Integration von ADFS mit DoubleClue als Provider für Multi-Faktor-Authentifizierung (MFA)

1. Einführung

Diese Dokumentation ist für Nutzer von Microsoft ADFS gedacht, die eine DoubleClue-Authentifizierung als zweiten Faktor zur Anmeldung an Webapplikationen, die mit ADFS authentifiziert werden, hinzufügen möchten.

Anforderungen:

- Installation von ADFS 4 auf einem Windows Server.
- Eine Installation des DoubleClue Enterprise Management-Systems (DCEM) mit einer Benutzergruppe, die von derselben Active Directory-Instanz des Domain-Controllers importiert wurde, welchen der ADFS-Server verwendet.

⚠ Bitte beachten Sie: DCEM verwendet REST Web-Services für die Kommunikation, deshalb sollte es idealerweise im selben internen Netzwerk wie der ADFS-Server installiert werden.

2. Einrichtung des ADFS MFA-Provider-Plugins

DoubleClue kann mittels eines speziellen MFA-Provider-Plugins, das mit einer laufenden Instanz von DCEM kommuniziert, als zusätzlicher Faktor zu ADFS-Logins eingerichtet werden.

Kopieren Sie den Ordner “adfs” aus dem Ordner “DcemInstallation” an einen Ort auf Ihrem ADFS-Server.

2.1 Konfiguration

Zuerst müssen Sie die Konfigurationsdatei einrichten.

1. Öffnen Sie im Ordner “adfs”, den Sie gerade kopiert haben, die Datei “dcAdfsMfaProvider_config.json” mit einem Texteditor Ihrer Wahl. Die Inhalte dieser Datei sollten folgendermaßen aussehen:

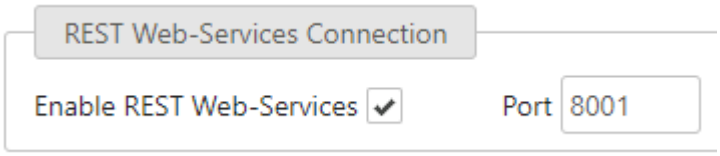
```
{
    "restApiUrl": "https://dcem_server:8001/dcem/restApi/as",
    "restOperatorName": "RestServicesOperator",
```

```
        "restPassword": "test",
        "restConnectionTimeout": 5000,
        "messageResponseTryDuration": 1,
        "messageResponseMaxTries": 120
}
```

2. Ändern Sie den Wert bei “restApiUrl” in eine zugängliche URL der REST-Services Ihrer DCEM-Installation. Das Format sollte sein:

   ```
   <Base URL of DCEM server>:<REST port number>/dcem/restApi/as
   ```

   Sie finden die REST-Portnummer, indem Sie sich in DCEM einloggen und zum Hauptmenüpunkt “System”, Untermenü “Cluster-Konfiguration” navigieren. Hier finden Sie die Einstellungen für die REST-Verbindung.



3. Falls Sie die Anmeldedaten des REST-Services-Operators von DCEM geändert haben, müssen Sie die Werte bei “restOperatorName” und “restPassword” ebenfalls verändern. Sie können die entsprechenden Werte finden, indem Sie sich bei DCEM einloggen und zum Hauptmenüpunkt “Administration”, Untermenü “Operatoren” navigieren. Suchen Sie nach dem Operator mit der Rolle “RestServices”.

4. Optional können Sie die anderen Konfigurationseinstellungen nach Belieben verändern.
   - restConnectionTimeout: Wie lange (Zeitangabe in Millisekunden) auf eine erfolgreiche Verbindung mit dem REST-Service gewartet werden muss, bis eine Zeitüberschreitung ausgegeben wird.
   - messageResponseTryDuration: Wie lange (Zeitangabe in Sekunden) zwischen Pings von Statusmeldungen gewartet werden muss.
   - messageResponseMaxTries: Wie viele Male eine Meldung gepingt wird, bevor eine Zeitüberschreitung angezeigt wird.

5. Speichern und schließen Sie die Datei.

2.2 Installation des MFA-Provider-Plugins

1. Öffnen Sie Windows PowerShell als Administrator.
2. Navigieren Sie zum Setup-Ordner, indem Sie “cd” verwenden.
3. Führen Sie “.\Install.ps1” aus.
4. Warten Sie, bis das Setup beendet ist (dies kann bis zu einer Minute dauern).

⚠ Bitte beachten Sie: Durch das Setup wird der ADFS-Service neu gestartet, stellen Sie also sicher, dass es zu einer Zeit ausgeführt wird, in der es kein Problem darstellt, dass der Service einige Sekunden lang nicht verfügbar ist.

Wenn alles korrekt eingerichtet wurde, wird jedes Mal, wenn ein Benutzer sich via ADFS einzuloggen versucht, ein sekundärer Screen angezeigt, in welchem der Benutzer gebeten wird, einen Code mit seiner DoubleClue App zu bestätigen. Sichere Meldungen, die an Benutzergeräte gesendet werden, verwenden die “adfs.login”-Vorlage.

Wenn Sie weitere Änderungen an den Textquellen oder der Konfigurationsdatei vornehmen möchten, müssen Sie dieses Setup erneut ausführen, damit die Änderungen wirksam werden. Bitte bewahren Sie Ihre Kopie der Installationsdateien für einen möglichen zukünftigen Gebrauch auf.

2.3 Textquellen (Optional)

In “adfs/resources” können Sie die Textdateien für Englisch (“en.txt”), Deutsch (“de.txt”) und Französisch (“fr.txt”) finden. Diese werden als Quellen für angezeigten Text während der Authentifizierung mit DoubleClue verwendet.

Sie können diese verändern, wie Sie möchten, sodass Sie den Erfordernissen Ihrer Firma genügen. Des Weiteren können Sie neue Sprachen hinzufügen, indem Sie einfach mehr Textdateien hinzufügen und dabei dieselben Schlüssel verwenden. Alle neuen Textdateien müssen mit ihren entsprechenden Kultur-Codes benannt werden. Eine vollständige Liste von Kultur-Codes, die von Microsoft unterstützt werden, finden Sie auf https://msdn.microsoft.com/en-us/library/hh441729.aspx

Veränderungen werden erst wirksam, nachdem Sie das MFA-Provider-Plugin neu installiert haben. Wenn das nicht funktioniert, könnte es nötig sein, den gesamten Server neu zu starten und dann das Plugin nochmals zu installieren. Dies ist unglücklicherweise eine Einschränkung von ADFS, für die es zum jetzigen Zeitpunkt keine andere bekannte Lösung gibt.

2.4 Veränderung des Identity Claims (Optional)

Standardmäßig identifiziert der DoubleClue-MFA-Provider Benutzer von DoubleClue anhand ihres “SAM-Account-Name” (a.k.a. Windows Account Name), weshalb Sie, wenn Sie Benutzer von LDAP in DCEM importieren, sicherstellen sollten, dass Sie diese Eigenschaft als deren Login-ID verwenden.

Sollte diese jedoch, aus welchen Gründen auch immer, geändert werden, ist es möglich, einzustellen, welche Eigenschaft der MFA-Provider verwendet, um Benutzer zu identifizieren, sodass sie zur importierten Gruppe in DCEM passt.

Um dies zu tun, öffnen Sie “regedit” und suchen Sie nach:

“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DcAdfsMfaProvider”

Innerhalb gibt es einen String-Schlüssel, der “LoginAttribute” heißt. Dessen Wert kann zu einem der folgenden verändert werden:

- `http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn`
- `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
- `http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid`

Unglücklicherweise unterstützt ADFS nur eine von diesen vier Optionen als Identity Claims für MFA-Provider, es ist also zum jetzigen Zeitpunkt nicht möglich, andere Attribute zu verwenden.

Veränderungen werden erst wirksam, nachdem Sie ADFS neu gestartet haben. Wenn das nicht funktioniert, könnte es nötig sein, den gesamten Server neu zu starten und dann ADFS nochmals neu zu starten. Dies ist unglücklicherweise eine Einschränkung von ADFS, für die es momentan keine andere bekannte Lösung gibt.