ReDoKS

Revisions-, Dokumentations- und Kontroll-System

Anpassungen auf die FIDUCIA IT-Cloud

Inhalt

1 ReDoKS – Anpassungen auf die FIDUCIA IT-Cloud

Die Einführung der FIDUCIA IT-Cloud bringt eine Reihe von Änderungen mit sich, die umfangreiche Anpassungen bei ReDoKS erfordern.

Die dringlichste Anpassung betrifft den Domänenscan mit der ScanAD.exe. Mit der bisherigen Version der ScanAD.exe kann die IT-Cloud-Domäne (pb.rz.in.gad.de) nur von einem Arbeitsplatz aus gescannt werden, der Teil der IT-Cloud ist (z.B. ein PaaS-Server).

Mit der Neufassung der ScanAD.exe (siehe Kapitel 0) können sowohl die alte R-Domäne als auch die IT-Cloud-Domäne (oder auch andere Domänen) vom Arbeitsplatz des Admins aus gescannt werden, auch wenn dieser nicht Teil der gescannten Domäne ist.

Die ScanPC.exe kann unverändert weiter genutzt werden, doch sind beim automatisierten Aufruf per GPO einige Änderungen zu beachten (siehe Kapitel 0)

Mit der bisherigen Version des Viewers können auch die von der neuen ScanAD.exe erzeugten Dateien eingelesen werden. Im Laufe des Jahres werde ich allerdings noch eine neue Version der Viewer.exe (unter dem Namen ReDoKS.exe) erstellen, die parallel zum alten Viewer verwendet werden kann und in einer Reihe von Punkten deutliche Verbesserungen umsetzen wird:

- Deutlich bessere Möglichkeiten zu Filterung, Sortierung, Suche etc in allen Tabellen
- Die Möglichkeit, Scans mehrerer Domänen zugleich zu laden und Querverweise herzustellen
- Reporting-Möglichkeiten (also Erzeugen durch Templates vorgegebener Berichte z.B. als Word-Dokument), z.B. zur automatischen Erstellung eines „Management Summary“ etc

Gerade bei Parallelbetrieb von R-Domäne, IT-Cloud-Domäne und ggf. weiteren Domänen (z.B. von bn-its) wird es damit besser möglich sein, z.B. die Berechtigungen eines Benutzers über alle Domänen hinweg darzustellen.

Wichtig:

- Die „alten“ Komponenten von ReDoKS führen die bisherige Versionsnummer 1.x. weiter
- Die „neuen“ Komponenten von ReDoKS (erst einmal die ScanAD.exe) beginnen mit Versionsnummer 2.x

1.1 Templateanpassungen

Die folgenden Definitionsdateien für den Viewer wurden angepasst und sind im Paket enthalten:

1. FTypes.ini: Die Datei für die Funktionstypen wurde um Einträge für die IT-Cloud erweitert und ersetzt die gleichnamige Altdatei
2. FIDUCIA_IT-Cloud.tpl: Dieses Domänentemplate ist für die Auswertung der IT-Cloud-Domäne pb.rz.in.gad.de anstelle des FIDUCIA_AD.tpl zu verwenden. Letzteres bleibt gültig für die R-Domäne.

1.2 Änderungen beim Aufruf der ScanPC.exe

Bisher wird die ScanPC.exe typischerweise über eine Group Policy beim Hochfahren des PCs aufgerufen. In der IT-Cloud ergeben sich hier folgende Besonderheiten:

Auf sog. „Standardarbeitsplätzen“ können keine bankindividuellen Programme gestartet werden, auch nicht per Group Policy. Daher ist dort der Aufruf der ScanPC.exe nicht möglich. Allerdings ist der Einsatz dort auch kaum notwendig, da die Arbeitsplätze ohnehin nicht verändert werden können.

Auf „Erweiterten Arbeitsplätzen“ dagegen ist der Einsatz möglich. Dort ist wie bei jeder Anwendung eine entsprechende Ausnahme im AppLocker einzutragen.

Ein zusätzliches Problem ergibt sich allerdings, wenn die Programmdateien und/oder die Scanergebnisse auf Servern der IT-Cloud abgelegt werden sollen: Wird der Scan beim Hochfahren des PCs gestartet, so läuft er mit den Berechtigungen des lokalen Systemaccounts und Zugriffe ins Netzwerk finden mit den Berechtigungen des Computeraccounts statt. Entsprechend muss auf das Programm- bzw. Scandatenverzeichnis die Gruppe Domänencomputer Lese- bzw. Änderungsrechte erhalten. Das ist in der IT-Cloud nicht möglich.

Als Workaround kommen drei Alternativen in Frage:

1. ReDoKS Programm- und Scandaten auf einen Server außerhalb der IT-Cloud verlegen (sofern verfügbar)
2. Die ScanPC.exe nicht beim Hochfahren des PCs, sondern bei Anmeldung des Benutzers starten (entsprechende Änderung der Group Policy). Dann läuft der Scan und der Netzwerkzugriff mit den Rechten des angemeldeten Benutzeraccounts. Für den standardmäßig konfigurierten Scanumfang sind normale Benutzerrechte ausreichend (nur falls lokale Dateien/Zugriffsrechte erfasst werden sollen reichen diese ggf. nicht mehr aus).
   Anmerkung:
   Der Aufruf der ScanPC.exe kann dann um den Parameter /i:1 ergänzt werden. Dieser sorgt dafür, dass der Scan nur ausgeführt wird, wenn der letzte Scan mindestens 1 Tag alt ist. Dadurch wird vermieden, dass der Scan bei mehrmaligem Anmelden im Laufe eines Tages jedes Mal wiederholt wird.
3. Eine gesonderte Group Policy bei Anmeldung des Benutzers einsetzen, welche die benötigten Programmdateien lokal kopiert und das lokal abgelegte Scanergebnis ins Netzwerk kopiert. Der Aufruf der ScanPC.exe in der Group Policy beim Hochfahren des PCs ist dann so abzuändern, dass der Start vom lokalen Speicherort erfolgt und das Scanergebnis ebenfalls lokal (zwischen)gespeichert wird. Das ist weniger elegant als die vorausgehend geschilderten Alternativen, aber notwendig, wenn weder ein Server außerhalb der IT-Cloud zur Verfügung steht noch normale Benutzerrechte für den gewünschten Scanumfang ausreichen.

1.3 Neue Version der ScanAD.exe

Die ScanAD.exe dient zum Scan der Active Directory Domäne und der Zugriffsrechte auf Serververzeichnisse. Aus technischen Gründen kann die IT-Cloud-Domäne der FIDUCIA mit der bisherigen Version der ScanAD.exe allerdings nur von einem Arbeitsplatz aus gescannt werden, der Teil der IT-Cloud-Domäne ist (z.B. ein PaaS-Server).

Die neu verfügbare ScanAD.exe dagegen unterliegt solchen Beschränkungen nicht. Beliebige Domänen (z.B. R-Domäne oder IT-Cloud-Domäne der FIDUCIA, bn-its Domänen oder sonstige bankindividuelle Domänen) können damit gescannt werden. Der Arbeitsplatz auf dem der Aufruf der ScanAD.exe erfolgt muss nicht zu der gescannten Domäne gehören.

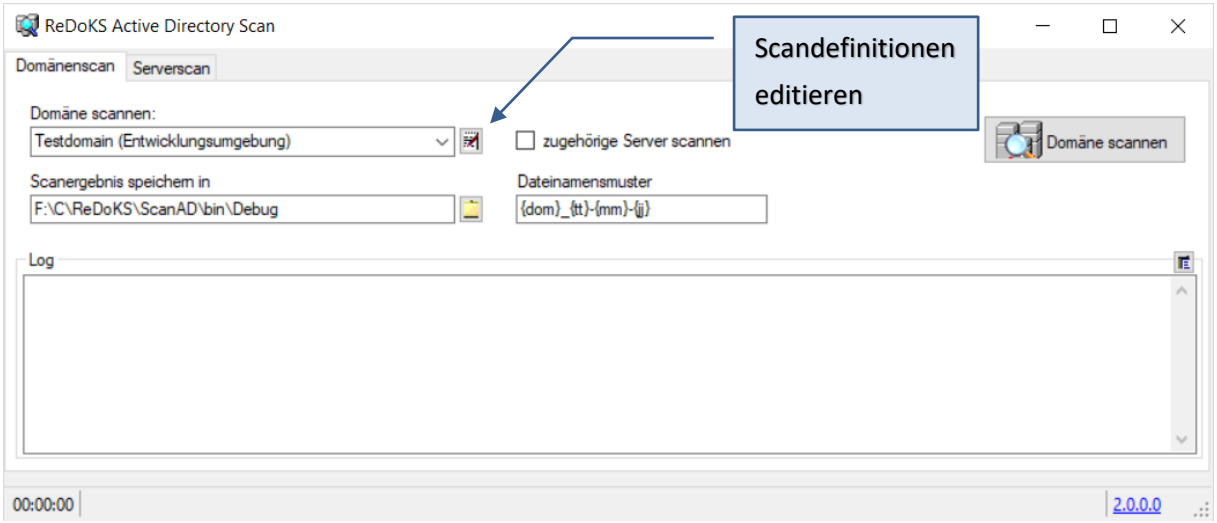
Die zu scannenden Domänen müssen allerdings in der Scankonfiguration der ScanAD.exe hinterlegt werden.

Anmerkung:
Für eine Übergangszeit wird die alte Version der ScanAD.exe noch unter dem Namen ScanAD_alt.exe im Verteilpaket enthalten sein.

1.4 Active Directory Domänen scannen (ScanAD.exe)

1.4.1 Scankonfiguration

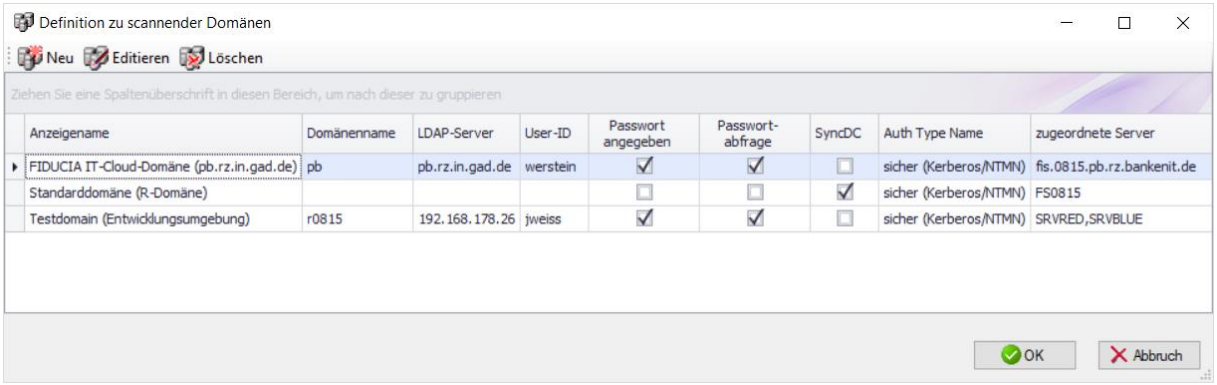
Die zu scannenden Domänen müssen zunächst in der Scankonfiguration hinterlegt werden.



In der Konfiguration werden Einträge für die FIDUCIA R-Domäne und die IT-Cloud-Domäne bereits automatisch angelegt.

Der Eintrag für die IT-Cloud muss für einen funktionierenden Scan aber noch ergänzt werden: **Hier ist eine User-ID mit Kennwort einzutragen**, mit welcher der Scan durchgeführt werden soll (d.h. dieses Account muss in der IT-Cloud existieren).

Die vordefinierten Einträge können nach Belieben ergänzt, verändert oder gelöscht werden. Die Speicherung der Scankonfiguration erfolgt in der Datei *DomDefs.ini*. Löscht man diese Datei, so werden beim nächsten Start die Standardeinträge wieder angelegt.



Für jeden Konfigurationseintrag können folgende Einstellungen festgelegt werden:

Einstellung	Erläuterung
Domänenname	Bezeichnung in der Domänenauswahl
LDAP-Server	Der Name der zu scannenden Domäne oder eines Domain Controllers/LDAP-Servers der Domäne. Falls die DNS-Namensauflösung für diese Namen nicht funktioniert kann auch die IP-Adresse eines Servers direkt angegeben werden. Fehlt der Eintrag, so wird die Domäne gescannt, zu welcher der Arbeitsplatz gehört auf dem der Scan läuft.
Domänenname	(NetBios-)Name der Domäne (z.B. ‚pb' oder ‚R0815'. Fehlt die Angabe, so wird die Standarddomäne des Arbeitsplatzes verwendet.
User-ID	Benutzer-Account, mit dem die AD-Abfrage durchgeführt wird. Dieses Account muss aus der gescannten Domäne stammen oder aus einer Domäne, die über eine Vertrauensstellung mit der gescannten Domäne verbunden ist. Fehlt der Eintrag, so wird der Scan mit den Rechten des angemeldeten Benutzers durchgeführt.
Passwort	Zugehöriges Kennwort zur angegebenen User-ID. Das Kennwort wird nicht angezeigt und verschlüsselt gespeichert
Passwort abfragen	Bestimmt, ob das User-ID und Kennwort vor jedem Scan abgefragt werden sollen. Ggf. konfigurierte Werte werden dann als Vorgabewerte des Abfragedialogs verwendet. Diese Option ist insbesondere dann nützlich, wenn das verwendete Kennwort regelmäßig geändert werden muss. Anmerkung: Bei einem bedienerlosen Scan (Aufruf mit dem Parameter /nogui) wird die Option ignoriert.

Authentifikation	Wenn Sie unsicher sind bei der Wahl der Authentifikationsmethode, dann treffen Sie keine Auswahl. Es wird dann die sichere Authentifikation über Kerberos/NTLM verwendet.
Sync DCs	Abgleich nicht replizierter Attribute über alle Domain Controller

Anmerkungen zum FIDUCIA-Umfeld

- Für die R-Domäne muss kein Eintrag bei LDAP-Server/Domäne/User-ID/Passwort erfolgen (die Arbeitsplätze der Bank sind Teil der Domäne und die Anmeldung erfolgt auch dort). Die Option zum Abgleich nicht replizierter Attribute sollte verwendet werden, da die R-Domäne mehrere Domain Controller enthält.
- Für die IT-Cloud-Domäne ist als LDAP-Server der Name der Domäne (pb.rz.in.gad.de) eingetragen, der über DNS-Auflösung in einen gültigen Servernamen aufgelöst wird, der NetBios-Domänenname ist ‚pb'. Es muss noch ein User-Account mit Kennwort aus der IT-Cloud-Domäne angegeben werden, da die Anmeldung am Bankarbeitsplatz in der R-Domäne erfolgt und keine Vertrauensstellung zwischen der R-Domäne und der IT-Cloud-Domäne besteht.

1.4.2 Active Directory Scan manuell durchführen

Bei Start der ScanAD.exe wird unmittelbar der Scandialog geöffnet. Dort sind folgende Bedienelemente verfügbar:

Element	Erläuterung
Domäne scannen (Schaltfläche)	Startet den Scan der ausgewählten Active Directory Domäne
Domäne scannen (Combobox)	Auswahl der zu scannenden Domäne. Die rechts angeschlossene Schaltfläche öffnet einen Editierdialog zur Verwaltung der Einträge (siehe Kapitel 1.4.1)
Zugehörige Server scannen	Regelt, ob im Anschluss an den Domänenscan automatisch die der gescannten Domäne zugeordneten Server ebenfalls gescannt werden sollen
Scanergebnis speichern in	Speicherverzeichnis für das Scanergebnis (standardmäßig das Programmverzeichnis). Die rechts angeschlossene Schaltfläche öffnet einen Verzeichnisauswahldialog. Anmerkung: Das Speicherverzeichnis kann auch über den Aufrufparameter /t gesetzt werden
Dateinamensmuster	Ermöglicht die Angabe eines Namensmusters für die Ergebnisdatei. Standardmäßig wird der Domänenname verwendet, was dazu führt, dass jeder Scan den vorangegangenen überschreibt. Ist dies nicht gewünscht, so kann ein Muster mit Datumsplatzhaltern verwendet werden. Zulässige Platzhalter sind *{dom}* - Domänenname *{tt}* - Tag des aktuellen Datums *{mm}* – Monat des aktuellen Datums *{jj}* –Jahr des aktuellen Datums

	Beispiel: „Scan_{tt}-{mm}-{jj}.dom“ erzeugt z.B. „Scan_23-01-2019.dom“ Anmerkung: Das Dateinamensmuster kann auch über den Aufrufparameter /f gesetzt werden (wenn Leerzeichen darin vorkommen, muss der Wert aber in Anführungszeichen gesetzt werden, etwa /f:“Scan {dom}“). Außerdem ist zu beachten, dass das Dateinamensmuster keine in Dateinamen unzulässigen Zeichen (z.B. „\“ oder „:“) enthalten darf.

Über die Schaltfläche „Domäne scannen“ wird der Domänenscan ausgelöst. Der Scanverlauf wird in einem Textlog protokolliert. Das Verlaufslog wird auch automatisch in Dateiform gespeichert (der Dateiname entspricht dem der Scandatei mit der Endung *.log).

1.4.3 Active Directory Scan automatisiert durchführen

Der Active Directory Scan kann auch bedienerlos erfolgen – dazu müssen vom Standard abweichende Einstellungen per Aufrufparameter eingestellt werden. Ein Scan per Skriptaufruf ist beispielsweise für die Erstellung turnusmäßiger Scans für Vergleichs- oder Dokumentationszwecke hilfreich.

Der Aufrufparameter /nogui unterdrückt die Graphische Benutzeroberfläche und führt den Scan bedienerlos aus. Mit /dom:{Domänenname} wird die zu scannende Domänenkonfiguration ausgewählt (es werden alle Domänen gescannt, in deren Konfigurationsname der angegebene Begriff vorkommt.

Wenn etwa die die Domänen „FIDUCIA IT-Cloud-Domäne“ und „Standardomäne (R-Domäne)“ definiert sind, dann kann die Auswahl z.B. mit /dom:IT-Cloud oder /dom:R-Domäne erfolgen. Ein Aufruf mit /dom:domäne scannt beide Domänen (und /dom:* scannt stets alle definierten Domänen).

Eine vollständige Auflistung der Parameter finden Sie im Anhang (siehe Kapitel 2.1.1).

Beispielaufrufe:

```
// alle definierten Domänen scannen
ScanAD.exe /nogui /dom:*

// IT-Cloud-Domäne scannen
ScanAD.exe /notui /dom:it-cloud

// zusätzlich Speicherverzeichnis (Q:\Scans) und Dateimuster angeben
ScanAD.exe /nogui /t:Q:\Scans /f:Scan_{mm}-{jj}.dom
```

Beachten Sie, dass beim bedienerlosen Scan keine Passwortabfrage erfolgt, auch wenn diese für die gescannte Domäne konfiguriert ist.

1.5 Zugriffsrechte auf Serververzeichnisse scannen (ScanAD.exe)

1.5.1 Scankonfiguration

Der Scan von Zugriffsrechten auf Serververzeichnisse erfolgt in der Rubrik *Serverscan* der ScanAD.exe.

Ähnlich wie beim Domänenscan muss auch hier eine Konfiguration für jeden Server angelegt werden. Folgende Konfigurationseinträge sind vorzunehmen:

Einstellung	Erläuterung
Servername	Der Name des Servers (ohne vorangestellter Doppelbackslash), also z.B. „FS0815“ oder „fis0815-pb.rz.bankenit.de“
Zugehörige Domäne	Name der Domänenkonfiguration der Domäne, zu welcher der Server gehört. Diese Angabe ist wichtig, wenn für den Scan der Domäne bzw. der zugehörigen Server die konfigurierte User-ID mit Passwort verwendet werden soll oder wenn mit der Domäne auch die zugeordneten Server gescannt werden sollen.
Freigabename mit Verzeichnistiefe	Es sind die zu scannenden Freigaben (Shares) des Servers anzugeben (z.B: „C$“, „GROUPDATA“ oder „inst_0815“) zusammen mit der Verzeichnistiefe. Die Verzeichnistiefe gibt die Anzahl der Verzeichnisebenen unterhalb der Freigabe selbst an, für welche Zugriffsrechte ermittelt werden. Eine hohe Verzeichnistiefe lässt die Scandaten stark anwachsen und ist nur sinnvoll, wenn in der entsprechenden Verzeichnisebene auch tatsächlich noch Zugriffsrechte administriert werden. In der Regel sollte eine Verzeichnistiefe von 2-3 ausreichend sein.
Für den Scan vorselektieren	Gibt an, dass der betreffende Server bei Programmstart für den Scan vorausgewählt ist (d.h. bei Klick auf „Server scannen“ wird er im Scan eingeschlossen, wenn die Auswahl nicht verändert wurde.

Die Speicherung der Scankonfiguration erfolgt in der Datei *SrvDefs.ini*.

1.5.2 Serverscan manuell durchführen

Zur manuellen Durchführung eines Serverscans sind zunächst in der Rubrik „Serverscan“ die gewünschten Server in der Liste auszuwählen. Die Standardauswahl der Server nach Programmstart wird durch die Option „für den Scan vorselektieren“ in der Scankonfiguration der Server festgelegt.

Über die Schaltfläche „Server scannen“ wird der Scan dann ausgelöst. Ist für einen Server die zugehörige Domänenkonfiguration spezifiziert, so erfolgt der Scan mit den dort hinterlegten Angaben (User-ID/Passwort, ggf. Passwortabfrage). Ansonsten wird mit den Berechtigungen des angemeldeten Benutzers gescannt.

Das Scanergebnis wird in einer Datei mit dem Namen des Servers und Endung „*.srv“ im angegebenen Scanverzeichnis gespeichert.

Der Scanverlauf wird in einem Textlog protokolliert. Das Verlaufslog wird auch automatisch in Dateiform gespeichert (der Dateiname entspricht dem der Scandatei mit der Endung *.log).

Treten werden des Scans Fehler auf, so werden diese nicht nur im normalen Verlaufslog, sondern zusätzlich in der Scanstatus-Statistik angezeigt. Durch Klick auf die (rote) Fehlerzahl oder die Schaltfläche „Error-Log anzeigen“ in der rechten oberen Ecke des Verlaufslogs kann ein gesonderter Dialog zur Fehleranzeige geöffnet werden.

Typische Fehlerursache sind z.B. mangelnde Zugriffsrechte auf einzelne Verzeichnisbereiche etc.

1.5.3 Serverscan automatisiert durchführen

Wie der bedienerlose Domänenscan wird auch der Serverscan über Parameter gesteuert. Der Aufrufparameter /nogui unterdrückt die Graphische Benutzeroberfläche und führt den Scan bedienerlos aus. Mit /srv:{Server1,Server2…} werden die zu scannenden Server angegeben.

Diese können entweder explizit aufgeführt werden oder es können mit „/srv:*“ alle Server bzw. mit „/srv:+“ alle für den Scan vorselektierten Server ausgewählt werden.

Eine vollständige Auflistung der Parameter finden Sie im Anhang (siehe Kapitel 2.1.1).

Beispielaufrufe:

```
// alle definierten Server scannen
ScanAD.exe /nogui /srv:*

// nur Server FS0815 und FS2301 scannen
ScanAD.exe /nogui /srv:fs0815,fs2301

// eine Domäne und vorselektierte Server scannen
ScanAD.exe /nogui /dom:R0815 /srv:+
// eine Domäne und die dieser Domäne zugeordneten Server scannen
ScanAD.exe /nogui /dom:R0815 /srv:#
```

2 Anhang

2.1 Aufrufparameter

2.1.1 Aufrufparameter ScanAD.exe

Parameter	Erläuterung
nogui	Unterdrückt die Anzeige der Bedieneroberfläche für automatisierte Ausführung
t:<zielverzeichnis>	Zielverzeichnis, in dem die Datei mit dem Scanergebnis erzeugt werden soll. Das Verzeichnis muss existieren, Umgebungsvariablen werden aufgelöst.
f:<muster>	Gibt ein Dateinamensmuster für die Benennung der Datei mit dem Scanergebnis an. Dabei können folgende Variablen verwendet werden: {dom}=Domänenname {jj}=Jahr {mm}=Monat {tt}=Tag
dom:<domäne>	Angabe der Domänenkonfiguration, die gescannt werden soll. Es werden alle Domänen gescannt, deren Konfigurationsname den angegebenen Begriff enthält. Die Angabe von * scannt stets alle konfigurierten Domänen.
srv:<Srv1,Srv2…|*|+|#>	Angabe der Server, die gescannt werden sollen. Die Server müssen bereits konfiguriert sein. Es sind entweder die einzelnen Server aufzuzählen oder diese Kürzel zu verwenden: * = alle Server + = alle für den Scan vorselektierten Server # = alle den gescannten Domänen zugeordneten Server
?	Eine Hilfe mit gültigen Parametern anzeigen