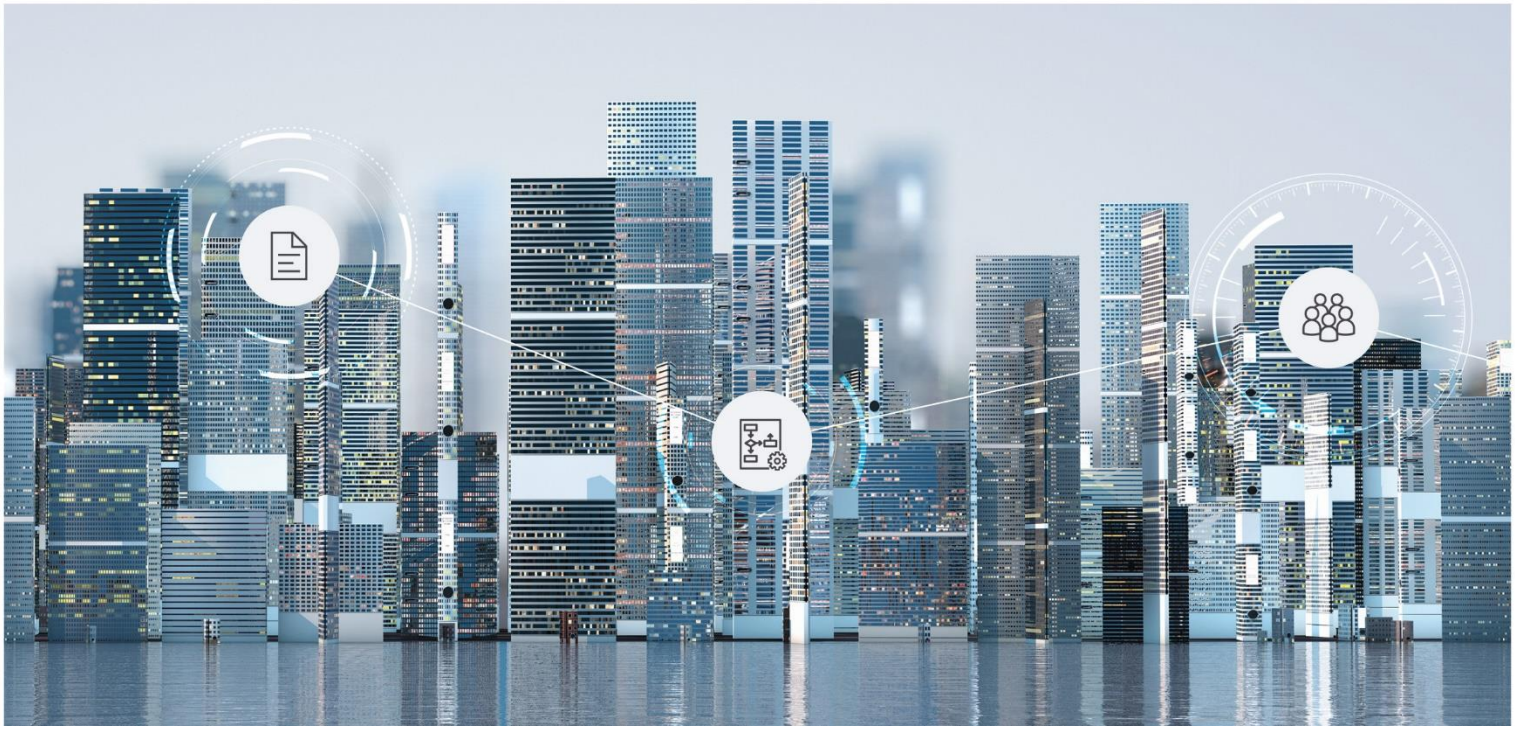
Fabasoft



Erste Schritte

Fabasoft Private Cloud

2022 June Release

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

Willkommen in der Fabasoft Private Cloud.

Diese Kurzübersicht zeigt Ihnen, was Sie für Ihre Fabasoft Private Cloud vorbereiten müssen und begleitet Sie bis zum initialen Einrichten Ihrer Organisation in der Fabasoft Private Cloud.

2 Hardware-Komponenten

Die Fabasoft Private Cloud besteht aus zwei Dell R740 Server (rackmount). Der Server wird mit der folgenden – für den Einbau in Serverschränke relevanten - Konfiguration bereitgestellt:

Konfiguration	
Power Supply	1 Dual, Hot-plug, Redundant Power Supply (1+1), 1100W
Rackmount	ReadyRails Gleitschienen mit Kabelführungsarm
Reck Height	2U

Je Server sind folgende Anbindungen erforderlich:

Anbindungen		
Power	Power Supply	2 x C13
Netzwerk	Customer-LAN	2 x 10 Gbps Ethernet **Cu** (empfohlen) oder 2 x 1 Gbps Ethernet **Cu**
	Interconnect Services (Services-LAN)	2 x 10 Gbps Ethernet **Cu** (empfohlen) oder 2 x 1 Gbps Ethernet **Cu**
	Interconnect Cluster (Cluster-LAN)	2 x 10 Gbps Ethernet **Cu** (empfohlen) oder 2 x 1 Gbps Ethernet **Cu**
	Management-LAN (iDRAC)	1 x 1 Gbps Ethernet **Cu**

3 Systemkonfiguration

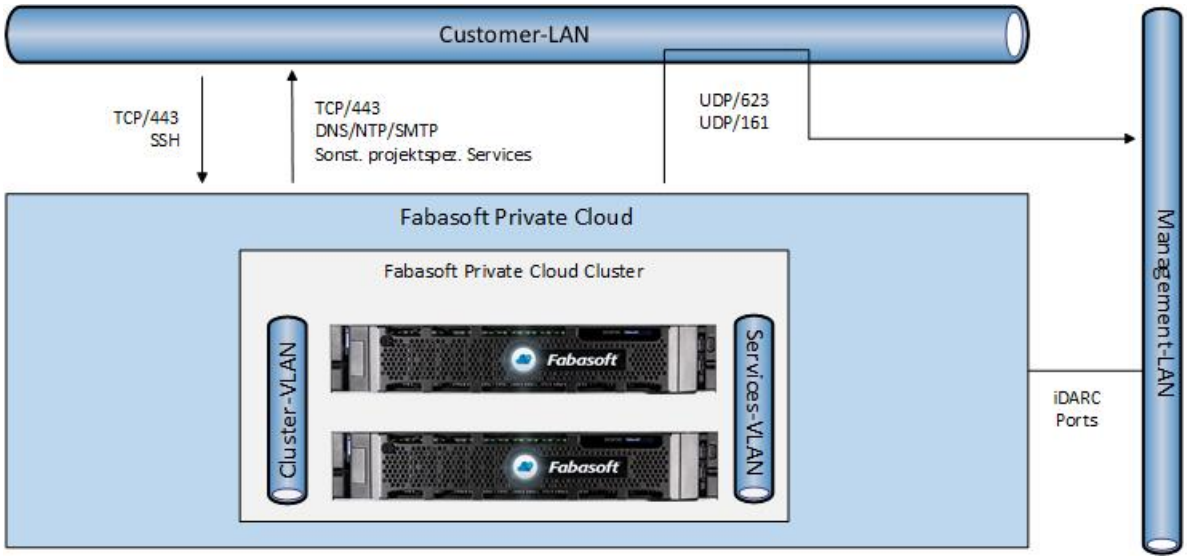
3.1 Allgemeines

Aus Gründen der Ausfallsicherheit wird eine örtlich verteilte Installation der Server empfohlen, wobei für die Cluster- und Services-Kommunikation eine Round Trip Time (RTT) von < 2 ms zwischen den beiden Servern erforderlich ist.

Die Strom- und Netzwerk-Anbindung sollte redundant erfolgen. Jeder Server soll an zwei unterschiedliche Stromkreise angebunden werden. Die Netzwerk-Ports für das Customer-LAN, die Cluster- und Services-Kommunikation sollen an unterschiedliche Switches angeschlossen werden.

3.2 Netzwerkübersicht

Die grundlegende Netzwerkarchitektur der Fabasoft Private Cloud sieht folgendermaßen aus:



Auf die Fabasoft Private Cloud wird via Customer-LAN über Port TCP/443 (HTTPS) zugegriffen. Die Services der Fabasoft Cloud benötigen einen Zugriff via Customer-LAN auf DNS, NTP und SMTP, den Backup-Server bzw. sonstige projektspezifische Services, die über Schnittstellen eingebunden werden.

Des Weiteren müssen die Ports UDP/623 bzw. UDP/161 vom Customer-LAN in das Management-LAN freigeschalten werden.

Der Fabasoft app.telemetry Server ist ebenfalls über Port TCP/443 zugänglich.

Für die Administration der Fabasoft Private Cloud Server und Services ist ein Zugang via SSH erforderlich.

Für die Kommunikation zwischen den Services der Fabasoft Private Cloud sowie für die Kommunikation im Cluster ist je ein VLAN zwischen den beiden Cluster-Knoten der Fabasoft Private Cloud einzurichten.

Für die Cluster- und Services-Kommunikation wird eine **MTU von 9000 Byte** verwendet, somit müssen auf dem gesamten Pfad zwischen den Servern der Fabasoft Private Cloud **Jumbo-Frames aktiviert** sein.

Die Netzwerkanbindungen an das Customer-LAN, Services-LAN und Cluster-LAN sind redundant ausgelegt. Die beiden Interfaces je LAN jedes Servers haben ein Bonding, somit ist kein LACP am Switch notwendig.

Beide Server haben je eine eigene IP im Customer LAN. Die „Loadbalancer IP" wird zusätzlich über den Cluster auf den Server auf dem die „Loadbalancer IP" läuft zugewiesen. Die „Loadbalancer IP" macht gegebenenfalls einen Failover somit ist auch dafür kein LACP am Switch notwendig.

Für ein Update der Fabasoft Private Cloud muss auf den Repository-Server **https://repo.cloud.fabasoft.com** über Port 443 zugegriffen werden können.

3.3 Anforderungen für die Inbetriebnahme

- 2 IPv4-Adressen für das Management-LAN (Dell iDRAC)
- 3 IPv4-Adressen für das Customer-LAN (eine je Server in RZ1, RZ2 und eine Cluster IP-Adresse)
- VLAN für Cluster-LAN (verwendet von den Servern in RZ1 und RZ2)
- VLAN für Services-LAN (verwendet von den Servern in RZ1 und RZ2)
- Für die Cluster- und Services-Kommunikation wird eine MTU von 9000 Byte verwendet, somit müssen auf dem gesamten Pfad zwischen den Servern der Fabasoft Private Cloud Jumbo-Frames aktiviert sein.
- Für die Cluster- und Services-Kommunikation wird eine Round Trip Time (RTT) von < 2 ms erwartet.
- Zwischen dem Customer-LAN und dem Management-LAN muss folgende Firewall-Freischaltung gegeben sein:
  - Customer-LAN → Management-LAN: **UDP Port 623**
  - Customer-LAN → Management-LAN: **UDP Port 161 (SNMP)**
- Fully Qualified Domain Name (FQDN) inkl. DNS-Eintrag und Serverzertifikat für den HTTPS-Zugang
- Falls für die Anmeldung Client-Zertifikate zum Einsatz kommen soll: Ein DNS-Eintrag und ein Serverzertifikat für cert.<FQDN> für die Authentisierung mit Client-Zertifikaten. Es muss ein separates Serverzertifikat sein. Das Serverzertifikat des HTTPS-Zugangs darf nicht wiederverwendet werden.
- DNS-Server
- NTP-Server
- SMTP-Server
- Backup-Server

3.4 Authentisierung

3.4.1 Administration der Fabasoft Private Cloud Server und Services

Für die Administration der Fabasoft Cloud Server bzw. Services kann über SSH auf die jeweiligen Server bzw. in weiterer Folge auf die Management-VM und von dort auf die unterschiedlichen servicespezifischen VMs als root User eingestiegen werden.

3.4.2 Administration in der Fabasoft Private Cloud Browser-Oberfläche

Für die Administration in der Fabasoft Private Cloud Browser-Oberfläche können entweder Benutzername/Passwort mit E-Mail-PIN, Client-Zertifikate oder ADFS/SAML 2.0 verwendet werden.

Bei der Authentisierung mit Client-Zertifikate werden Benutzer über den CN des Client-Zertifikats zugeordnet. Für die Konfiguration der Anmeldung mit Client-Zertifikaten müssen

- alle Zertifizierungsstellen, die Client-Zertifikate für Ihre Organisation ausstellen dürfen, als CER-Dateien im PEM-Format,
- für die ausstellenden Zertifizierungsstellen die übergeordneten Stamm- und Zwischenzertifizierungsstellen als CER-Dateien im PEM-Format und
- für jede Stamm-, Zwischen- und ausstellende Zertifizierungsstelle die entsprechenden Zertifikatssperrlisten-URLs

in der Fabasoft Private Cloud hinterlegt werden.

4 Erforderliche Informationen vor dem Versand der Fabasoft Private Cloud

Wir installieren in Ihrer Fabasoft Private Cloud schon vorab Ihr zukünftiges System und bereiten dieses teilweise bereits vor. Dafür brauchen wir von Ihnen einige Informationen.

Lieferanschrift	
Vollständige Adresse, an die wir die Server liefern sollen	
Sonstige Anmerkungen zur Lieferung	

Name der Fabasoft Private Cloud und der Organisation	
Fully Qualified Domain Name (FQDN) Über diesen Namen greifen die Benutzer auf Ihre Fabasoft Private Cloud zu (z.B. https://cloud.myorg.com/cloud).	
Name der Fabasoft Private Cloud (z.B. Myorg Cloud)	
Name der Cloud-Organisation (z.B. Myorg)	

Sonstige Einstellungen (können auch nachträglich geändert werden)

E-Mail-Adresse der Organisation (optional)	
Logo Ihrer Organisation als SVG- bzw. PNG-Datei mit transparentem Hintergrund	
Zum Logo passende Hintergrundfarbe im Kopfbereich und auf der Loginseite	
No Reply E-Mail-Adresse E-Mail-Adresse für Mails auf die nicht geantwortet werden soll.	
Absender E-Mail-Adresse E-Mail-Adresse, die als Absender verwendet wird, wenn E-Mails im Auftrag von Benutzern verschickt werden.	

Initiale Benutzer	
Wir legen für Sie initial einen Eigentümer und optional bis zu drei Administratoren für Ihre Cloud Organisation an. Die Benutzer werden mit einem Standardpasswort angelegt, dass Ihnen auf separatem Weg übermittelt wird. Sie sollten nach der Installation der Private Cloud in Ihrem Rechenzentrum die Passwörter dieser Benutzer ändern. Mehr zu den Rollen einer Cloud Organisation erfahren Sie unter: http://help.privatecloud.fabasoft.com/index.php?topic=doc/Administrationshilfe-Fabasoft-Private-Cloud-ger/organisationsrollen.htm	
Eigentümer der Cloud Organisation Kann auf alle Objekte der Organisation zugreifen, Miteigentümer und Organisationsadministratoren verwalten. Es wird empfohlen, einen virtuellen Benutzer zu verwenden, der in der Regel nicht interaktiv tätig ist. Für die Änderung des Passworts muss auf das Postfach dieses Benutzers zugegriffen werden können.	
Vorname	
Nachname	
E-Mail-Adresse	
Standardsprache	Deutsch/Englisch
Optional: Administrator 1 der Cloud Organisation	

Vorname	
Nachname	
E-Mail-Adresse	
Standardsprache	Deutsch/Englisch
Optional: Administrator 2 der Cloud Organisation	
Vorname	
Nachname	
E-Mail-Adresse	
Standardsprache	Deutsch/Englisch
Optional: Administrator 3 der Cloud Organisation	
Vorname	
Nachname	
E-Mail-Adresse	
Standardsprache	Deutsch/Englisch

Netzwerkkonfiguration für die Management-Interfaces (Dell iDRAC)			
Server 1 (IPv4-Adresse, Mask, Gateway)			
Server 2 (IPv4-Adresse, Mask, Gateway)			
Netzwerkkonfiguration für die Customer-LAN-Anbindung der Nodes			
Server 1 (IPv4-Adresse, Mask, Gateway)			
Server 2 (IPv4-Adresse, Mask, Gateway)			
Konfiguration für den Benutzerzugriff auf die Fabasoft Private Cloud im Customer-LAN			
IPv4-Adresse (Customer-LAN, daher gleiches Subnet wie die IPv4-Adressen der Nodes oben)			
Fully Qualified Domain Name (FQDN) (siehe oben z.B. cloud.myorg.com)			

DNS-Eintrag und Serverzertifikat (HTTPS-Zugang) für den FQDN (z.B. cloud.myorg.com)	
DNS-Eintrag und Serverzertifikat (HTTPS-Zugang) für cert.<FQDN> (z.B. cert.cloud.myorg.com)	
Einbindung in die bestehenden Infrastruktur-Services	
DNS-Server	
NTP-Server	
SMTP-Server (inkl. Port, Standard 25)	
Backup-Share (SMB/CIFS oder NFS)	
Zugangsdaten zum Backup-Share	

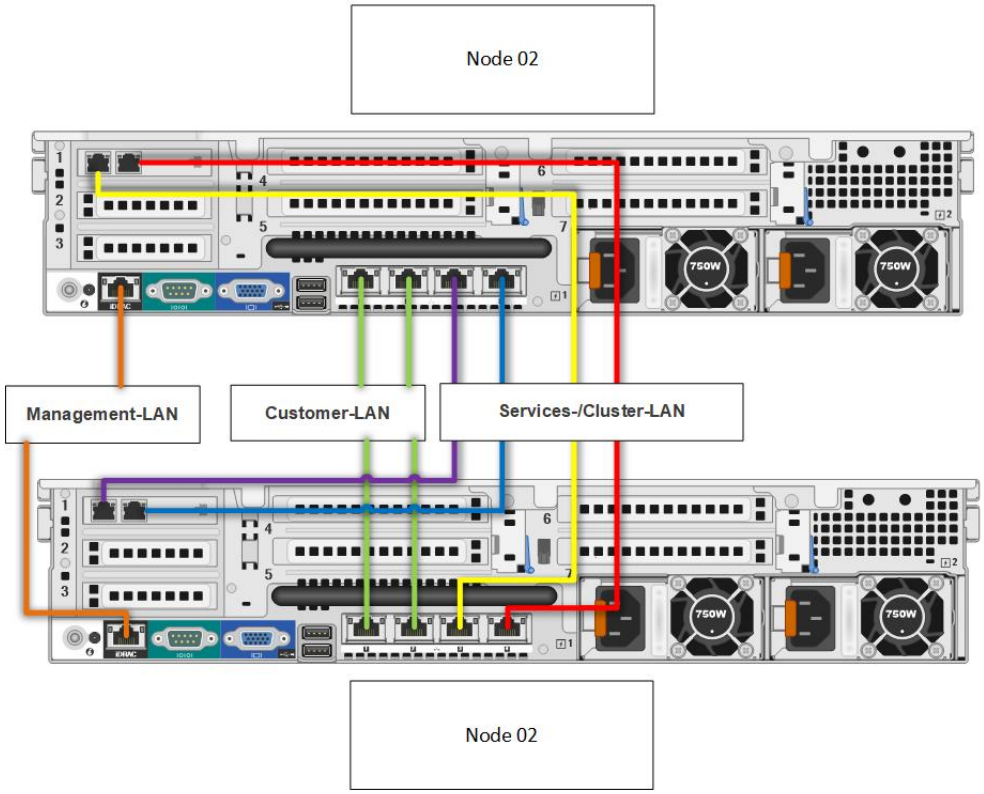
5 Vorbereitung für die Installation in Ihrer Infrastruktur

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

Einbindung in die bestehenden Infrastruktur-Services	
Zugangsdaten zum Backup-Share	

6 Voraussichtlicher Anschlussplan

Fabasoft Private Cloud/Fabasoft Personalakte
Anschlussplan



Die Netzwerk-Anbindung ist folgendermaßen vorgesehen:

- Customer-LAN
  Netzwerk-Ports 1 und 2
- Services-LAN
  Netzwerk-Ports 3 und 5
- Cluster-LAN
  Netzwerk-Ports 4 und 6
- Management-LAN
  Netzwerk-Port „iDRAC“ (Zugriff durch Administratoren auf Dell iDRAC)

7 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)

8 Server-Konfiguration

Führen Sie die nachfolgenden Konfigurationsschritte auf beiden Nodes durch.

8.1 Dell iDRAC

8.1.1 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.

8.1.2 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, das Sie von uns übermittelt bekommen, an.
   Nach der ersten Anmeldung sollten Sie das Passwort ändern.
3. Navigieren Sie zu „Übersicht“ > „iDRAC-Einstellungen“ > „Netzwerk“ > „IPv4-Einstellungen” und nehmen Sie folgende Einstellungen vor:
   - Statischer bevorzugter DNS-Server
   - Statischer alternativer DNS-Server

   Bestätigen 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.

8.2 Festplatten-Einstellungen

Die Festplatten der Fabasoft Private Cloud werden mithilfe von LUKS verschlüsselt. Für das entschlüsseln der Festplatten während des Bootvorgangs existieren zwei Schlüssel. In „Key-Slot" 1 befindet sich der Schlüssel der vom TPM des Servers generiert wurde und für die automatische Entschlüsselung während des Bootvorgangs verwendet wird. Eine Änderung dieses Schlüssels ist nicht vorgesehen. In „Key-Slot" 0 befindet sich der Schlüssel für die manuelle Eingabe. Dieser Schlüssel wird nur im Notfall benötigt und sollte sicher aufbewahrt werden. Dieser Schlüssel kann mit den folgenden Schritten geändert werden.

1. Login mit `root` auf beiden Knoten.
2. Ändern des Passworts mittels `cryptsetup --key-slot 0 luksChangeKey /dev/sda3`.
3. Testen des neuen Passworts mit `cryptsetup --test-passphrase luksOpen /dev/sda3`.

9 Fabasoft Private Cloud Organisation

Nach erfolgreicher Installation können Sie den Fabasoft Webbrowser Client Ihre Organisation initial einrichten und die Benutzer festlegen.

Melden Sie sich dazu als Organisations-Administrator mit dem Ihnen übermittelten Benutzer und Passwort an.

Das Dashboard der Organisation finden Sie im Home-Bereich. Legen Sie in einem ersten Schritt die Benutzer und Anmeldedaten fest. Die nachfolgenden Kapitel unterstützen Sie dabei.

Achtung: 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 9.4 „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.

9.1 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.

9.1.1 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 9.2 „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: `SEX_FEMALE` und `SEX_MALE`)
`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 *Sprache*)

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.

9.1.2 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 9.2 „Mitglieder einladen“).

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

9.2 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.

9.3 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.

9.4 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“.

10 Services der Fabasoft Private Cloud

10.1 Hypervisoren

Auf den beiden Knoten der Fabasoft Private Cloud werden die Services in Virtuellen Maschinen betrieben.

Die Knoten der Fabasoft Private Cloud kommunizieren über zwei IPsec Tunnel auf den direkt verbundenen Netzwerkinterfaces.

Ein Tunnel wird dabei für die Clusterkommunikation verwendet, der zweite Tunnel für die Kommunikation zwischen den Virtuellen Maschinen.

Die in Punkt 10.2 beschriebenen Virtuellen Maschinen werden mittels Pacemaker Cluster hochverfügbar betrieben. Die Disken werden dabei mittels DRBD zwischen den Knoten synchron gehalten.

Die in Punkt 10.3 beschriebenen Virtuellen Maschinen werden mit je einer Instanz auf den beiden Fabasoft Private Cloud Konten betrieben.

Statusabfrage:

IPsec Tunnel: `ipsec status`

DRBD: `drbdadm status`

Pacemaker Cluster: `pcs status`

Virtuelle Maschinen: `virsh list`

10.2 Hochverfügbar betriebene Virtuelle Maschinen

- <CUSTOMER>-auth-01:

  Der Service `fscidpd` des Fabasoft Private Cloud Identity Provider wird mittels `systemctl` gesteuert. Die Logfiles sind unter `/var/opt/fabasoft/log` zu finden

  Der Service `slapd` des LDAP Server wird mittels `systemctl` gesteuert. Das Logfile ist unter `/var/log/ldap.log` zu finden

- <CUSTOMER>-db-01:

  Der Service `postgresql-<version>` der PostgreSQL Datenbank wird mittels `systemctl` gesteuert. Die Logfiles sind unter `/data/db1/pgdata/pg_log` zu finden.

  Die Fabasoft Private Cloud Backendservices werden mittels `/opt/fabasoft/bin/fscmgmt` gesteuert. Die Logfiles sind unter `/var/opt/fabasoft/log` zu finden.

- <CUSTOMER>-lb-01:

  Der Service `nginx_cloud` des nginx Loadbalancers wird mittels `systemctl` gesteuert. Die Logfiles sind unter `/var/log/nginx` zu finden.

- <CUSTOMER>-mgmt-01:

  Die Services des Chef Servers werden mittels `chef-server-ctl` gesteuert. Die Logfiles sind unter `/var/log/opscode` zu finden.

  Die Management Virtuelle Maschine wird genutzt um die anderen Virtuellen Maschinen per SSH zu erreichen

- <CUSTOMER>-mon-01:

  Die Services des Fabasoft app.telemetry Servers werden mittels `systemctl` gesteuert. Die Logfiles sind unter `/var/log/app.telemetry` zu finden.

10.3 Mehrfach instanziierte Virtuelle Maschinen

- <CUSTOMER>-conv-01/<CUSTOMER>-conv-02:

  Die Fabasoft Private Cloud Konvertierungsservices werden mittels `/opt/fabasoft/bin/fscmgmt` gesteuert. Die Logfiles sind unter `/var/opt/fabasoft/log` zu finden.

  Die Fabasoft Data Transformation Services werden mittel `docker-compose` gesteuert.

  Die Konfiguration liegt unter `/root/Docker`. Die Logs können über `docker-compose` ausgelesen werden.

- <CUSTOMER>-at-01/<CUSTOMER>-at-02:

Die Fabasoft Private Cloud AT-Services werden mittels `/opt/fabasoft/bin/fscmgmt` gesteuert. Die Logfiles sind unter `/var/opt/fabasoft/log` zu finden.

- <CUSTOMER>-web-01/<CUSTOMER>-web-02:

  Die Fabasoft Private Cloud Webservices werden mittels `/opt/fabasoft/bin/fscmgmt` gesteuert. Die Logfiles sind unter `/var/opt/fabasoft/log` zu finden.

- <CUSTOMER>-fs-01/<CUSTOMER>-fs-02:

  Der Service `smb` der Dateiserver wird mittels `systemctl` gesteuert. Die Logfiles sind unter `/var/log/samba` zu finden.

11 Server Stoppen bzw. Starten

11.1 Stoppen bzw. Starten eines Fabasoft Private Cloud Knotens

- Stoppen eines Knotens am Beispiel Knoten 2

  Failover der Services auf Knoten 1

  ```
  pcs cluster standby <node2>
  ```

  Prüfen des Failovers

  ```
  pcs status
  ```

  Stoppen der mehrfach instanziierten Virtuellen Maschinen

  ```
  virsh shutdown <CUSTOMER>-at-02
  virsh shutdown <CUSTOMER>-web-02
  virsh shutdown <CUSTOMER>-fs-02
  virsh shutdown <CUSTOMER>-conv-02
  ```

  Prüfen ob die Virtuellen Maschinen heruntergefahren wurden

  ```
  virsh list
  ```

  Herunterfahren des Knotens

  ```
  shutdown -h now
  ```

- Starten eines Knotens am Beispiel Knoten 2

  Starten des Knotens über Dell iDRAC

  Prüfen der beiden IPsec Tunnel

  ```
  ipsec status
  ```

  Aktivieren des Knotens

  ```
  pcs cluster unstandby <node2>
  ```

11.2 Stoppen bzw. Starten beider Fabasoft Private Cloud Knoten

- Stoppen der Knoten

  Aktivieren der Cluster Maintenance auf einem Knoten

  ```
  pcs property set maintenance-mode=true
  ```

  Auslesen der laufenden Virtuellen Maschinen auf beiden Knoten

```
virsh list
```

Stoppen der Virtuellen Maschinen auf beiden Knoten

```
virsh shutdown <VM>
```

Prüfen ob alle Virtuellen Maschinen heruntergefahren wurden

```
virsh list
```

Deaktivieren des automatischen Starts der Virtuellen Maschinen

Für `${CUSTOMER}-conv-01 ${CUSTOMER}-at-01 ${CUSTOMER}-web-01 ${CUSTOMER}-fs-01` auf Knoten 1 und `${CUSTOMER}-conv-02 ${CUSTOMER}-at-02 ${CUSTOMER}-web-02 ${CUSTOMER}-fs-02` auf Knoten 2

```
virsh autostart --disable <VM>
```

Herunterfahren beider Knoten

```
shutdown -h now
```

- Starten der Knoten

  Starten der Knoten über Dell iDRAC

  Prüfen der beiden IPsec Tunnel

  ```
  ipsec status
  ```

  Deaktivieren der Cluster Maintenance auf einem Knoten

  ```
  pcs property set maintenance-mode=false
  ```

  Aktivieren des automatischen Starts der Virtuellen Maschinen

  Für `${CUSTOMER}-conv-01 ${CUSTOMER}-at-01 ${CUSTOMER}-web-01 ${CUSTOMER}-fs-01` auf Knoten 1 und `${CUSTOMER}-conv-02 ${CUSTOMER}-at-02 ${CUSTOMER}-web-02 ${CUSTOMER}-fs-02` auf Knoten 2

  ```
  virsh autostart <VM>
  ```

  Starten der Virtuellen Maschinen

  Knoten 1

  ```
  virsh start <CUSTOMER>-fs-01
  ```

  Knoten 2

  ```
  virsh start <CUSTOMER>-fs-02
  ```

  Knoten 1

  ```
  virsh start <CUSTOMER>-web-01
  virsh start <CUSTOMER>-conv-01
  virsh start <CUSTOMER>-at-01
  ```

  Knoten 2

  ```
  virsh start <CUSTOMER>-web-02
  virsh start <CUSTOMER>-conv-02
  virsh start <CUSTOMER>-at-02
  ```

12 Server-Zertifikate

Der Zugriff auf die Fabasoft Private Cloud ist ausschließlich über HTTPS möglich.

Um ihre Zertifikate zu hinterlegen, gehen Sie folgendermaßen vor:

- Es wird für die DNS-Namen <FQDN> und cert.<FQDN> ein Serverzertifikat im PEM Format benötigt
- Die Zertifikate müssen jeweils inkl. Private Key und CA Zertifikat in eine einzelne Datei im PEM Format zusammengeführt werden:

  ```
  cat servercert.pem > <fqdn>.pem
  cat cacert.pem >> <fqdn>.pem
  cat serverkey.pem >> <fqdn>.pem

  cat servercert_cert.pem > cert.<fqdn>.pem
  cat cacert.pem >> cert.<fqdn>.pem
  cat serverkey_cert.pem >> cert.<fqdn>.pem
  ```

- Die Zertifikate werden dann base64 codiert im entsprechenden Data-Bag abgelegt:

  Auf der Management VM:

  ```
  knife data bag edit encrypted nginx_certificates
  ```

  unter certs das entsprechende Zertifikat suchen

  `"filename": "<fqdn>.pem"` bzw. `"filename": "cert.<fqdn>.pem"`

  und den "content" durch den base64 String tauschen:

  ```
  base64 -w0 <fqdn>.pem
  base64 -w0 cert.<fqdn>.pem
  ```

- Auf der Loadbalancer VM ist ein chef-client Lauf durchzuführen und der nginx Service durchzustarten.

  ```
  chef-client
  service nginx_cloud restart
  ```

13 Einspielen von Hotfixes

Ein Hotfix wird in Form eines Softwarekits im Zip Format bereitgestellt.

Der Kit muss über einen Fabasoft Private Cloud Knoten auf die Management VM unter `/var/www/kit` kopiert werden.

Danach wird die Installation am Management Server mittels Update Skript durchgeführt:

```
/var/www/kit/update.sh <VERSION>
```

Nach dem Einspielen können die Logfiles unter `/var/opt/fabasoft/log/update` geprüft werden, und danach der Kit unter `/var/www/kit` bereinigt werden.

Hinweis: Im Zuge des Updates sind die Services der Fabasoft Private Cloud nicht verfügbar.

14 Durchführen von Updates

Für ein Update der Fabasoft Private Cloud wird ein Updatepacket über einen Download Link zur Verfügung gestellt.

Dieses beinhaltet eine aktualisierte Infrastrukturdefinition, ein Software-Kit, neue Docker Images und eine Updateanleitung.

Im Zuge des Updates werden auch Sicherheitsupdates auf allen VMs und Hypervisoren eingespielt, und diese durchgestartet.

Hinweis: Im Zuge des Updates sind die Services der Fabasoft Private Cloud nicht verfügbar.

15 Backup

15.1 Interne Backups

15.1.1 MMC

Die MMC Daten werden im laufenden Betrieb zusätzlich auf einen Backup Share (`/data/mmcbackup`) auf der Fileserver VM des ersten Fabasoft Private Cloud Knotens gespeichert.

15.1.2 Datenbank

Die PostgreSQL Write-Ahead Logs sowie die Datenbank Backups werden auf Backup Shares (`/mnt/backup1, /mnt/backup2`) auf beiden Fileserver VMs gespeichert.

15.1.3 Chef Server / LDAP Server

Die Backups des Chef und LDAP Servers werden auf Backup Shares (`/mnt/backup1, /mnt/backup2`) auf beiden Fileserver VMs gespeichert.

15.2 Externe Backups

Im Zuge des Backups werden die internen Backups auf den konfigurierten externen Backupshare synchronisiert.

15.2.1 Externen Backupshare konfigurieren

Auf der Fabasoft Private Cloud Management VM muss der Backupshare und ein berechtigter Benutzer konfiguriert werden:

```
knife environment <CUSTOMER> edit
"override_attributes": {
  "fabasoft_pc_backup": {
    "ext_target": "//<backupshare IP>/<share>",
    "ext_sec": "ntlm"
  }
}
knife data bag edit encrypted passwords
```

```
  "raw_data": {
    "backupshare": {
      "user": "<backupuser>",
      "password": "<password>",
      "domain": "<optional domain>"
    }
  }
```

Danach muss die Konfiguration übernommen werden

```
knife ssh name:<CUSTOMER>-mgmt-01 "chef-client"
knife ssh name:<CUSTOMER>-auth-01 "chef-client"
knife ssh name:<CUSTOMER>-mon-01 "chef-client"
knife ssh roles:foliokernel "chef-client"
```

15.3 Erstellen eines Backups

Das tägliche Backup wird automatisiert um 02:00 erstellt.

Ein zusätzliches Backup kann von der Fabasoft Private Cloud Management VM mittels `/opt/fabasoft-ai/sbin/do_backup.sh "demand"`

gestartet werden.

15.4 Fehlerbehandlung

15.4.1 Externer Backupshare nicht erreichbar

Falls zum Zeitpunkt des Backups der externe Backupshare nicht erreichbar sein sollte, wird das Backup beim nächsten Lauf synchronisiert.

Das kann wie folgt geprüft werden:

Am `<CUSTOMER>-mgmt-01: find /mnt/backup{1,2} -name ".pendingBackups" -exec cat {} \; | sort`

Sobald der externe Backupshare wieder vollständig synchronisiert wurde kann der Check in der Fabasoft app.telemetry wie folgt zurückgesetzt werden:

Am `<CUSTOMER>-mgmt-01: echo -n 0 > /var/opt/app.telemetry/status/do_backup_status`

15.4.2 MMC Bereiche inkonsistent

Falls die MMC Bereiche auf den 2 Knoten der Fabasoft Private Cloud asyncron werden, kann nach Lösung des Problems der Check in der Fabasoft app.telemetry wie folgt zurückgesetzt werden:

Am `<CUSTOMER>-db-01: echo -n 0 > /var/opt/app.telemetry/status/syncmmc`

16 Weiterführende Dokumente

Weiterführende Themen finden Sie in folgenden Dokumenten:

- 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.