Create. Learn. Guide.

datango

Technische Voraussetzungen für datango collaborator & live! 3.2.7

Inhaltsverzeichnis

Zweck: Die Anleitung soll Ihnen eine reibungslose Installation der datango Produkte ermöglichen. Wenn Sie zu den Punkten Fragen haben, können Sie sich gerne per Mail an support@datango.de wenden oder an die Support Hotline +49 2131 76201 112.

1 Grundvoraussetzungen

1.1 Software

Sollten Sie einen Server installieren, der keinen Internetzugriff hat, stellen Sie bitte sicher, dass die folgenden Software-Pakete auf dem Server zur Verfügung stehen. Diese werden Ihnen vom datango Support Team ggf. als Download Link im Kundenbereich bereitgestellt.

- JAVA OpenJDK 17 (Long term support Version)
- Microsoft SQL 2016 und neuer x64 (Express Edition reicht ggf. aus, wenn höchstens zwei Autoren geplant sind und der Lern-Content später für ein LMS exportiert wird)
- collaborator.jar

1.2 Systemanforderungen

Die folgenden Systemanforderung sind für grob 20 parallel arbeitende Autoren ausgelegt und es können ca. 100-200 Lernende zeitgleich auf den Server zugreifen. Dies ist jedoch auch von Art und Größe Ihres erstellten Contents abhängig.

1.2.1 Variante 1 ohne MSSQL lokal

8x CPUs 2,1 Ghz Intel Xeon, neuer oder vergleichbar empfohlen.
8GB RAM, für jeden gleichzeitigen User werden etwa 15MB RAM benötigt.
1x 10 Gbit/s LAN-Interface empfohlen.

Speicherplatz:

- 15GB für Java und die collaborator.jar (Wachstum je nach Nutzung und Log Level des Servers)
- 50GB für die Content-Ablage (Wachstum je nach Anzahl der Autoren und deren Aktivität. Rechnen Sie bitte mit mehreren 100MB pro Monat beginnend bei unter 100MB pro initialisiertem Server-Arbeitsbereich)

1.2.2 Variante 2 mit MSSQL lokal:

8x CPUs 2,8 Ghz Intel Xeon, neuer oder vergleichbar empfohlen.
16GB RAM, für jeden gleichzeitigen User werden etwa 15MB RAM benötigt.
1x 10 Gbit/s LAN-Interface empfohlen.

Festplatten Speicherplatz:
- 15GB für Java und die collaborator.jar
- 20GB für die Datenbank (Wachstum je nach Nutzung und Log Level des Servers)
- 50GB für die Content-Ablage (Wachstum je nach Anzahl der Autoren und deren Aktivität. Rechnen Sie bitte mit mehreren 100MB pro Monat beginnend bei unter 100MB pro Initialisiertem Server-Arbeitsbereich)

Backup
Empfohlen ist ein Backup des gesamten Servers in regelmäßigen Abständen. (Snapshots incl. der Datenbanken, wenn diese nicht lokal auf demselben Server laufen. Im Idealfall sollten die Datenbanksicherungen und Content-Sicherungen zeitgleich stattfinden.)

1.3 User-Konten

Im datango Installationsprozess werden die folgenden User angelegt oder von Ihnen benötigt:

Von datango erstellt in Ihrer Anwesenheit:

1.) Service-User mit dem die collaborator.jar-Datei als Dienst ausgeführt wird

2.) MSSQL Lokaler User nur bei einer lokalen Installation

Von Ihnen benötigt:

1.) Der datango collaborator benötigt einen Service-User („Dienstkonto“), der Teil der lokalen Administratoren-Gruppe ist, damit dieser Zugriff auf lokale Ressourcen erhält, z.B. Vollzugriff auf das Content-Verzeichnis, Neustart des Service.

2.) Wenn Sie planen Ihre User via LDAP aus Ihrem Active Directory Server zu importieren, benötigen wir ein Dienstkonto (z.B. datango@domain.com), dessen Kennwort nicht abläuft. Bitte stellen Sie dieses Dienstkonto bereit und setzen den entsprechenden Haken („Kennwort läuft nicht ab“ im AD Konto).

3.) Wenn Sie möchten, dass der Server E-Mails versenden kann und die Kommunikation mit Ihrem E-Mail-Server verschlüsselt wird (SMTP Port 587 TLS), benötigen wir einen E-Mail-User mit Kennwort. Dies kann auch das obige Dienstkonto sein.
Wenn Sie ein Portal eines Drittanbieters, wie z.B. Exchange 365 oder Gmail, verwenden möchten, dass StartTLS für die Verschlüsselung verwendet, lesen Sie bitte in der Dokumentation des Drittanbieters nach, wie Sie das Portal so konfigurieren, dass der datango collaborator E-Mails versenden kann.

4.) Wenn Sie eine MSSQL Cluster-Installation haben und Sie unsere Datenbank dort vorhalten möchten, benötigen wir einen lokalen MSSQL User auf Ihrem DB Cluster. Hierzu bitte kein Domain-Konto anlegen. Dieser User benötigt Lese- und Schreibrechte. Bitte stellen Sie sicher, dass die Passwörter dieser User nicht ablaufen.

1.4 Datenbank Variante 1 (Ihr Cluster / Server)

Ab Version 3.2.4 benötigen wir eine bereits angelegte, leere Datenbank, die während der Installation ausgewählt werden kann. Hierzu benötigen wir einen lokalen MSSQL User mit „Lese- und Schreibrechten“ - kein Domain-Konto.

Die IP oder FQDN des MSSQL Clusters mit Port (z.B. db01.domain.com:1433) wird benötigt, um diese während der Installation anzugeben.

1.5 Datenbank Variante 2 (localhost)

Wenn Sie kein Datenbank-Cluster bzw. keinen Datenbankserver verwenden möchten, können wir beim Installationstermin eine „lokale“ Version des MS SQL Servers installieren.

1.6 SSL

Die Datenübertragung vom datango creator (dem Autoren-Werkzeug) an den datango collaborator erfolgt ausschließlich verschlüsselt, da wir sicherstellen wollen, dass Sie keine unternehmensinternen Daten unverschlüsselt übertragen.

Ebenso wird Lern-Content ausschließlich verschlüsselt an die Lernenden übertragen, da wir auch hier sicherstellen wollen, dass Sie keine Interna unverschlüsselt übertragen.

Alle unsere Produkte verwenden daher zur Kommunikation mit dem datango collaborator ausschließlich das HTTPS-Protokoll und wir verwenden TLS 1.2 oder TLS 1.3.

Um die Netzwerk-Kommunikation zu verschlüsseln, benötigen Sie:
- 1x Server Zertifikat oder
- 1x Domain Wildcard mit Privatem Schlüssel

Dieses Zertifikat sollte die DNS URL ohne Sicherheitswarnungen verifizieren. Nur so kann eine reibungslose Kommunikation gewährleistet werden.

Unterstützte Java-Keystore-Formate sind „.pfx“ und „.p12“.

Wenn gestattet, können wir auch gerne während der Installation mit der „mmc Konsole“ die benötigten Zertifikate bei Ihrer internen CA anfragen.

Bitte beachten Sie, dass das Zertifikat auf die DNS-Adresse Ihres Servers ausgestellt sein muss, wenn Sie nicht den FQDN Ihres Servers an Autoren und Lernende kommunizieren möchten – siehe unten.

Zertifikate belegen für den End-User, dass Sie und Ihr Server tatsächlich von Ihnen – und nur von Ihnen – kontrolliert wird und kein Unbefugter Zugriff erhält. Aus diesem Grund können wir Ihnen kein Zertifikat mitliefern – wir können nicht belegen, dass wir Sie sind.

Darüber hinaus muss das Zertifikat einen SAN enthalten (SAN steht für Subject Alternative Name), weil Edge, Chrome und Firefox dies benötigen und ansonsten einen Zertifikatsfehler anzeigen.

2 Optionale Voraussetzungen

Die folgenden Voraussetzungen sind nicht kritisch, aber dennoch empfohlen:

2.1 DNS-Name

Der Einsatz eines DNS-Namens ist eine kurze Überlegung wert, da die URL des Servers mehrfach von Ihnen an Kollegen oder Teams weitergeben werden wird, um sich mit der datango Plattform zu verbinden. Hierzu benötigen wir einen DNS-Namen (URL für die User / Client) z.B. datango.domain.local. Alternativ benötigen Ihre User immer den FQDN des Servers. Der DNS-Name oder aber der FQDN wird von uns nach der Installation in den Servereinstellungen hinterlegt, um automatisierte Links bei der Generierung von E-Mails zu verwenden. Mehr zum E-Mail-Versand: siehe unten.

In datango-Versionen vor 3.2.4 wird der DNS-Name bzw. der FQDN des Servers um „/register/data“ ergänzt, um die Anmelde-URL für datango live! zu erzeugen. Ab Version 3.2.4 entspricht die Anmelde-URL von datango live! der Anmelde-URL für den datango creator und der URL für den Aufruf der datango collaborator Weboberfläche.

2.2 LDAP AD (User Import)

Das oben angesprochene AD-Service-Konto wird dazu verwendet um bei Bedarf, einen LDAP-Import Ihrer Organisationsstruktur in den collaborator zu ermöglichen. Da dieser über ein eigenes Berechtigungssystem verfügt, können Sie Organisationseinheiten, Gruppen und einzelne User verwenden, um Berechtigungen zu verwalten und die Struktur Ihrer Organisation aktuell halten. Der Abgleich läuft hierzu in der Regel einmal täglich. Der Zeitpunkt und die Häufigkeit können von Ihnen frei definiert werden. Hierzu können Sie, falls gewünscht, einen Report per E-Mail erhalten.

Ab Version 3.2.4 können Sie aus unterschiedlichen Optionen wählen, wie Ihre Struktur importiert werden kann, z.B. selektiv oder rekursiv. Vor Version 3.2.4 können Sie keine Unterknoten ausschließen. Zudem ist in Version 3.2.4 neu, dass Subdomains via LDAP Global Catalog abgefragt werden können.

Zusätzlich dazu können Sie ab Version 3.2.6 parallele Abfragen von mehreren LDAP-Servern einrichten; auch wenn diese Server in keinerlei Vertrauensstellung zueinander existieren. Der datango collaborator ist damit ab dieser Version voll Multidomain-LDAP fähig.

2.3 E-Mails

Der datango collaborator besitzt eine E-Mail-Funktion, mithilfe derer es möglich ist User und Autoren zu benachrichtigen, wenn relevante Ereignisse stattgefunden haben. Beispielsweise können sich Autoren untereinander benachrichtigen, wenn Content fertiggestellt ist und zur Qualitätssicherung übergeben werden soll.

Zudem können End-User automatisiert darauf hingewiesen werden, dass Kurse erstellt wurden, ab einem bestimmten Datum zur Verfügung stehen, noch nicht begonnen wurden oder bald ablaufen. (Dies setzt die Lizenz „Academy“ voraus.)

Auch Reports können abonniert werden und lösen einen automatischen Versand von Tabellen aus. (Dies setzt voraus, dass der „Analyzer“ lizenziert wurde.)

Wenn Sie dieses Feature nutzen möchten, benötigen wir von Ihnen die Daten Ihres SMTP Servers (Adresse, IP mit Port oder DNS-Namen des Relay Gateways). StartTLS wird ebenfalls unterstützt.

2.4 GPO

Es ist empfehlenswert den Server via Richtlinie ins „Intranet“ einzutragen. Wir arbeiten in unseren Contents mit Pop-Ups und so kann der Pop-Up-Blocker der meisten Browser automatisch konfiguriert werden, um datango nicht zu blockieren.

Zusätzlich stellen Sie mit den Standardsicherheitseinstellungen der Zone „Intranet“ sicher, dass Ihre Lernenden ein möglichst reibungsloses Lernerlebnis haben.

Wenn Sie Single-Sign-on via Kerberos einrichten möchten (siehe unten) ist es zwingend erforderlich, dass sich der collaborator in der Zone „Intranet“ befindet.

2.5 SSO

Der collaborator besitzt eine SSO Kerberos Funktion im KRB5 Prinzip mit SPN. Ein Domain Admin sollte für die Anfrage der Keytab-Datei anwesend sein.

Beispiel der PowerShell Befehle:

1.) setspn -A HTTP/DNSURL ADUser

2.) ktpass /out collaborator.keytab /princ HTTP/DNSURL@DOMAIN /ptypeKRB5_NT_PRINCIPAL -crypto All /target DOMAIN /pass “” /mapuser ADUser

Alternativ können Sie Simple-Sign-On (SSO) via SAML konfigurieren. Bitte sprechen Sie hierzu unseren Support an, um gemeinsam eine SAML-Datei für und mit Ihnen zu entwickeln.

Voraussetzung ist dennoch, dass Sie Ihre User per LDAP importieren. Importierte User können nach der Eingabe des Usernamens auf SSO klicken und werden dann via SAML authentifiziert.

2.6 Sonstiges

Wir empfehlen einen Texteditor wie bspw. Notepad++, Sublime, Ultra Edit oder Ähnliches zu installieren. Außerdem sollte ein Browser wie Edge, Chrome oder Firefox installiert sein. Der Internet Explorer wird von Microsoft und uns **nicht** mehr unterstützt.