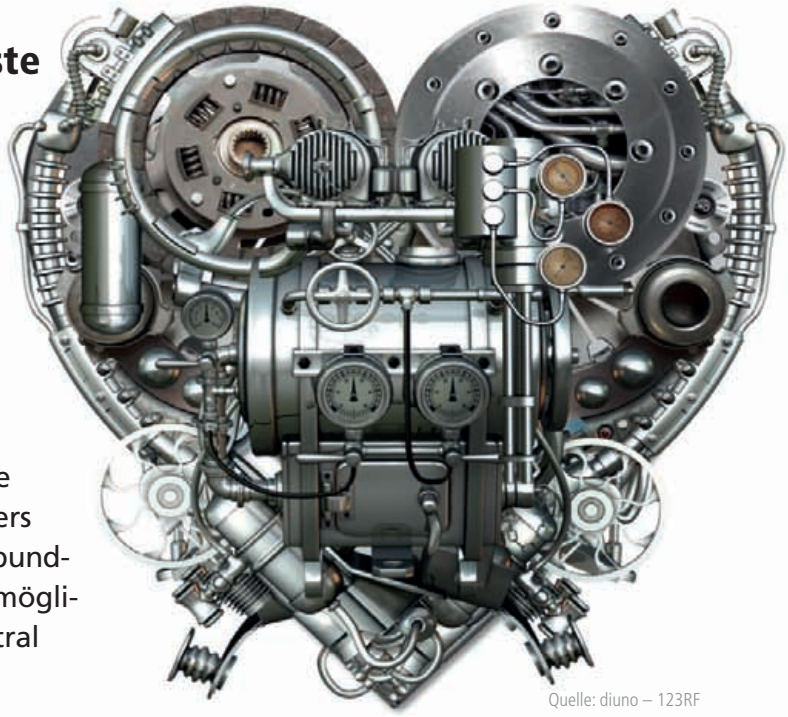
Active-Directory-Domänendienste, -Zertifikatdienste und -Verbunddienste

Im Herz des Servers



Quelle: diuno – 123RF

Umfangreiche Active-Directory-Neuerungen warten in Windows Server 2016 nicht auf den Administrator. Dennoch gibt es viele Bereiche, die erst durch die AD-Dienste funktionieren. Besonders wichtig werden in Zeiten mobiler Clients die Verbund- und Zertifikatdienste, die etwa Single Sign-on ermöglichen. Auch Themen wie die Replikation sind zentral für einen störungsfreien AD-Betrieb.

Eine der wichtigsten Neuerungen in Windows Server 2016 sind die Verbesserungen in den Active-Directory-Verbunddiensten (Active Directory Federation Services, ADFS). Hier ist es zum Beispiel möglich, eine Zugriffsteuerung auf Basis bestimmter Bedingungen zu konfigurieren. Und mit "Conditional Access Control" lassen sich vor allem mobile Anwender effizienter anbinden. Außerdem können Sie Rechner mit Windows 10 über die Geräteauthentifizierung an Windows Server 2016 anbinden.

Verbesserungen in ADFS

Windows Server 2016 erlaubt, auch Benutzerkonten in ADFS zu authentifizieren, die nicht aus dem Active Directory kommen. Beispiel dafür sind X.500-kompatible LDAP-Verzeichnisse oder auch SQL-Datenbanken (AD LDS, Apache DS, IBM Tivoli DS, Novell DS, Open LDAP und mehr). Passive Authentifizierungsmöglichkeiten wie SAML, OAuth, "WS-Trust Active Authorization Protocol" und WS-Federation sind ebenfalls möglich. Unter Windows Server 2016 lassen sich auch mehrere LDAP-Verzeichnisse mit einer ADFS-Farm verbinden.

Mit den Active-Directory-Verbunddiensten können Sie im Unternehmen eine zentrale Authentifizierungsinfrastruktur aufbauen, die Single-Sign-on-Szenarien zwischen verschiedenen Active-Directory-Gesamtstrukturen bietet, aber auch die Möglichkeit, Benutzer sicher für den Zugriff auf Office 365 und Microsoft Azure zu authentifizieren. Damit die Lösung stabil und sicher eingesetzt werden kann, müssen Sie einiges beachten.

Die grundlegende Installation von ADFS erfolgt über das Hinzufügen von Serverrollen im Server-Manager. Um eine ADFS-Infrastruktur optimal und sicher zu betreiben, benötigen Sie neben einer Active-Directory-Gesamtstruktur auch eine interne Zertifizierungsstelle, am besten auf Grundlage der Active-Directory-Zertifikatsdienste. Außerdem sollten Sie mit verwalteten Dienstkonten arbeiten, damit notwendige Systemdienste ihre Kennwörter selbst sicher und stabil verwalten und auch ändern können. Für ADFS verwenden Sie am besten ein gruppiertes verwaltetes Dienstkonto. Dieses legen Sie in der PowerShell an. Die Kommandos zum Anlegen des verwalteten Dienstkontos sehen für einen Server mit der Bezeichnung "s1.contoso.com" folgendermaßen aus:

```
Add-KdsRootKey -EffectiveTime
  (Get-Date).AddHours(-10)
New-ADServiceAccount adfsGmsa
  -DNSHostName s1.contoso.com
  -ServicePrincipalNames
  http/s1.contoso.com
```

Die Daten des angelegten Dienstkontos zeigen Sie mit

```
Get-ADServiceAccount adfsGmsa
```

an. Außerdem sollten Sie dem Server ein SSL-Zertifikat zuweisen. Haben Sie alle Vorbereitungen getroffen, installieren Sie ADFS als Serverrolle auf dem ADFS-Server. Dazu spielen Sie über "Verwalten / Rollen und Features hinzufügen" den Rollendienst "Active Directory-Verbunddienste" ein.

Während der Installation müssen Sie keine Einstellungen vornehmen, die eigentliche Konfiguration erfolgt nachträglich. Zunächst hinterlegen Sie nur den Namen der verwalteten Dienste. Stehen Kennwortänderungen an, können die Systemdienste diese Aktion selbst durchführen.

ADFS sicher einrichten

Nachdem die Installation abgeschlossen ist, richten Sie über das Benachrichtigungscenter des Server-Managers die Infrastruktur im Netzwerk über einen Assistenten ein: Bestätigen Sie die Startseite und geben Sie dann die Anmeldedaten eines Domänenadministrators ein. Wählen Sie auf der Seite "Diensteigenschaften

bearbeiten" das von Ihnen installierte Zertifikat. Als Anzeigenamen können Sie einen beliebigen Namen verwenden, zum Beispiel "ADFS Contoso".

Der erste Server, den Sie in der Farm installieren, ist automatisch der primäre Verbundserver. Alle nachfolgenden Verbundserver, die der Farm hinzugefügt werden, synchronisieren die Konfigurationsdaten vom primären Server. Die Daten werden anschließend in die lokale Konfigurationsdatenbank des Servers gespeichert.

Die anderen Server bleiben in Betrieb, wenn der primäre Server im Verbund ausfällt, aber diese Server sind nicht in der Lage, Änderungen an der ADFS-Konfiguration vorzunehmen, bis der primäre Verbundserver wiederhergestellt ist oder ein anderer Verbundserver als primärer Server heraufgestuft wird. Um einen sekundären Verbundserver zum primären heraufzustufen, führen Sie folgenden Befehl auf dem sekundären Server aus:

```
Set-AdfsSyncProperties
  -Role PrimaryComputer
```

Sobald Sie einen neuen Primärserver eingerichtet haben, müssen Sie die anderen sekundären Verbundserver mit dem neuen primären Verbundserver verbinden. Verwenden Sie dazu diesen Befehl, um auf den verbleibenden Farm-Mitgliedsservern die Synchronisierung zu starten und den neuen Server zu hinterlegen:

```
Set-AdfsSyncProperties -Role Secon-
  daryComputer -PrimaryComputerName
  FQDN des primären Verbundservers
```

Betreiben Sie im Netzwerk den System Center Operations Manager, können Sie für ADFS ein eigenes Management Pack herunterladen und auf diesem Weg ADFS überwachen. ADFS lässt sich aber auch über die Ereignisanzeige monitoren. In der ADFS-Konsole steuern Sie über das Kontextmenü von ADFS auf der Registerkarte "Ereignisse" genauer, was die Umgebung in die Ereignisanzeige schreiben soll.

Öffnen Sie die Ereignisanzeige, klicken Sie auf das Menü "Ansicht" und wählen Sie "Analytische und Debugprotokolle

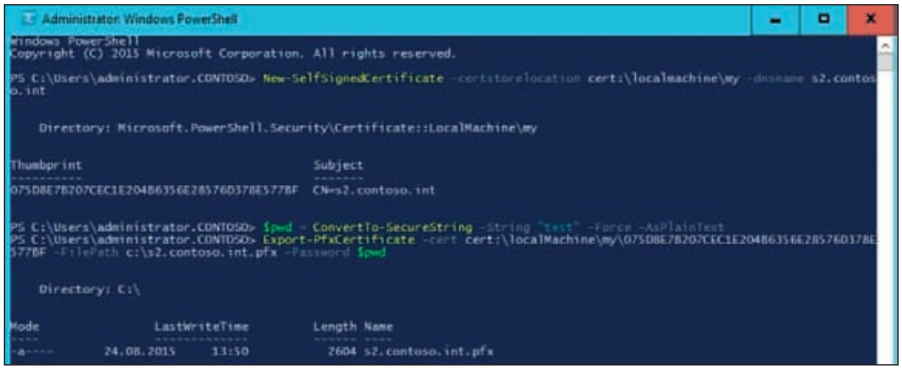


Bild 1: Zum Test verschiedener neuer Dienste wie ADFS reicht ein selbstsigniertes Zertifikat.

einblenden". Danach müssen Sie die Ansicht aktualisieren, damit das ADFS-Tracing-Log zu sehen ist. Mit einem Rechtsklick auf das Debug-Protokoll aktivieren Sie das Protokoll. Sobald dies erledigt ist, erhalten Sie einen umfassenden Überblick zu den Vorgängen in der ADFS-Infrastruktur. Das Filtern des ADFS-Ereignisprotokolls zeigt Ihnen beispielsweise alle Ereignisse einer bestimmten Transaktion. Sie müssen dazu nur einen Filter basierend auf der ActivityID erstellen, indem Sie zunächst die Ereignisanzeige öffnen. Dort erweitern Sie "Anwendungs- und Dienstprotokolle" und dann den Admin-Bereich beim ADFS-Protokoll. Wählen Sie aus dem Menü "Aktion" den Punkt "Aktuelles Protokoll filtern". Jetzt klicken Sie auf die Registerkarte "XML" und wählen "Manuell bearbeiten". Eine Beispielabfrage für ADFS sieht folgendermaßen aus:

```
<QueryList>
  <query Id="0" Path="AD FS 2.0
    Eventing/Admin">
    <Select Path=" AD FS 2.0/Admin
      "> * [System [ Correlation [@
      ActivityID = ' { 77269359 -
      0b7d - 45cb - 9760 -
      e3a4009883d9 }' ]]]
    </ select >
  < / Query >
</ Querylist >
```

Mit einer benutzerdefinierten Abfrage können Sie ADFS-Fehlermeldungen effektiver auslesen. Aus Gründen der Sicherheit zeigt ADFS nicht genau, wann ein Fehler aufgetreten ist oder eine Aktion durchgeführt wurde.

Fügen Sie den folgenden Schlüssel zu der Datei "web.config" hinzu, um benutzerdefinierte Fehler und Informationen anzuzeigen. Die Datei ist im Verzeichnis "C:\ InetPub \ Adfs \ ls" zu finden. Suchen Sie die Zeile "<system.web>" und fügen Sie den Eintrag "<customErrors mode= "Off" />" hinzu.

Sie können die Ereignisse aber auch in der PowerShell anzeigen und filtern lassen:

```
Get-WinEvent -FilterHashTable
  @{LogName='AD FS Admin'; Level=2;
  StartTime=(Get-Date) -Computername
  Servername
```

Für erweiterte Überwachung und Diagnosezwecke bietet Microsoft auch kostenlose PowerShell-Cmdlets zum Monitoring an. Sie können sich das "AD FS Diagnostics Module" [2] kostenlos in der TechNet-Gallery herunterladen.

Single Sign-on mit ADFS

Mit ADFS können Sie lokale und Cloud-Dienste wie Office 365 für Single Sign-On (SSO) konfigurieren. Anwender müssen sich in solchen Umgebungen nur einmal an der Weboberfläche von ADFS anmelden und können dann ohne weitere Anmeldungen auf Ressourcen in Office 365 und anderen Webdiensten zugreifen. Während der Installation von ADFS sollten Sie eine Verbundfarm erstellen. Auf diese Weise können Sie jederzeit weitere Server zum Verbund hinzufügen und so sicherstellen, dass die Infrastruktur hochverfügbar ist. Auch wenn Sie zunächst nur einen Server betreiben wollen, ist das Verwenden einer Farm immer der bessere Weg.

Als Alternative zur internen Datenbank können Sie auch eine SQL-Datenbank für ADFS verwenden. Dies erfordert einige

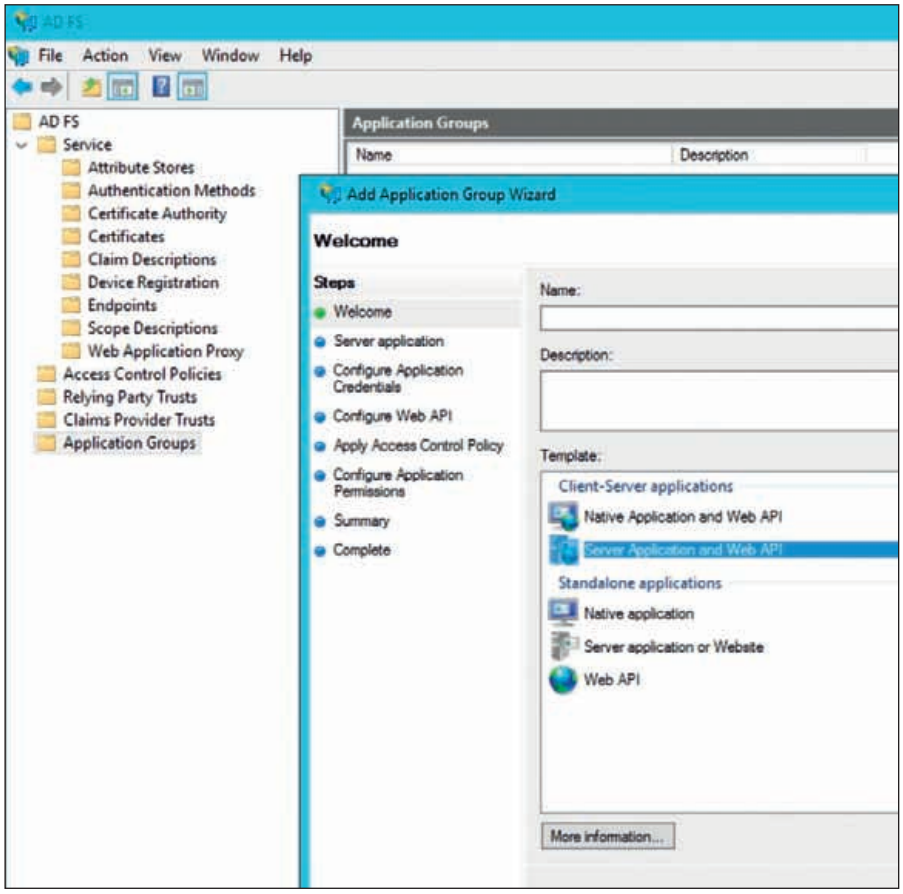


Bild 2: Über einen Assistenten richten Sie die ADFS-Authentifizierung ein, wodurch sich anschließend beispielsweise OpenID Connect nutzen lässt.

zusätzliche Arbeit beim Setup, aber Sie können SQL für hohe Verfügbarkeit nutzen. Außerdem gibt es keine primären oder sekundären ADFS-Server in der Farm, da alle Daten in der SQL-Datenbank gespeichert werden. Wenn Sie bereits SQL im Unternehmen einsetzen und eine SQL-Infrastruktur zur Verfügung haben, bietet es sich an, diese zu nutzen. Dies bedeutet auch, dass Sie mehr als fünf Server in einer Farm und zusätzliche ADFS-Funktionen wie SAML integrieren können.

ADFS unterstützt für SSO zudem OpenId Connect Web Sign On sowie OAuth2. Um ADFS oder auch andere neue Dienste in Server 2016 umfassend zu nutzen, sind Zertifikate notwendig. Ein soches lässt sich selbstsigniert ganz einfach in der PowerShell erstellen:

```
New-SelfSignedCertificate -certsto-
  relocation cert:\localmachine\my
  -dnsname FQDN des Servers
```

Auf Basis des Fingerabdruckes können Sie das Zertifikat in eine Datei exportieren. Dazu speichern Sie das notwendige Kennwort für das Exportieren als Variable:

```
$pwd = ConvertTo-SecureString
  -String "test" -Force -AsPlainText
```

Danach exportieren Sie das Zertifikat auf Basis seines Thumprints:

```
Export-PfxCertificate -cert
  cert:\localMachine\my\075D8E7B207C
  EC1E204B6356E28576D378E577BF
  -FilePath c:\s2.contoso.int.pfx
  -Password $pwd
```

Anschließend arbeiten Sie den Assistenten zum Erstellen einer neuen ADFS-Konfiguration durch. Als Zertifikat verwenden Sie das selbstsignierte. Natürlich können Sie auch auf Zertifikate aus den AD-Zertifikatdiensten von Server 2016 setzen. Nachdem ADFS eingerichtet ist, starten Sie in der ADFS-Verwaltungskonsole über "Application Groups" den Assistenten zum Einrichten des Single Sign-on. Dieser bietet einige Vorlagen und ermöglicht die Einrichtung von OpenId Connect.

Kennwörter und Identitäten schützen

Windows Server 2016 macht es Angreifern schwerer, mit Pass-the-Hash-Angriffen (PtH) an vertrauliche Anmeldedaten von Administratoren zu gelangen. PtH-Angriffe zielen nicht auf die Kennwörter ab, sondern auf die Hashes, die im Active Directory erzeugt werden, nachdem sich ein Benutzer authentifiziert hat. In diesem Zusammenhang bietet Windows Server 2016 "Privileged Access Management" (PAM) [3] und "Microsoft Identity Manager" (MIM) [4]. Dabei wird eine neue Active-Directory-Gesamtstruktur mit MIM erstellt und mit PAM geschützt.

In diesem Zusammenhang spielt auch Microsoft Passport [5] eine wichtige Rolle. Dieser Dienst für schlüsselbasierte Authentifizierung geht über die Anmeldung mit herkömmlichen Kennwörtern weit hinaus. Die Anmeldung mit Passport kann entweder zertifikatbasiert stattfinden oder über eine PIN. Letztere wird in Zusammenhang mit dem Trusted Plattform Module (TPM) auf Rechnern genutzt, genauso wie für die Verwendung bei BitLocker. Für die Anmeldung über Microsoft Passport an Domänen mit Windows Server 2016 lassen sich auch biometrische Funktionen wie Fingerabdruckscanner oder die neue Hello-Funktion in Windows 10 nutzen. Die Anmeldung mit Microsoft Passport ist vor allem für mobile Anwender mit Notebooks interessant.

Microsoft Passport ermöglicht SSO-Szenarien und die Authentifizierung ohne Kennwörter. Das funktioniert für das AD, aber auch für Microsofts Cloud-Dienste und andere Anmeldebereiche. Microsoft hat dazu auch einige neue Schema-Attribute in das AD integriert.

Admin auf Zeit

Um PAM mit Windows Server 2016 einzusetzen, sind zwei Active-Directory-Gesamtstrukturen notwendig, die Sie über eine Vertrauensstellung verbinden. Die Administratorenkonten sind in einer solchen Infrastruktur von der produktiven Domäne getrennt. Die Gesamtstruktur mit den Administratorkonten wird auch als "Bastion Active Directory Forest" bezeichnet. Er wird durch den

Microsoft Indentity Manager zur Verfügung gestellt, überwacht und gesteuert.

In sicheren AD-Umgebungen arbeiten Administratoren nicht mit Administratorkonten, sondern erhalten einen Zugang mit "Just Enough Administration" (JEA). Dazu definieren Sie eine Gruppe an Cmdlets in der PowerShell sowie eine genaue Zielgruppe an Objekten, die für einen bestimmten administrativen Vorgang nötig sind. Nur diese Cmdlets darf der entsprechende Account dann nutzen. Auch die Zeitdauer für diese Rechte lässt sich über JEA steuern. Sobald der Zeitraum abgelaufen ist, kann der Zugang nicht mehr für die Administration genutzt werden, auch nicht für den fest definierten Zielbereich.

AD in der PowerShell installieren

Mit Windows Server 2016 können Sie problemlos die Active-Directory-Binärdateien über die PowerShell installieren und neue Domänen, Gesamtstrukturen oder Domänencontroller anlegen. Hier gibt es im Vergleich zu Windows Server 2012 R2 zwar keine allzu großen Neuerungen, dennoch kann es sinnvoll sein, im Rahmen von Migrationen die Bereitstellung von Windows Server 2016 über die PowerShell zu automatisieren. Das geht zwar auch mit Windows Server 2012 R2, da Windows Server 2016 aber in vielen Bereichen mehr Möglichkeiten in der PowerShell bietet, ergibt es Sinn, spätestens mit der neuen Version auf die PowerShell zu setzen. Zum Beispiel, um Umgebungen für PAM oder für Migrationsszenarien zu installieren.

Die PowerShell erlaubt Ihnen auch, Domänencontroller (DC) auf Core-Servern zu installieren, wobei Nano-Server nicht als DC dienen können. Für die AD-Installation auf herkömmlichen Servern ist der Einsatz der PowerShell dann sinnvoll, wenn Sie die Installation über WAN-Leitungen vornehmen.

Installieren lassen sich die Binärdateien des Active Directory mit dem Befehl *Install-windowsfeature AD-domain-services*. Die erfolgreiche Installation prüfen Sie mit *get-windowsfeature* und auch, ob die Binärdateien für das Active Directory installiert sind, erfahren Sie mit *get-windowsfeature*. Auf diesem Weg lässt sich in der PowerShell zudem anzeigen, welche Serverdienste bereits installiert sind.

Neue AD-Gesamtstruktur über die PowerShell

Eine neue Gesamtstruktur erstellen Sie mit dem Befehl *Install-AddsForest*. Mit verschiedenen Optionen geben Sie die Daten der Gesamtstruktur mit, um eine neue Domäne in einer neuen Gesamtstruktur zu installieren. Eine typische Testumgebung zeigt die folgende Befehlskette, bei der wir den Domänenmodus "Windows Server 2012 R2" verwenden. Das ermöglicht die Bereitstellung von zusätzlichen DCs mit Windows Server 2012 R2, neben den Domänencontrollern mit Windows Server 2016:

```
Install-ADDSForest
 -CreateDnsDelegation:$false
 -DatabasePath "C:\Windows\NTDS"
 -DomainMode "Win2012R2"
 -DomainName "testdom.int"
 -DomainNetbiosName "testdom"
 -ForestMode "Win2012R2"
 -InstallDns:$true
 -LogPath "C:\Windows\NTDS" `
 -NoRebootOnCompletion:$false
 -SysvolPath "C:\Windows\SYSVOL"
 -Force:$true
-SafeModeAdministratorPassword
  (read-host -prompt Kennwort
  -assecurestring)
```

Anschließend erstellt der Server die Domäne und Gesamtstruktur. Während der Installation der Gesamtstruktur startet der Server automatisch neu und auch der DNS-Dienst nimmt den Betrieb auf. Nachdem der Server zum Domänencontroller heraufgestuft ist, konfiguriert die PowerShell die DNS-Zone der Domäne automatisch mit sicheren DNS-Updates. Das heißt, es können sich zwar neue Clients in der DNS-Zone registrieren, aber nur dann, wenn sie Mitglied der Domäne sind.

Neue DCs in bestehenden Domänen installieren

Einen neuen DC in einer vorhandenen Domäne installieren Sie mit dem Cmdlet "Install-ADDSDomainController". Dabei geben Sie den Namen der Domäne an und konfigurieren das Kennwort für den Verzeichnisdienst-Wiederherstellungsmodus als SecureString:

```
Install-ADDSDomainController
  -Domainname DNS-Name der Domäne
  -SafeModeAdministratorPassword
  (read-host -prompt Kennwort
  -assecurestring)
```

Standardmäßig registriert Windows Server 2016 den Server mit dem Namen als Domänencontroller, den er beim Start erhält. Sie können den Server in der PowerShell aber auch umbenennen:

```
Rename-Computer -Name Computername
```

Wurde der Server zum DC heraufgestuft wurde, ist ein Umbenennen nicht mehr möglich. Um den Server danach neu zu starten, können Sie ebenfalls die PowerShell verwenden. Als Cmdlet nutzen Sie dazu *Restart-Computer*.

In der PowerShell können Sie aber nicht nur DCs erstellen, sondern auch Computer mit Server 2016 als Mitgliedscomputer in die Domäne aufnehmen:

```
Add-Computer -DomainName Domänenname
```

Um sich die Domänencontroller im Netzwerk anzuzeigen, reicht es aus, wenn Sie den Befehl *Get-ADDomainController* ein-

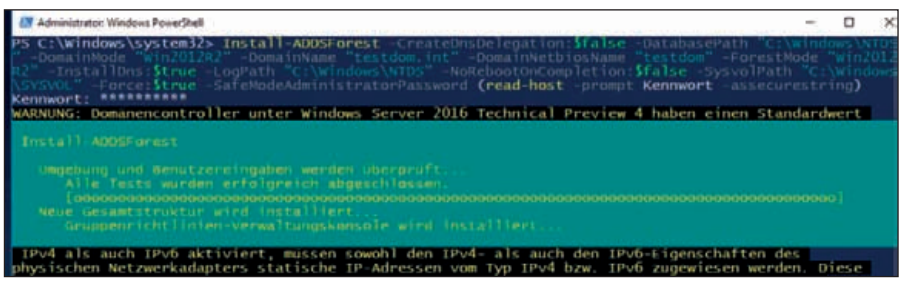


Bild 3: Eine neue Domäne und Gesamtstruktur lässt sich auch in der PowerShell einrichten.

geben. Dadurch erhalten Sie Informationen zur Domäne, Organisationseinheit, GUID, IP-Adresse, FSMO-Rollen und weitere Infos zum DC.

Wie alle Cmdlets kann auch dieses die Anzeige formatieren, indem Sie den Befehl um "|fl" ergänzen und dahinter die Spalten eintragen, die in der PowerShell angezeigt werden sollen. Benötigen Sie zum Beispiel nur den Namen, das Betriebssystem, die IP-Adresse und die installierten FSMO-Rollen, verwenden Sie:

```
Get-ADDomainController |fl hostname,
  IPV4Address, OperationMasterroles,
  OperatingSystem
```

Mit "|ft" zeigen Sie die Informationen als formatierte Tabelle an. Bei dem Cmdlet haben Sie auch die Möglichkeit, die Anzeige zu filtern. Ein Beispielfilter ist etwa das Anzeigen von schreibgeschützten Domänencontrollern:

```
Get-ADDomainController -Filter
  {isreadonly -eq $true}
```

Die schreibgeschützten Domänencontroller blenden Sie mit

```
Get-ADDomainController -Filter
  {isreadonly -eq $false}
```

aus. Mit dieser Syntax können Sie auch nach allen anderen Feldern filtern lassen, die sich über *Get-ADDomainController* anzeigen lassen. Dazu verwenden Sie die Option "-Filter" und den Namen der Spalte in geschweiften Klammern, zusammen mit der Option, ob der Filter "zutreffen" ($true) oder "nicht zutreffen" ($false) verwendet werden soll. In diesem Zusammenhang ist auch die Spalte "IsGlobalCatalog" interessant, da sich hier nach globalen Katalogen filtern lässt. Das ist vor allem in größeren Umgebungen von Bedeutung.

FSMO-Rollen auslesen

Die Filteroptionen in der PowerShell sind auch interessant, um aus Spalten Informationen als Text auszulesen. In der Spalte "OperationMasterroles" werden alle FSMO-Rollen von Domänencontrollern angezeigt. Einen Filter, um die PDC-Master zu zeigen, erzeugen Sie mit:

```
Get-ADDomainController -Filter {Ope-
  rationMaster-Roles -like "PDC*"}
```

Wollen Sie nur die Namen und die installierten Betriebsmaster anzeigen, ergänzen Sie das Cmdlet um "|fl Hostname, OperationMasterroles".

Sie haben auch die Möglichkeit, die Ergebnisse eines Get-Cmdlets an ein anderes Cmdlet weiterzugeben, das Konfigurationen ändert. Beispiel dafür ist das Verschieben an einen anderen Standort, was vor allem bei Migrationen hilfreich ist:

```
Get-ADDomainController Name des
  Servers | Move-ADDirectoryServer
  -Site Name des Standortes
```

Domänen und Gesamtstrukturen abfragen

Die PowerShell erlaubt Ihnen auch, Daten einzelner Domänen abzufragen. Dazu verwenden Sie *Get-ADDomain*. Über *Get-ADForest* erhalten Sie Informationen zu Gesamtstrukturen. Auch hier können Sie Spalten auf dem gleichen Wegen filtern, wie zuvor dargestellt. Sinnvoll ist das Cmdlet, wenn die FSMO-Rollen pro Domäne angezeigt werden sollen. In jeder Domäne gibt es drei FSMO-Rollen, die Sie wie folgt ermitteln:

```
Get-ADDomain | Select Infrastructu-
  reMaster, RID-Master, PDCEmulator
```

Schemamaster und Domänennamenmaster gibt es nur einmal pro Gesamtstruktur. Diese Informationen lassen sich so anzeigen:

```
Get-ADForest |
  Select-Object DomainNamingMaster,
  SchemaMaster
```

Betriebsmasterrollen lassen sich in der PowerShell auf andere Domänencontroller verschieben:

```
Move-ADDirectoryServerOperation-
  MasterRole
```

Mit

```
get-help Move-ADDirectoryServer-
  OperationMasterRole
```

erhalten Sie die umfassende Syntax und einige Beispiele für das Cmdlet.

Replikation sicherstellen

Sie sollten in regelmäßigen Abständen testen, ob die Replikation im Active Directory noch funktioniert – vor allem dann, wenn Sie DCs mit Server 2016 in das Netzwerk integriert haben. Microsoft bietet in der Befehlszeile einige Tools an, mit denen Sie problemlos Tests durchführen können. Die wichtigsten Befehle sind:

- *Dcdiag /v*: Ausführliche AD-Diagnose inklusive der Replikation.
- *Repadmin /showreps*: Anzeigen der Replikationsverbindungen zwischen DCs.
- *Nltest /dclist:Domäne*: Abrufen der DCs.
- *Nltest /dsgetsite*: Anzeigen der AD-Standorte.

Mit diesen Tests lässt sich recht schnell erkennen, ob Probleme im Netzwerk vorliegen und die neuen DCs korrekt eingebunden wurden.

Darüber hinaus sollten Sie nicht mehr vorhandene Computer aus den Computerkonten entfernen, vor allem wenn es sich um DCs handelt. Über die Verwaltungskonsole "Active Directory-Standorte und -Dienste" sehen Sie die einzelnen Standorte und Domänencontroller. Die Konsole zeigt hier auch die Replikationsverbindungen an, die Sie regelmäßig über das Kontextmenü überprüfen sollten.

Unersetzliche Active-Directory-Zertifikatdienste

Der Einsatz einer internen Zertifizierungsstellen ist im Active Directory nahezu unerlässlich. Viele Serversysteme von Microsoft oder auch Drittanbietern benötigen Zertifikate für den Zugriff. Beispiele dafür sind Exchange und SharePoint, aber auch SQL-Server benötigen ein Zertifikat, wenn Sie Verbindungen verschlüsseln wollen.

Da die Standard-Edition von Windows Server 2016 nahezu die gleichen Funktionen und Serverrollen unterstützt wie die Datacenter-Edition, können Sie alle verfügbaren Funktionen der Active-Directory-Zertifikatdienste auch auf Servern mit Windows Server 2016 Standard Edition betreiben. Außerdem unterstützen

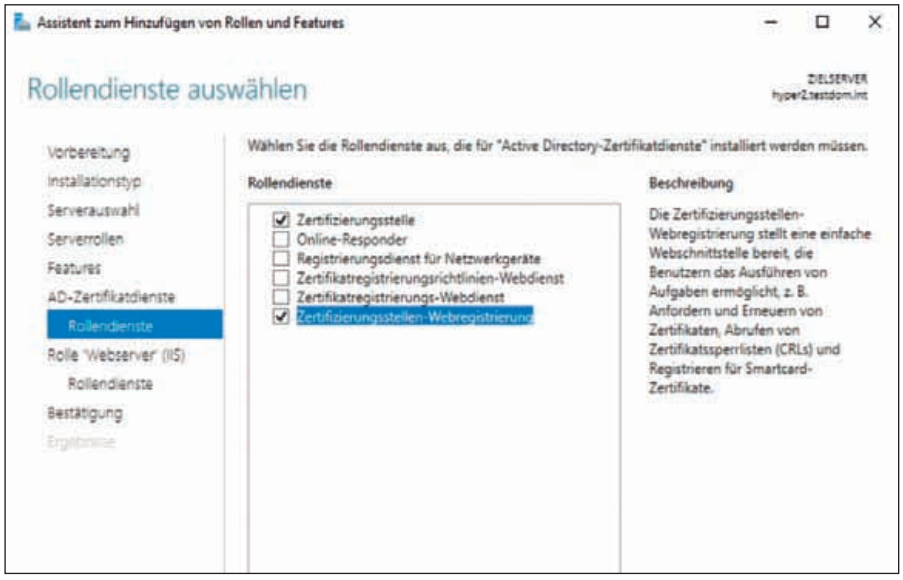


Bild 4: Die Installation der Active-Directory-Zertifikatdienste erfolgt über den Server-Manager.

alle Funktionen der AD-Zertifikatdienste vollständig Core-Installationen von Windows Server 2016. Sie können die Zertifikatdienste allerdings nicht auf einem Nano-Server installieren.

Die Installation führen Sie über das Hinzufügen der Rolle "Active Directory-Zertifikatdienste" im Server-Manager durch. Wählen Sie diese Rolle aus, startet der Installationsvorgang der Zertifikatdienste mit einem Assistenten, über den Sie verschiedene Auswahlmöglichkeiten haben.

Generell ist es nicht empfehlenswert, die Installation auf einem Domänencontroller durchzuführen. Sie sollten als Server für die Zertifikatdienste am besten einen Mitgliedsserver verwenden. Sie haben bei der Installation die Auswahl zwischen insgesamt sechs Rollentypen:

- Zertifizierungsstelle: Hierbei handelt es sich um den wichtigsten Rollendienst, der die Basis der Zertifikatdienste darstellt. Dieser Rollendienst wird für das Ausstellen und Verwalten der Zertifikate benötigt.
- Online-Responder: Stellt die Funktion zur Verfügung, über die Clients erweiterte Informationen über den aktuellen Zustand der Zertifikatsabfrage erhalten. Der Dienst setzt IIS voraus.
- Registrierungsdienst für Netzwerkgeräte: Diese Funktion lässt sich nur alleine installieren, nicht zusammen mit einer Zertifizierungsstelle. Mit diesem Rollendienst wird die Funktion zum automatischen Ausstellen von Zertifikaten an Netzwerkgeräte ermöglicht.
- Zertifikatregistrierungsrichtlinie-Webdienst: Diesen Dienst benötigen Sie, wenn Sie eine richtlinienbasierte Zertifikatregistrierung ermöglichen, der Clientcomputer jedoch kein Mitglied einer Domäne ist.
- Zertifikatregistrierungs-Webdienst: Stellt einen Webdienst zur Verfügung, der Clients eine Aktualisierung der Zertifikate erlaubt, ohne dass die Computer Mitglied einer Domäne sein müssen.
- Zertifizierungsstellen-Webregistrierung: Wird dieser Rollendienst installiert, können auch Zertifikate über die Webadresse "http://Servername/certsrv" angefordert werden. Hierbei handelt es sich um die Webschnittstelle der Zertifikatdienste.

Wie bei der AD-Installation starten Sie nach der Installation der Serverrolle für die Zertifizierungsstelle den Einrichtungs-Assistenten über das Wartungssymbol im Server-Manager. Nach dem Start des Assistenten geben Sie den Benutzernamen ein, mit dem Sie den Dienst einrichten wollen. Standardmäßig übernimmt der Assistent den Benutzer, mit dem Sie am Server angemeldet sind. Als Nächstes bestimmen Sie, welche Rollendienste Sie konfigurieren wollen. Nicht installierte Rollendienste sind deaktiviert. Auf der nächsten Seite legen Sie den Setuptyp fest. Hier sollten Sie die Option "Unternehmenszertifizierungsstelle" auswählen, da Sie bei der ersten CA eine Root-CA installieren. Bei dieser Auswahl wird auch die CA in das AD integriert. Auf diese Weise verteilt die Zertifizierungsstelle das Zertifikat auf allen Servern und Clientcomputern im Netzwerk.

Auf der nächsten Seite des Assistenten legen Sie den Zertifizierungsstellentyp fest. Hier sollten Sie bei der ersten Installation möglichst eine Stammzertifizierungsstelle auswählen. Bei der ersten Installation einer Zertifizierungsstelle legen Sie fest, dass Sie einen neuen privaten Schlüssel erstellen wollen, da es für diese Zertifizierungsstelle noch keinen Schlüssel gibt. Auf der nächsten Seite des Assistenten bestimmen Sie, mit welcher Verschlüsselung Sie Zertifikate ausstellen wollen. Hier sollten Sie möglichst den Standard belassen. Über die folgende Seite legen Sie den Namen für die neue Zertifizierungsstelle fest. Hier wählen Sie bei der ersten Stammzertifizierungsstelle im Unternehmen einen passenden Namen. Im Anschluss bestimmen Sie die Gültigkeitsdauer für die Zertifikate und schließen die Konfiguration ab. Nach der Installation können Sie über das Verwaltungsprogramm "Zertifizierungsstelle" im Menü "Tools" des Server-Managers überprüfen, ob die Installation erfolgreich war. Der Server sollte mit einem grünen Häkchen in der Verwaltungsoberfläche angezeigt werden.

Haben Sie bei der Installation noch den Rollendienst "Zertifizierungsstellen-Webregistrierung" ausgewählt, steht über den Link "http://Servername/certsrv" zusätzlich noch die Weboberfläche der Zertifizierungsstelle zur Verfügung. Diese sollte sich nach erfolgter Authentifizierung fehlerfrei öffnen lassen. Zusätzlich gibt es das Zusatztool "Pkiview", mit dem Sie den Zustand der Zertifizierungsstelle überprüfen. Findet das Tool Fehler, werden diese in einer Konsole angezeigt. Das Werkzeug starten Sie am schnellsten durch die Eingabe von *pkiview* in der Eingabeaufforderung.

Alle Mitgliedscomputer einer Domäne vertrauen einer internen Stammzertifizierungsstelle mit dem Typ "Unternehmen" automatisch. Das Zertifikat dieser Zertifizierungsstelle wird dazu auf den Client-

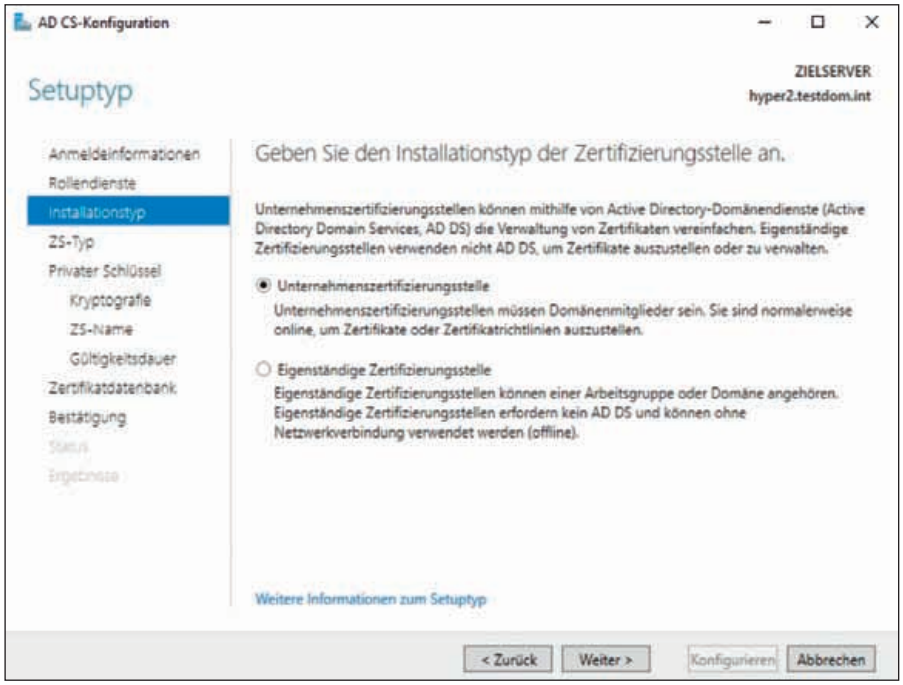


Bild 5: Beim Anlegen der Zertifizierungsstelle ist das Auswählen des Installationstyps erforderlich.

computern und Mitgliedsservern in den Zertifikatspeicher der vertrauenswürdigen Stammzertifizierungsstellen integriert. Damit der Server fehlerfrei Zertifikate ausstellen kann, muss er Mitglied der Gruppe "Zertifikateherausgeber" sein. Diese Gruppe befindet sich in der OU "Users". Haben Sie die Active-Directory-Zertifikatdienste installiert, können Sie den Import des Zertifikats auf Clients und dem Server beschleunigen, wenn Sie auf dem Server über *gpupdate /force* die Gruppenrichtlinien erneut abrufen.

Die wichtigsten Daten der Active-Directory-Zertifikatdienste lassen sich auch sichern. Wählen Sie im Kontextmenü der Zertifizierungsstelle in der Verwaltungskonsole die Option "Alle Aufgaben / Zertifizierungsstelle sichern". Anschließend startet der Sicherungsassistent. Darin wählen Sie zunächst aus, welche Dateien gesichert werden sollen und in welcher Datei die Sicherung abgelegt wird. Anschließend vergeben Sie ein Kennwort für die Sicherung. Auf dem gleichen Weg lassen sich auch Daten wiederherstellen.

Zertifikate mit Assistenten aufrufen

In der lokalen Verwaltung von Zertifikaten können Sie im Active Directory auch Zertifikate auf einem Server installieren. Dazu starten Sie durch die Eingabe von *certlm.msc* auf der Startseite die Verwaltung der lokalen Zertifikate. Klicken Sie mit der rechten Maustaste auf "Zertifikate" und wählen Sie dann "Alle Aufgaben / Neues Zertifikat anfordern". Aktivieren Sie auf der nächsten Seite die Option "Active Directory-Registrierungsrichtlinie" und auf der folgenden Seite "Computer" und klicken Sie auf "Registrieren". Das Zertifikat erscheint anschließend in der Konsole und lässt sich nutzen.

Über den IIS-Manager auf einem Server erledigen Sie die Aufgabe, indem Sie den IIS-Manager zunächst über das Menü "Tools" im Server-Manager öffnen und dann auf den Servernamen klicken. Jetzt doppelklicken Sie auf das Feature "Serverzertifikate" im mittleren Bereich der Konsole. Navigieren Sie im Bereich "Aktionen" auf "Zertifikatanforderung erstellen". Alternativ können Sie auch "Domänenzertifikat erstellen" auswählen, wenn Sie mit den Active-Directory-Zertifikatdiensten arbeiten. Die folgenden Fenster sind dabei identisch.

SSL für Zertifikatdienste einrichten

Viele Optionen für den Webdienst der Zertifizierungsstelle funktionieren erst dann, wenn Sie SSL für die Webdienste aktivieren. Standardmäßig erreichen Sie den Webdienst über "http://Servername/certsrv". Wollen Sie ein Zertifikat über diese URL abrufen, erhalten Sie aber die Meldung, dass Sie erst SSL für den Webdienst aktivieren müssen. Dazu gehen Sie folgendermaßen vor:

1. Klicken Sie im Internetinformationsdienste-Manager auf "Sites / Default Web Site".
2. Wählen Sie rechts "Bindungen".
3. Klicken Sie im neuen Fenster auf "Hinzufügen" und wählen Sie "HTTPS" aus.
4. Wählen Sie bei SSL-Zertifikat ein Zertifikat aus. Sie können das Zertifikat jederzeit anpassen.
5. Klicken Sie zweimal auf "OK", um die Änderungen zu speichern.

Sobald Sie die Bindung definiert haben, können Sie bereits per SSL auf die Seite zugreifen. Greifen Sie mit URLs auf den Server zu, erscheint unter Umständen mehrere Male ein Authentifizierungsfenster. In diesem Fall sollten Sie zunächst überprüfen, ob im Browser die Adresse auch als lokales Intranet konfiguriert ist. Achten Sie in diesem Fall auch darauf, dass Sie entweder mit einem Platzhalterzertifikat arbeiten, oder für die entsprechende URL den richtigen Namen im Zertifikat angeben.

Fazit

Auch wenn es vergleichsweise wenig Neuerungen gibt, gilt für den Admin dennoch nach wie vor, sein Active Directory aus dem Effeff zu kennen. Zu wichtig ist die Leistung für die Stabilität und Funktion der gesamten Serverinfrastruktur. Dienste wie die übergreifende Authentifizierung oder die Zertifikatsausstellung sollten reibungslos funktionieren. Das gilt noch mehr für die Replikation, auf die jeder IT-Verantwortlich regelmäßig einen prüfenden Blick werfen sollte. *(jp)*

Link-Codes

[1] Active Directory Federation Services
GS212

[2] AD FS Diagnostics Module
GS241

[3] Privileged Access Management (PAM)
GS213

[4] Microsoft Identity Manager (MIM)
GS242

[5] Microsoft Passport
GS243