Vorbereitungen für Office 365

Den Weg ebnen

von Florian Frommherz

Bevor Office 365 in Betrieb gehen kann, sind einige vorbereitende Tätigkeiten zu erledigen. Denn damit die Anwender den Cloud-Dienst nahtlos nutzen können, muss dieser möglichst gut in die bisherige Infrastruktur eingegliedert werden. Dazu gehören sowohl die Domänen als auch die saubere Übernahme der Active-Directory-Daten.

Quelle: bogdanhoga – 123RF

Das Office-365-Abo enthält eine Reihe von Software-as-a-Service (SaaS)-Angeboten für Kunden. Die prominentesten sind Exchange als E-Mail-System, SharePoint für Kollaboration und Informationsspeicherung und Skype for Business für Echtzeitkommunikation und Telefonie. Abhängig von den genutzten Komponenten fällt die Konfiguration des Cloud-Dienstes einfacher oder etwas umfangreicher aus. Wer Office-Anwendungen wie Planner, Sway oder den Store for Business für Windows 10 verwenden will, muss in den meisten Fällen zumindest die Synchronisation von Benutzerkonten und Lizenzverwaltung betreiben.

Domänen registrieren

Einer der wichtigsten Schritte für Exchange Online und Skype for Business, aber auch wenn Benutzer Single Sign-on (SSO) mit ihrem Active-Directory-(AD)-Passwort durchführen können sollen, ist die Registrierung der Firmendomäne mit Office 365 und Azure AD. Exchange muss schließlich wissen, in welchem Namen und für welche Domänen E-Mails empfangen und verschickt können werden sollen. Die Empfangs- und Sendedomänen müssen also im Voraus bekannt sein.

Greifen Mitarbeiter mit ihrem Browser oder einem Client wie Outlook auf Online-Ressourcen zu, möchte Azure AD zusammen mit Office 365 zuerst eine erfolgreiche Authentifizierung durchführen. Sofern der Mitarbeiter keinen Cloud-Account nutzt, sondern seinen Benutzeraccount und das Passwort aus der Windows-AD-Domäne, muss Azure AD einen Hinweis auf die Heimatdomäne und das Heimat-AD des Nutzers erhalten – Microsoft nennt das "Home Realm Discovery". Für Office 365 und Azure AD ist dieser Hinweis der Domänenname, unter dem das Unternehmen zu erreichen ist. Im Bestfall deckt sich die Domäne auch mit dem UPN-Anmeldenamen des Benutzers im Windows-AD.

Damit Azure AD den Login an die richtige Stelle weiterleiten kann und Exchange Online weiß, für welche Domänen Senden und Empfangen möglich sein soll, registrieren Administratoren alle relevanten DNS-Domänen im Azure AD. Der Prozess ist dabei einfach: Sie geben die DNS-Domäne im Azure AD an und starten den Verifikationsprozess. Azure AD verlangt dann das Eintragen eines DNS-Textes auf Root-Ebene für jede Domäne. Dieser Eintrag ist zufällig. Existiert er, kann Azure AD sicher sein, dass die Domäne tatsächlich Ihnen gehört – denn nur Sie als DNS-Admin der Domäne können einen solchen Eintrag anlegen.

Das Erstellen des TXT-Eintrages hat keinen Einfluss auf die anderen DNS-Einträge dieser Domäne und kann nach der Verifikation wieder entfernt werden. Bestehende Produktionsumgebungen für Exchange oder Skype werden nicht in Mitleidenschaft gezogen, da der TXT-Record keine Auswirkung auf die Funktion der Dienste hat. Hier geht es lediglich um die Bestätigung des Besitzes und den Zugriff auf die DNS-Konfiguration. Die Verifikation müssen Sie einzeln für jede neue Domäne durchführen, über die Benutzer authentifiziert oder später E-Mails versendet oder empfangen werden sollen. Subdomains werden einfach hinzugefügt, wenn die Hauptdomäne schon verifiziert wurde.

DNS-Records erstellen

Die Verifikation der öffentlichen, routbaren Domäne ist erforderlich, um Office 365 sinnvoll zu nutzen. Spätestens, wenn der E-Mail-Versand eine Rolle spielt, ist die Domäne entscheidend. Des Weiteren sollte die Domäne im Idealfall mit der AD-Domäne übereinstimmen, aus der die allermeisten Benutzer später synchronisiert werden – dann ist das Setup einfach. Lautet der First-Level-Domain-Teil anders, etwa bei contoso.net als AD-Domäne und contoso.com für Online Services, entstehen daraus Nachteile für einzelne Szenarien, was die User Experience anbelangt. Dazu später mehr.

Zunächst registrieren Sie also die Domäne. Im Office-365-Portal als "Globaler Administrator" angemeldet, starten Sie den Assistenten, indem Sie unter "Setup" auf den Punkt "Domains" klicken. "Add domain" startet den Assistenten. Zunächst geben Sie den Domänennamen an. Das System prüft, ob die Domäne bereits in einem anderen Azure AD verwendet wird. Ist das nicht der Fall, folgt der zweite Schritt: die Verifikation.

Die Verifikation der Domäne erfolgt wie schon erwähnt über das Erstellen eines DNS-Records, der vom Internet aus einzusehen ist. Damit kann Microsoft überprüfen, dass Sie als Administrator von Office 365 tatsächlich der Besitzer der Domäne sind – oder zumindest in der Firma arbeiten. Denn nur der Besitzer sollte in der Lage sein, den öffentlichen Namensraum der Domäne zu ändern. Möglich sind ein TXT- oder ein MX-Record. Dieser ist an oberster Stelle des Namensraums mit "@" und mit dem vom Portal angezeigten Wert anzulegen. Der komplette Wert inklusive des "MS" vor dem Gleichzeichen ist entscheidend. Die TTL ist dabei nicht ausschlaggebend. Mit Hilfe der PowerShell lässt sich die Domäne ebenfalls hinzufügen und die DNS-Records anfragen:

```
> New-MsolDomain -Authentication
  Managed -Name contoso.net
> Get-MsolDomainVerificationDns
  -DomainName contoso.net -Mode
  DnsTxtRecord

Label: contoso.net
Text: MS=ms99384745
TTL: 3600
```

Haben Sie den Eintrag erfolgreich im DNS erstellt, kann die Verifikation durch Office 365 via PowerShell oder per Klick auf "Verify" im Portal gestartet werden:

```
> Confirm-MsolDomain –DomainName
  contoso.net
```

Die weiteren Schritte nach der Verifikation setzen Office 365 korrekt auf und beschrieben die notwendigen Änderungen in DNS für Exchange Online und Skype for Business. Den Assistenten können Sie an dieser Stelle beenden.

Synchronisation aktivieren

Eine weitere anstehende Vorarbeit ist das Aktivieren der Verzeichnissynchronisation. Bevor Azure AD Connect seine Arbeit verrichten kann, müssen Sie die Synchronisierung erlauben. Die PowerShell im Admin-Modus ist hierfür die einfachste Methode:

```
> Set-MsolDirSyncEnabled
  -EnableDirSync $true
```

Unabhängig von der Zielkonfiguration für Azure AD Connect verwenden Sie das genannte Kommando, um das Verzeichnis für die Synchronisation zu aktivieren. Die Details der Synchronisierung definieren Sie später. Die Verzeichnissynchronisation wird mit demselben Kommando wieder deaktiviert – allerdings mit dem Wert "$false" als Parameter.

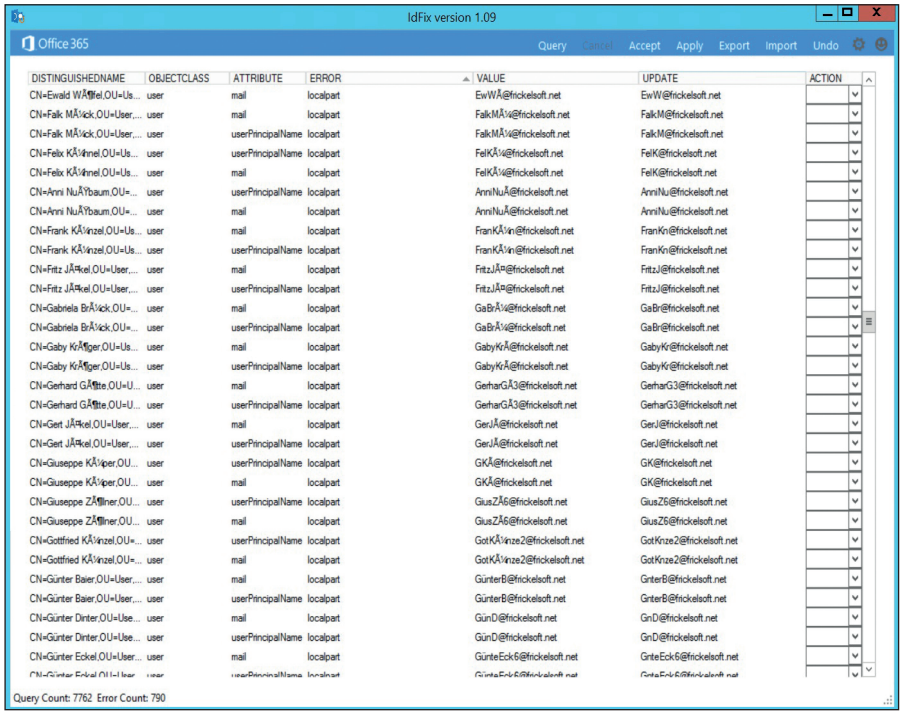
Lokale Identitäten bereinigen

Microsoft empfiehlt, vor der Synchronisation von Benutzer-, Gruppen- und Kontaktobjekten ein paar Bereinigungsmaßnahmen durchzuführen. Aus Erfahrung mit bisherigen Office-365-Kunden weiß Microsoft, dass die Datenreinheit in Windows-ADs nicht allerorts die Qualität hat, die die Cloud-Systeme gerne hätten. So benötigt Exchange Online beispielsweise eindeutige E-Mail-Adressen und kann Dubletten in einigen Attributen nur schwer verdauen.

Für das Windows-AD sind diese Doppelungen kein Problem, da das Verzeichnis bis auf wenige Attribute keine Einzigartigkeitsprüfung oder Syntaxprüfung durchführt. Überhaupt wird die Mehrzahl der Attribute im AD bei Objekterstellung nicht überprüft. Alles, was Betriebslogik darstellt und speziell formatierte Daten wie etwa Büroplatz, Telefonnummer oder E-Mail-Adresse darstellt, muss separat eingepflegt und erzwungen werden.

Mit steigender Anzahl an Objekten, die in die Cloud synchronisiert werden, bietet es sich an, zuvor eine Überprüfung der Objekte durchzuführen. Gerade bei Unternehmen, in denen die Objekterstellung nicht automatisiert stattfindet oder in denen Identity-Management-Systeme existieren, gibt es erfahrungsgemäß etwas mehr zu tun. Falls nicht-eindeutige Daten gefunden werden, lassen sich diese einfach vor dem Sync bereinigen. Das geht zwar später immer noch, aber wenn die Synchronisation Fehler um Fehler auswirft und einige Benutzer bereits in der Cloud arbeiten, andere wiederum nicht, kann das zur Unzufriedenheit beitragen. Zudem können Sie Ihre Cloud-Bereinigungen besser planen, wenn Sie möglichst frühzeitig wissen, welche und wie viele Objekte betroffen sind.

Microsoft stellt hierfür das Tool IdFix [1] zur Verfügung, das sich ohne Installation starten lässt. Generell ist das Werkzeug sowohl bei der Erkennung möglicher Pro-



Das IdFix-Bereinigungstool liest und prüft die AD-Daten auf Fehler vor der Synchronisation in die Cloud.

bleme hilfreich als auch – falls gewünscht – bei der Bereinigung. Das Tool liest das Verzeichnis aus und erstellt eine Übersicht, die dann exportiert und zur Weiterverarbeitung in einem anderen Tool genutzt werden kann.

Ist IdFix gestartet, überprüfen Sie die automatisch geladenen Einstellungen über das Zahnrad-Icon in der rechten, oberen Ecke. Wichtig ist, dass die Option "Multi-Tenant" und der richtige Active-Directory-Forest ausgewählt sind. Haben Sie das Tool als AD-Administrator gestartet, müssen Sie keine besonderen Benutzerdetails mehr angeben. Ansonsten geben Sie noch die nötigen Anmeldedaten an, wenn Sie das Tool auch zur Bereinigung und nicht nur zur Erstellung eines Berichts nutzen möchten.

Der Klick auf "Query" lädt Daten aus dem AD und analysiert die Objekte entsprechend der Regeln für Office 365. Die Ergebnisse in Form von potenziellen Fehlern sehen Sie direkt im Tool angezeigt. Die Statistik ist im unteren, linken Fensterrand abzulesen: die Anzahl der gelesenen Objekte und die gefundenen Probleme.

Problematische Objekte werden tabellarisch dargestellt. Neben dem Objektnamen, der Objektklasse und welches Attribut als Problem anerkannt wurde, schlägt IdFix auch gleich die mögliche Bereinigung vor – und wie das Attribut dann aussehen könnte. Mit einem Klick auf "Export" überführen Sie den Ergebnissatz in eine CSV-Datei.

In der letzten Spalte "Action" bestimmen Sie, was mit den einzelnen Ergebnissätzen passieren soll. Die vorgeschlagenen Änderungen von IdFix können Sie via "EDIT"-Auswahl aus der Auswahlliste markieren und später mit dem Schalter "Apply" übernehmen. "DELETE" löscht das Objekt aus dem Verzeichnis und sollte nur verwendet werden, wenn der Account nicht weiter zum Einsatz kommt.

Sind alle Vorschläge von IdFix in Ordnung und erscheinen nach einer manuellen Kontrolle akzeptabel, beschleunigt der Knopf "Accept" die Aufräumarbeiten. "Accept" übernimmt alle Änderungsvorschläge, die IdFix anzeigt und markiert alle Zeilen mit "EDIT", sodass der Admin nur noch auf "Apply" klicken muss. Nach Änderung der problematischen AD-Objektdaten sollte ein erneutes Ausführen von IdFix mit "Query" schnell Besserungen zeigen – natürlich nach Abwarten der AD-Replikation.

Saubere Datenhaltung

Mit steigender Anzahl der Nutzer, die vom Windows-AD ins Azure AD synchronisiert werden, wächst auch die Bedeutung eines guten Datenmanagements dieser Benutzerobjekte. Ganz klassisch regeln das die Identity-Management-Systeme, die in unterschiedlicher Ausprägung und Komplexität in Unternehmen existieren.

Welches Produkt eingesetzt wird, ist zweitranging – wichtig ist, dass im Windows-AD letztlich nur Änderungen aus bekannten Quellen auftauchen – und irgendwie sowohl die Geschäftslogik zu den wichtigen Attributen als auch die Delegation und Verwaltbarkeit im Tool abgebildet werden kann. Schließlich sollen trotz aller Datenreinheit weiterhin wichtige Operationen möglich sein.

Wichtig ist all das deshalb, weil Azure AD und dort integrierte Systeme die lokalen Objekte, sowohl Benutzer als auch Computer, für den Zugriff auf Daten und Ressourcen nutzen. Azure AD erkennt synchronisierte Objekte und erlaubt die Änderung einzelner Daten zu diesen Objekten nicht in der Cloud. Das gilt auch für einzelne Attribute, spätestens wenn die Delegation und Administration mit "Administrative Units" über Benutzer- oder Gruppenattribute aus dem Verzeichnis eingerichtet wird.

Fazit

Bevor Sie mit Office 365 und Co. loslegen können, sind ein paar Vorarbeiten zu erledigen. Zunächst sorgen Sie dafür, dass der Cloud-Dienst auf die passende Domäne zugreifen kann. Anschließend bereinigen Sie noch Ihren Verzeichnisdienst, denn Azure AD und integrierte Systeme sind auf korrekt formatierte und sinnvolle Daten aus dem Windows-AD angewiesen. Es ist sinnvoll, die Daten bereits im Windows-AD zu bereinigen und erst dann in die Cloud zu synchronisieren. *(dr)*

Link-Codes

[1] IdFix DirSync Error Remediation Tool
HS121