglichst „sprechend“ sein. Dies erleichtert das spätere Auffinden und Managen der EPA Sans, wir verwenden hier „Full_Access“.

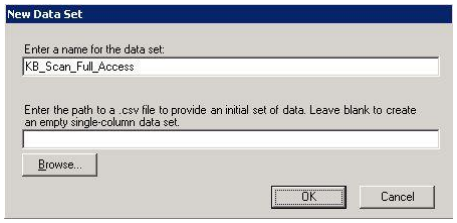
Welche Betriebssysteme unterstützt werden sollen, ist individuell verschieden und hat hier praktisch keinen Einfluss.



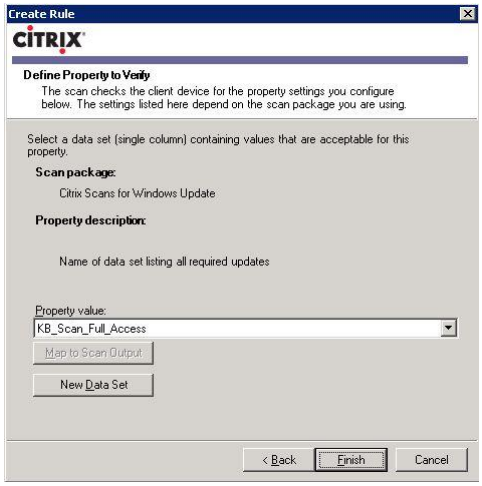
Hier wird nun ein neues „Data Set“ benötigt, welches den zu überprüfenden Registry Key enthält. Über den Button „New Data Set“ wird er erstellt.



Hier kann ein neues, leeres „Data Set“ erstellt werden. Der Name sollte auch hier wieder „sprechend“ sein und auf den erwünschten Zweck schliessen lassen. Für jedes gewünschte Szenario wird ein eigenes „Data Set“ benötigt, wir verwenden hier „KB_Scan_Full_Access“. Weiter Beispiele wären *Restricted, oder *OWA_Only.

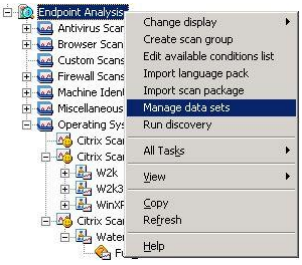


Mit Finish wird dieser Assistent beendet und das Ergebins sollte dann so aussehen:



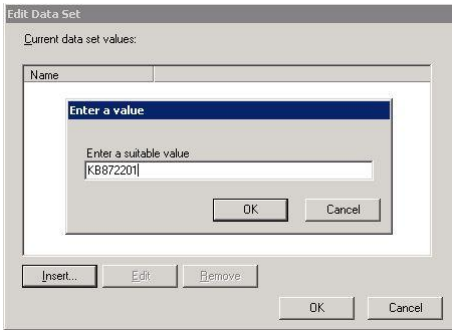
Data Set konfigurieren

Das gerade erstellte „Data Set“ ist momentan noch leer und muss nun mit einem Wert versehen werden, der später in der Client Registry wieder zu finden ist. Dazu genügt ein Rechtsklick auf den Knoten „Endpoint Analysis“ in der AMC. Im darauf erscheinenden Kontextmenü wird nun der Punkt „Manage Data Sets“ ausgewählt.

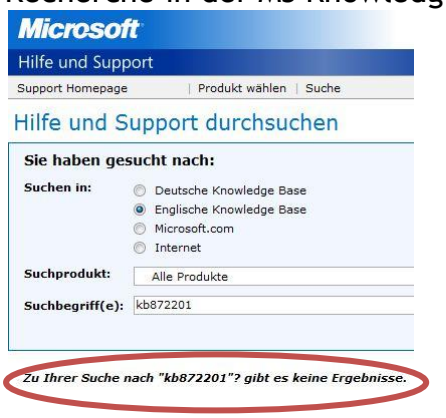


In dem folgenden Fenster wird das vorher erstellte „Data Set“ markiert und mit dem „Edit“ Button zum Bearbeiten geöffnet, hier „KB_Scan_Full_Access“.

Das „Data Set“ kann einen, oder auch eine beliebige Kombination von Werten enthalten. Es ist allerdings bei der Namensgebung darauf zu achten, dass keine bereits vorhandenen HotFix Bezeichner verwendet werden. In diesem Beispiel verwenden wir einen nicht existierenden HotFix KB872201.



Um sicher zu gehen, dass es nicht zu Konflikten kommt, empfiehlt sich eine kurze Recherche in der MS Knowledge Base.



Nach drei beherzten Klicks auf „OK“ ist das „Data Set“ erstellt und einsatzbereit. Diesen Vorgang sollte man für jedes weitere gewünschte Szenario wiederholen und dafür jeweils einen anderen „HotFix“ verwenden.

Den Client konfigurieren
Auf dem Client wird nun natürlich noch der korrekte Registry Key benötigt, um den EPA Scan erfolgreich abschliessen zu können. Dazu empfiehlt es sich, ein Reg File vorzubereiten, mit dem sich der Key bequem auf andere Maschinen verteilen lässt. Ein Beispiel findet sich hier:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\MSXML4SP2\KB872201]
"Description"="FIX: ASP stops responding when calling Response.Redirect to
another server using msxml4 sp2"
"InstalledDate"="29.12.2006"
"InstalledBy"="XYZ"
"IsInstalled"=dword:00000001
"ServicePack"=dword:00000001
```

Wichtig sind nur die beiden fett markierten ersten beiden Zeilen. Alles Weitere dient nur dazu, den Key plausibler erscheinen zu lassen, falls jemand sich die Mühe machen sollte, nach dem Key zu suchen. Prinzipiell genügt auch ein leerer Key.

Zu beachten ist weiterhin, dass Keys **nicht** berücksichtigt werden, die direkt unter

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\
```

Stehen. In dem Obigen Beispiel würde daher der Key“MSXML4SP2” vom EPA Scan ignoriert und der Scan würde einen Fehler zurückgeben. Es muss immer eine weitere Ebenen zwischen „HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\“ und dem abzufragenden Key existieren.

Fazit
Das oben beschriebene Vorgehen lässt sich bei vielen anderen EPA Scans in ähnlicher Form umsetzen, sei es ein AntiViren, oder ein Browser Scan. Es müssen nur der, oder die Keys, welche vom EPA Scan tatsächlich abgefragt werden, herausgefunden werden. Hier hefen zum Einen der gesunde Menschenverstand und zum Anderen Tools wie RegMon oder der ProcessMonitor von Sysinternals weiter.

Der praktische „Citrix Watermark“ Scan steht zwar in den aktuellen Versionen nicht mehr zur Verfügung, dieses Problem lässt sich aber mit dem oben beschriebenen Vorgehen leicht kompensieren. Der Zugewinn an Sicherheit durch signierte EPA Scans ist dieses kleine Manko sicher wert.

Ich wünsche allen ein „Happy Testing“
Gruss
Ecki