

Erste Schritte

Fabasoft Private Cloud

2017 Spring Release

www.fabasoft.com

Copyright © Fabasoft R&D GmbH, A-4020 Linz, 2017.

Alle Rechte vorbehalten. Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Marken der jeweiligen Hersteller.

Durch die Übermittlung und Präsentation dieser Unterlagen alleine werden keine Rechte an unserer Software, an unseren Dienstleistungen und Dienstleistungsergebnissen oder sonstigen geschützten Rechten begründet.

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z. B. Benutzer/-innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Inhalt

1 Fabasoft Private Cloud	4
2 Vorbereitung	4
3 Installation im Rechenzentrum	5
4 Server-Konfiguration	5
4.1 Dell iDRAC	6
4.1.1 Netzwerk-Einstellungen für Dell iDRAC	6
4.1.2 iDRAC-Einstellungen	6
4.2 Boot-Passwort	7
4.3 Festplatten-Einstellungen	7
4.4 Netzwerk-Konfiguration	8
5 Fabasoft Private Cloud Installation	8
6 Fabasoft Private Cloud Organisation	9
6.1 Anmeldung mit Client-Zertifikaten	9
6.2 Mitglieder hinzufügen	9
6.2.1 Mitglieder per CSV-Import erzeugen	10
6.2.2 Mitglieder manuell erzeugen	11
6.3 Mitglieder einladen	12
6.4 Servicedesk einrichten	12
6.5 Eigentümer und Administratoren festlegen	13
7 Server-Zertifikate	13
8 Weiterführende Dokumente	14

1 Fabasoft Private Cloud

Willkommen in der Fabasoft Private Cloud.

Diese Kurzübersicht führt Sie durch die Installation im Rechenzentrum und begleitet Sie bis zum initialen Einrichten Ihrer Organisation in der Fabasoft Private Cloud.



2 Vorbereitung

Für eine rasche und reibungslose Installation der Fabasoft Private Cloud in Ihrer Infrastruktur bereiten Sie bitte Folgendes vor:

Netzwerkconfiguration für die Management-Interfaces (Dell iDRAC)			
Node 1 (IP-Adresse, Mask, Gateway)			
Node 2 (IP-Adresse, Mask, Gateway)			
Netzwerkconfiguration für die Customer-LAN-Anbindung (Benutzerzugriff)			
Node 1 (IP-Adresse, Mask, Gateway)			
Node 2 (IP-Adresse, Mask, Gateway)			
Netzwerkconfiguration für die interne Cluster-Kommunikation			
Node 1 (IP-Adresse, Mask, Gateway)			
Node 2 (IP-Adresse, Mask, Gateway)			
Konfiguration für den Benutzerzugriff auf die Fabasoft Private Cloud im Customer-LAN			
IP-Adresse			
Fully Qualified Domain Name (FQDN)			
DNS-Eintrag für den FQDN			
DNS-Eintrag für cert.<FQDN>			

Infrastruktur-Services	
DNS-Server	
SMTP-Server	
NTP-Server	
Backup-Share (SMB/CIFS oder NFS)	
Zugangsdaten zum Backup-Share	
Mindbreeze InSpire	
Mindbreeze InSpire Server	
Zugangsdaten zu Mindbreeze InSpire	

3 Installation im Rechenzentrum

Installieren Sie die Fabasoft Private Cloud Nodes in Ihren Rechenzentren. Aus Gründen der Ausfallsicherheit wird eine örtlich verteilte Installation der beiden Fabasoft Private Cloud Nodes empfohlen, wobei für die Cluster-Kommunikation eine Round Trip Time (RTT) von < 2 ms zwischen den beiden Nodes erforderlich ist.

Die Strom- und Netzwerk-Anbindung sollte redundant erfolgen. Sie können jeden Node an zwei unterschiedliche Stromkreise anbinden und jeweils die Netzwerk-Ports für das Customer-LAN und das Cluster-LAN an unterschiedliche Switches anschließen.

Die Netzwerk-Anbindung ist folgendermaßen vorgesehen:

- Customer-LAN
Netzwerk-Ports 1 und 2
- Cluster-LAN
Netzwerk-Ports auf dem eigenen Einschub in Slot 4 (entweder ein eigenes VLAN für die beiden Fabasoft Private Cloud Nodes oder eine direkte Verbindung der beiden Fabasoft Private Cloud Nodes je Port)
- Management-LAN
Netzwerk-Port „iDRAC“ (Zugriff durch Administratoren auf Dell iDRAC)

4 Server-Konfiguration

Führen Sie die nachfolgenden Konfigurationsschritte auf beiden Nodes durch.

4.1 Dell iDRAC

4.1.1 Netzwerk-Einstellungen für Dell iDRAC

Es gibt zwei Möglichkeiten, um die Netzwerk-Einstellungen für Dell iDRAC zu ändern:

- Konfiguration direkt am Server über die LCD-Menü-Schaltflächen an der Vorderseite des Servers
- Konfiguration über die Konsole

Konfiguration direkt am Server

Nehmen Sie folgende Einstellungen vor:

- Enable DHCP: Disabled
- Static IP Address
- Static Gateway
- Static Subnet Mask

Konfiguration über die Konsole

Um die Konfiguration über die Konsole vorzunehmen, gehen Sie folgendermaßen vor:

1. Wechseln Sie während des Startvorgangs des Nodes mit **F2** ins BIOS.
2. Navigieren Sie zu „iDRAC Settings“ > „Network“ > „IPV4 Settings“ und nehmen Sie folgende Einstellungen vor:
 - Enable DHCP: Disabled
 - Static IP Address
 - Static Gateway
 - Static Subnet Mask
3. Speichern Sie die Einstellungen und starten Sie den Node neu.

4.1.2 iDRAC-Einstellungen

Um die iDRAC-Einstellungen zu ändern, gehen Sie folgendermaßen vor:

1. Verbinden Sie sich zu <https://<iDrac-IP-Adresse>/>.
Hinweis: Eine Webbrowser-Warnung ist möglich, da Dell iDRAC im ausgelieferten Zustand ein selbstsigniertes Server-Zertifikat einsetzt.
2. Melden Sie sich mit dem Benutzernamen `root` und dem Passwort `calvin` an.
Nach der Anmeldung werden Sie aufgefordert das Passwort zu ändern.
3. Navigieren Sie zu „Übersicht“ > „iDRAC-Einstellungen“ > „Netzwerk“ > „IPv4-Einstellungen“ und nehmen Sie folgende Einstellungen vor:
 - Statischer bevorzugter DNS-Server
 - Statischer alternativer DNS-ServerBestätigen Sie die Änderungen mit „Anwenden“.
4. Navigieren Sie zu „Übersicht“ > „iDRAC-Einstellungen“ > „Netzwerk“ > „IPMI-Einstellungen“ und nehmen Sie folgende Einstellungen vor:

- IPMI-Über-LAN aktivieren: Ja (Checkbox anhaken)
 - Beschränkung der Kanalberechtigungsebene: „Operator“
- Bestätigen Sie die Änderungen mit „Anwenden“.
5. Navigieren Sie zu „Übersicht“ > „iDRAC-Einstellungen“ > „Netzwerk“ > „Dienste“ > „SNMP-Agent“ und nehmen Sie folgende Einstellungen vor:
 - Aktiviert: Ja (Checkbox anhaken)
 - SNMP-Community-Name: FCA
 - SNMP-Protokoll: Alle
 Bestätigen Sie die Änderungen mit „Anwenden“.
 6. Navigieren Sie zu „Übersicht“ > „iDRAC-Einstellungen“ > „Einstellungen“ und nehmen Sie folgende Einstellungen vor:
 - Gewünschte Zeitzone setzen
 Bestätigen Sie die Änderungen mit „Anwenden“.
 - Netzwerkzeitprotokoll aktivieren (NTP): Ja (Checkbox anhaken)
 - NTP-Server setzen
 Bestätigen Sie die Änderungen mit „Anwenden“.
 7. Navigieren Sie zu „Übersicht“ > „Server“ > „Warnungen“ > „SNMP- und E-Mail-Einstellungen“ und nehmen Sie folgende Einstellungen vor:
 - SMTP (E-Mail)-Server-Adresseinstellungen: Verbindungsdaten zu Ihrem SMTP-Server
 Bestätigen Sie die Änderungen mit „Anwenden“.
 8. Navigieren Sie zu „Übersicht“ > „Server“ > „Warnungen“ > „Ziel-E-Mail-Adressen“ und nehmen Sie folgende Einstellungen vor:
 - E-Mail-Adressen, welche für die Hardware-Überwachung verwendet werden sollen
 Bestätigen Sie mit „Anwenden“ (auch falls Sie einen Test mit „Senden“ durchführen möchten).
 9. Richten Sie nach Bedarf weitere personalisierte Accounts unter „Übersicht“ > „iDRAC-Einstellungen“ > „Benutzer-Authentifizierung“ ein.

Hinweis: Ein Account muss für die Fabasoft Private Cloud Installation frei bleiben. Dieser wird später automatisch konfiguriert.

4.2 Boot-Passwort

Sie können optional ein Boot-Passwort für Ihre Fabasoft Private Cloud Nodes festlegen. Dies schützt bei Diebstahl des Servers vor unberechtigtem Zugriff und hat zur Folge, dass Sie bei jedem Boot-Vorgang das Passwort auf der Konsole (z. B. über Dell iDRAC) eingeben müssen. Wenn Sie das Boot-Passwort aktivieren möchten, gehen Sie folgendermaßen vor:

1. Wechseln Sie während des Startvorgangs des Nodes mit **F2** ins BIOS.
2. Navigieren Sie zu „System BIOS“ > „System Security“ und nehmen Sie folgende Einstellungen vor:
 - System Password (beachten Sie die angeführten Passwortrichtlinien)
 - Setup Password (beachten Sie die angeführten Passwortrichtlinien)

3. Navigieren Sie zu „TPM Security“ und wählen Sie „On with Pre-boot Measurements“ aus.
4. Wählen Sie `Back` und speichern Sie die Einstellungen mit `Finish`. Dabei müssen Sie die Frage zum Speichern mit `Yes` bestätigen.
5. Starten Sie den Node neu.

4.3 Festplatten-Einstellungen

Fabasoft empfiehlt die Schlüssel für die Self Encrypting Disks der Fabasoft Private Cloud Nodes zu ändern. Die Schlüssel werden automatisch vom RAID-Controller generiert. Sie benötigen dazu die bestehende Passphrase, die initial bei der Vorbereitung der Fabasoft Private Cloud von Fabasoft individuell je Node und je Kunde festgelegt worden ist. Die Passphrase wird von Fabasoft in einem Fabasoft Cloud Teamroom bereitgestellt. Um die Schlüssel zu ändern, gehen Sie folgendermaßen vor:

1. Wechseln Sie während des Startvorgangs des Nodes mit `F2` ins BIOS.
2. Drücken Sie `CTRL + R` während der BIOS-Bildschirm bezüglich des Raid-Controllers angezeigt wird. Das Virtual Disk Management wird gestartet.
3. Navigieren Sie mit der Tastatur zur ersten Zeile (PERC H710P Mini) und drücken Sie `F2`.
4. Navigieren Sie zu „Security Key Management“ und drücken Sie `Enter`.
5. Navigieren Sie zu „Change Key“ und drücken Sie `Enter`.
6. Legen Sie eine neue Passphrase fest.
7. Speichern Sie die Einstellungen mit `OK` und geben Sie die alte Passphrase an.
8. Nach Bestätigung verlassen Sie das Virtual Disk Management mit `ESC` und starten Sie den Node neu.

4.4 Netzwerk-Konfiguration

Verbinden Sie sich auf die Konsole, um die Netzwerk-Konfiguration der Nodes vornehmen zu können. Dies ist von Ihrem Arbeitsplatz mit Dell iDRAC möglich. Navigieren Sie zu „Übersicht“ > „Server“ und klicken Sie unter *Virtuelle Konsolenvorschau* auf „Starten“.

Melden Sie sich am Betriebssystem mit dem Benutzer `root` und dem Passwort `changeit` an. Ein Wizard für die Konfiguration der Netzwerk-Einstellung wird automatisch gestartet. Führen Sie diesen auf beiden Nodes nacheinander vollständig durch.

Hinweis: Das Ändern der Passwörter auf einen von Ihnen definierten Wert erfolgt im Rahmen der später folgenden Fabasoft Private Cloud Installation.

5 Fabasoft Private Cloud Installation

Nach erfolgreicher Netzwerk-Konfiguration können Sie die Fabasoft Private Cloud Installation starten. Verbinden Sie sich dazu mit einem Webbrowser über die IP-Adresse auf einen der beiden Fabasoft Private Cloud Nodes und melden Sie sich mit dem Benutzernamen `management` und dem Passwort `changeit` am Fabasoft Private Cloud Management an. Folgen Sie den Anweisungen des Installations-Wizards. Fahren Sie nach Abschluss des Installations-Wizards mit Kapitel 6 „Fabasoft Private Cloud Organisation“ fort.

Hinweis: Im Rahmen der Installation werden alle Passwörter auf einen von Ihnen definierten Wert geändert.

6 Fabasoft Private Cloud Organisation

Nach erfolgreicher Installation können Sie über das Fabasoft Private Cloud Management Ihre Organisation initial einrichten und die Benutzer festlegen.

1. Klicken Sie auf die Aktion „Configure Organization“, um die Organisation in der Fabasoft Private Cloud zu öffnen.
2. Melden Sie sich als Organisations-Administrator (Benutzername: `orgadmin`) mit dem bei der Installation festgelegten Passwort an.

Das Dashboard der Organisation wird direkt geöffnet. Legen Sie in einem ersten Schritt die Benutzer und Anmeldedaten fest. Die nachfolgenden Kapitel unterstützen Sie dabei.

Achtung: Der Benutzer `orgadmin` ist standardmäßig Eigentümer sowie Administrator der Organisation. Eigentümer haben Zugriff auf alle Teamrooms der Organisation und können somit alle Daten einsehen. Administratoren können die Mitglieder verwalten, haben aber keinen Zugriff auf die Teamrooms der Organisation. In Kapitel 6.5 „Eigentümer und Administratoren festlegen“ ist beschrieben, wie Sie diese ändern können.

Hinweis: Falls Ihr Client nicht optimal für die Verwendung der Fabasoft Private Cloud konfiguriert ist, wird dies durch ein Warnsymbol (Webbrowserstatus) in der Kopfzeile angezeigt. Klicken Sie gegebenenfalls auf das Symbol und folgen Sie den Anweisungen, um die optimale Konfiguration herzustellen.

6.1 Anmeldung mit Client-Zertifikaten

Benutzer können sich mit Client-Zertifikat und/oder mit Benutzername und Passwort anmelden. Zusätzlich wird die Anmeldung durch den zweiten Faktor E-Mail-PIN abgesichert. Wenn Sie eine zertifikatsbasierte Anmeldung bereitstellen möchten, müssen Sie die Zertifizierungsstellen in der Organisation hinterlegen.

1. Klicken Sie in der Organisation auf die Aktion „Zertifikatseinstellungen festlegen“.
2. Laden Sie die ausstellenden Zertifizierungsstellen für Ihre Client-Zertifikate als CER-Dateien im PEM-Format hoch. Führen Sie dazu im Feld *Ausstellende Zertifizierungsstellen für Client-Zertifikate* den Menübefehl „Zertifikat“ > „Hochladen“ aus. Wählen Sie die entsprechende CER-Datei im Dateisystem aus und bestätigen Sie das Hochladen.
3. Falls es übergeordnete Stamm- und Zwischenzertifizierungsstellen für die ausstellenden Zertifizierungsstellen gibt, müssen diese ebenfalls als CER-Dateien im PEM-Format im entsprechenden Feld hochgeladen werden.
4. Geben Sie für alle Zertifizierungsstellen die Zertifikatssperlisten-URLs (CRLs) an.
5. Klicken Sie auf „Weiter“, um die Änderungen zu speichern.

6.2 Mitglieder hinzufügen

Um Benutzern den Zugriff auf die Fabasoft Private Cloud zu ermöglichen, müssen diese als Mitglieder zur Organisation hinzugefügt werden.

Sie können die Mitglieder Ihrer Organisation per CSV-Import effizient erzeugen und auch aktualisieren. Zusätzlich besteht die Möglichkeit Mitglieder manuell anzulegen.

6.2.1 Mitglieder per CSV-Import erzeugen

Mithilfe des CSV-Imports können auch sehr viele Mitglieder komfortabel angelegt werden.

1. Klicken Sie im Dashboard der Organisation auf „Mitglieder“, um die Mitglieder-Liste zu öffnen.
2. Klicken Sie auf die Aktion „Mitglieder importieren“.
3. Über die Schaltfläche „CSV-Vorlage herunterladen“ erhalten Sie eine Vorlage, die die nötige Datenstruktur beschreibt.
4. Geben Sie im Feld *Inhalt* den Pfad zu der CSV-Datei ein, die die Mitglieder definiert.
5. Klicken Sie auf „Import starten“.
6. Nachdem der Import abgeschlossen wurde, klicken Sie auf „Weiter“.

Die importierten Mitglieder werden in der Mitglieder-Liste abgelegt. Bei einem erneuten Import, werden bereits bestehende Mitglieder aktualisiert. Die eindeutige Identifizierung der Mitglieder erfolgt über die E-Mail-Adresse.

Über die Aktion „Mitglieder einladen“ können Sie eine Einladungs-E-Mail an die importierten Mitglieder schicken (siehe Kapitel 6.3 „Mitglieder einladen“).

Datenstruktur der CSV-Datei

CSV-Spalte	Beschreibung
EMail	E-Mail-Adresse für die Anmeldung (eindeutig; erforderlich)
CN	Common Name (wird für die Anmeldung mit Client-Zertifikat benötigt und muss mit dem CN des Client-Zertifikats des jeweiligen Benutzers übereinstimmen)
PinEMail	E-Mail-Adresse, an die die E-Mail-PIN gesendet wird (wenn nichts angegeben wurde, wird die E-Mail-Adresse für die Anmeldung verwendet)
FirstName	Vorname (erforderlich)
MiddleInitial	weitere Vornamen
Surname	Nachname (erforderlich)
Title	Titel
PostTitle	nachgestellter Titel
Sex	Geschlecht (mögliche Werte: <code>SEX_FEMALE</code> und <code>SEX_MALE</code>)

Salutation	Anrede
Birthday	Geburtsdatum (Format: dd-mm-yyyy)
Street	Straße
ZipCode	Postleitzahl
City	Ort
State	Bundesland
Country	Land
Phone	Telefonnummer (geschäftlich)
Fax	Telefonnummer (Fax)
Mobile	Telefonnummer (mobil)
PrivatePhone	Telefonnummer (privat)
Function	Funktion in der Organisation
OrgUnitKey	Importkennung der Organisationseinheit (wenn keine Organisationseinheit mit der Importkennung gefunden wird, wird eine neue erzeugt, sonst wird gegebenenfalls der Name aktualisiert)
OrgUnitName	Name der Organisationseinheit
Website	Website
Language	Sprache (Schreibweise entsprechend der Sprache z. B. Español; die möglichen Werte finden Sie in der CSV-Vorlage oder in den „Grundeinstellungen“ unter <i>Sprache</i>)

Hinweis: Um mehrere Adressen zu hinterlegen oder Mitglieder mehreren Organisationseinheiten zuzuordnen, können in der CSV-Datei mehrere Zeilen mit derselben E-Mail-Adresse (EMail) angegeben werden.

6.2.2 Mitglieder manuell erzeugen

Zusätzlich zum CSV-Import können Mitglieder auch einzeln angelegt und administriert werden.

1. Klicken Sie in der Organisation auf die Aktion „Mitglieder hinzufügen“.
2. Führen Sie im Feld *Mitglieder hinzufügen* den Menübefehl „Kontakt“ > „Neu“ aus.
3. Geben Sie die Daten des Mitglieds ein und klicken Sie auf „Weiter“.

4. Um mehrere Mitglieder gleichzeitig hinzuzufügen, wiederholen Sie Schritt 2 und 3.
5. Klicken Sie auf „Einladung versenden“, um pro Mitglied eine E-Mail mit einem Link zum initialen Festlegen des Passworts zu senden. Klicken Sie auf „Nur hinzufügen“, um die Einladung später zu versenden (siehe Kapitel 6.3 „Mitglieder einladen“).

Die erzeugten Mitglieder können über den Kontextmenübefehl „Eigenschaften“ noch weiter bearbeitet werden.

6.3 Mitglieder einladen

Wenn Sie einen CSV-Import durchgeführt haben bzw. manuell hinzugefügte Mitglieder noch nicht direkt beim Hinzufügen eingeladen haben, können Sie dies über die Aktion „Mitglieder einladen“ nachholen.

Bei Anmeldung über Benutzername und Passwort ist die Einladungs-E-Mail mit einem individuellen Link für das initiale Festlegen des Passworts zwingend erforderlich. Wenn die Anmeldung ausschließlich über Zertifikat erfolgen soll, muss keine Einladung verschickt werden.

1. Klicken Sie auf die Aktion „Mitglieder einladen“. Die Aktion ist nur sichtbar, wenn noch einzuladende Mitglieder vorhanden sind.
2. Die Felder *An*, *Betreff* und *Nachricht* sind bereits vorbefüllt. Nehmen Sie gegebenenfalls entsprechende Anpassungen vor.
3. Klicken Sie auf „Senden“.

Es wird eine E-Mail mit einem Link zum initialen Festlegen des Passworts an die Mitglieder versendet.

6.4 Servicedesk einrichten

Die über die Support-Schaltfläche eingebrachten Anfragen können im Servicedesk abgearbeitet werden. Auf „Home“ finden Sie die Servicedesk-Konfiguration, in der Sie die App-Administratoren und App-Benutzer festlegen können. App-Administratoren können die Konfiguration bearbeiten und App-Benutzer repräsentieren die Servicedesk-Mitarbeiter.

App-Administratoren festlegen

1. Klicken Sie in der Servicedesk-Konfiguration auf die Aktion „Team berechtigen“.
2. Klicken Sie auf das Plus-Symbol neben dem Feld *App-Administrator*.
3. Geben Sie die E-Mail-Adresse des gewünschten Benutzers ein und bestätigen Sie mit „Enter“.

Bei den hinzugefügten App-Administratoren werden die Servicedesk-Konfiguration und das Servicedesk-Dashboard auf „Home“ abgelegt.

App-Benutzer festlegen

1. Klicken Sie in der Servicedesk-Konfiguration auf die Aktion „Team berechtigen“.
2. Klicken Sie auf das Plus-Symbol neben dem Feld *App-Benutzer*.
3. Geben Sie die E-Mail-Adresse des gewünschten Benutzers ein und bestätigen Sie mit „Enter“.

Bei den hinzugefügten App-Benutzern wird das Servicedesk-Dashboard auf „Home“ abgelegt. Über das Dashboard können die Support-Anfragen abgearbeitet werden.

6.5 Eigentümer und Administratoren festlegen

Nach Abschluss der initialen Konfiguration über das Fabasoft Private Cloud Management sollten die administrativen Aufgaben entsprechenden Organisationsmitgliedern übergeben werden. Dazu können bei der Organisation Eigentümer und Administratoren festgelegt werden. Eigentümer haben Zugriff auf alle Teamrooms der Organisation und können somit alle Daten einsehen. Administratoren können die Mitglieder verwalten, haben aber keinen Zugriff auf die Teamrooms der Organisation.

Administratoren festlegen

1. Klicken Sie in der Organisation auf die Aktion „Einstellungen“.
2. Wechseln Sie auf die Registerkarte „Administratoren“.
3. Wählen Sie im Feld *Administratoren* über die Suche einen zusätzlichen Administrator oder eine Organisationseinheit aus.
4. Wenn Informationen, die die Organisation betreffen (z. B. akzeptierte Einladungen), nicht an alle Administratoren per E-Mail gesendet werden sollen, legen Sie einen Hauptadministrator fest.
5. Klicken Sie auf „Weiter“.

Miteigentümer festlegen

1. Klicken Sie in der Organisation auf die Aktion „Einstellungen“.
2. Wechseln Sie auf die Registerkarte „Eigentümer“.
3. Wählen Sie im Feld *Miteigentümer* über die Suche einen zusätzlichen Miteigentümer oder eine Organisationseinheit aus.

Eigentümer der Organisation ändern

Achtung: Nur der Eigentümer der Organisation kann einen neuen Eigentümer festlegen. Der alte Eigentümer kann die Organisation nicht mehr verwalten.

1. Klicken Sie im Dashboard der Organisation auf „Mitglieder“, um die Mitglieder-Liste zu öffnen.
2. Klicken Sie auf die Aktion „Eigentümer der Organisation ändern“.
3. Wählen Sie aus den Mitgliedern der Organisation einen neuen Eigentümer aus.
Hinweis: Es können nur Mitglieder ausgewählt werden, die entweder einen *Common Name* (zertifikatsbasierte Anmeldung) hinterlegt haben bzw. bereits ihr Passwort festgelegt haben.
4. Klicken Sie auf „Weiter“.

7 Server-Zertifikate

Der Zugriff auf die Fabasoft Private Cloud und auf das Fabasoft Private Cloud Management ist ausschließlich über HTTPS möglich. Standardmäßig wird ein von der Fabasoft Private Cloud selbstsigniertes Zertifikat konfiguriert.

Um ein eigenes Zertifikat zu hinterlegen, gehen Sie folgendermaßen vor:

1. Falls Sie das Fabasoft Private Cloud Management geschlossen haben, verbinden Sie sich erneut mit einem Webbrowser über die IP-Adresse auf einen der beiden Fabasoft Private Cloud Nodes

und melden Sie sich mit dem Benutzernamen `management` und dem von Ihnen bei der Installation festgelegten Passwort an.

2. Klicken Sie auf die Aktion „Manage HTTPS Certificates“.
3. Wechseln Sie zu dem gewünschten Zugang („Management Access“ oder „Fabasoft Private Cloud Access“), für den Sie das Server-Zertifikat erstellen möchten.
4. Klicken Sie auf die Schaltfläche „Generate CSR“, um einen Certificate Signing Request (CSR) zu generieren.
5. Geben Sie die notwendigen Daten ein.
Hinweis: Im *CN (Common Name)* müssen Sie den Fully Qualified Domain Name (FQDN) festlegen, über den Ihre Benutzer auf die Fabasoft Private Cloud zugreifen.
6. Klicken Sie auf die Schaltfläche „Create“. Lassen Sie mit dem generierten CSR bei Ihrer CA bzw. Ihrem externen Zertifikats-Provider das Zertifikat ausstellen.
Hinweis: Für eine Authentifizierung mit Client-Zertifikaten ist ein zusätzlicher SAN im Zertifikat für die Private Cloud für `cert.<FQDN des Fabasoft Private Cloud Zugangs>` erforderlich. Wenn Sie beispielsweise `cloud.example.com` für den Fabasoft Private Cloud Zugang verwenden, fordern Sie den zusätzlichen SAN `cert.cloud.example.com` im Zertifikat an.
7. Importieren Sie das erstellte Zertifikat im Fabasoft Private Cloud Management.

8 Weiterführende Dokumente

Weiterführende Themen finden Sie in folgenden Dokumenten:

- Operations Manual Fabasoft Private Cloud
In diesem Dokument erhalten Sie Informationen zur Betriebsführung und zum Einrichten der Arbeitsplätze.
- Administrationshilfe Fabasoft Private Cloud
Dieses Dokument beschreibt die Konfigurationsmöglichkeiten einer Fabasoft Private Cloud Organisation.
- Benutzerhilfe Fabasoft Private Cloud
Die Endbenutzerhilfe finden Sie in diesem Dokument.