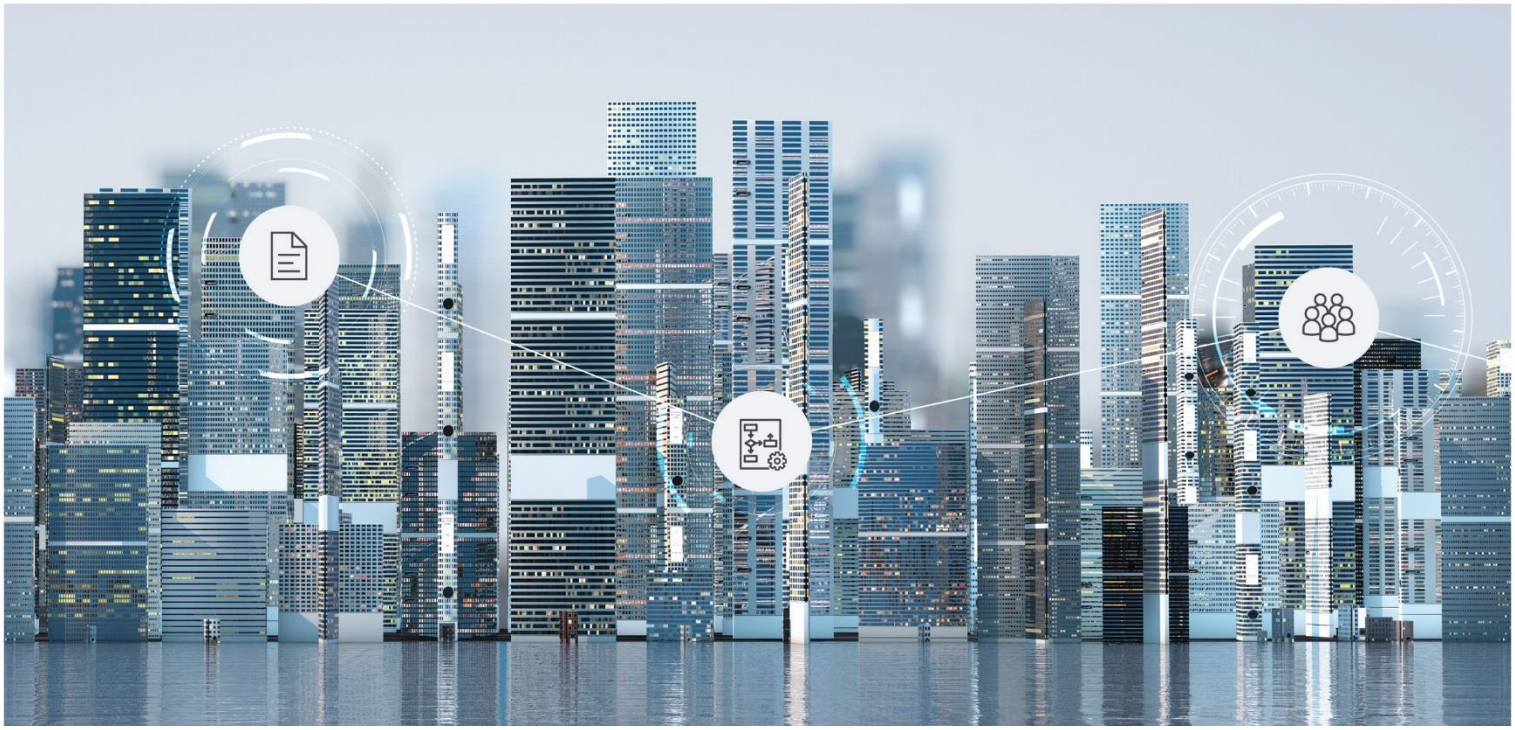
Fabasoft



White Paper

Fabasoft on Linux - Preparation Guide for AlmaLinux

Fabasoft Folio 2024 Update Rollup 1

Contents

1 Introduction

This document describes the installation and preparation of AlmaLinux to run Fabasoft Folio Services as there are:

- Fabasoft Folio Backend Services,
- Fabasoft Folio Web Services,
- Fabasoft Folio Conversion Services, and
- Fabasoft Folio AT Services.

Chapter 2 “Software Requirements” deals with assumed system environment and supported platform as well as software the descriptions in this document are based on.

Chapter 3 “Required Information” lists information needed during the installation process.

Chapter 4 “Installation of AlmaLinux” describes the installation of AlmaLinux.

Chapter 5 “AlmaLinux Tests” describes the tests, which have to be done after the installation of AlmaLinux.

Chapter 6 “Kerberos Authentication” describes the necessary steps to prepare the environment to use Kerberos authentication for Fabasoft Folio Services.

2 Software Requirements

System environments: All information contained in this document implicitly assumes a AlmaLinux environment.

Supported platforms: For detailed information on supported operating systems and software see the software product information on the Fabasoft distribution media.

This document assumes the utilization of a Microsoft Windows Active Directory domain controller as Kerberos Key Distribution Centre (KDC).

General Linux knowledge is necessary to perform and maintain an installation as described in this document.

Descriptions in this document are based on following software:

Third-party products for nodes running

- Fabasoft Folio Backend Services (COO, MMC and gateway services):
  - AlmaLinux 9.3 (x64)
- Fabasoft Folio Web Services
  - AlmaLinux 9.3 (x64)
  - OpenJDK 17 (JRE, headless, included in the supported operating system)
- Fabasoft Folio Conversion Services
  - AlmaLinux 9.3 (x64)
  - OpenJDK 17 (JRE, headless, included in the supported operating system)
  - LibreOffice 6.4.7 (x64)
    http://www.libreoffice.org
- Fabasoft Folio AT Services
  - AlmaLinux 9.3 (x64)

- OpenJDK 17 (JRE, headless, included in the supported operating system)

3 Required Information

The following information is necessary during the installation and/or preparation of AlmaLinux. Prepare this information before beginning the installation.

- Name or IP address of the time server
- IP address of the computer AlmaLinux is installed on
- Host name of the computer AlmaLinux is installed on
- IP address of the gateway server
- IP address(es) of the DNS server(s)
- Domain name
- IP address of the domain controller

4 Installation of AlmaLinux

Make sure that the following packages are installed.

Package	Fabasoft Folio Backend Services	Fabasoft Folio Web Services	Fabasoft Folio Conversion Services	Fabasoft Folio AT Services	Other Fabasoft Folio Services
unzip	x	x	x	x	x
bc	x	x	x	x	x
bzip2	x	x	x	x	x
chkconfig	x	x	x	x	x
dos2unix	x	x	x	x	x
net-tools	x	x	x	x	x
tar	x	x	x	x	x
procps-ng		x	x		
python3-lxml	x	x	x	x	x
yum-utils	x	x	x	x	x
libtool-ltdl	x	x	x	x	x
libtiff	x	x	x	x	x
libjpeg-turbo	x	x	x	x	x

libpng	x	x	x	x	x
httpd		x	x		
mod_ssl		x*			
unixODBC	x	x	x	x	
glibc-locale-source	x	x	x	x	x
Not on the Linux distribution media					
Java Runtime Environment	x	x	x	x	x
LibreOffice (64-bit)			x		
Oracle Instant Client (if Oracle is used as RDBMS)	x				

*(only if SSL enabled)

After the installation process has finished, perform the following steps:

1. To set the hostname execute the following command:
   # `nano /etc/hosts`.
2. Change the line
   `127.0.0.1 <computer name>  localhost.localdomain  localhost`
   into
   `127.0.0.1 localhost.localdomain  localhost`
3. Add a second line:
   `<IP address of the computer>  <computer name>.<domain name>  <computer name>`
   Note: Press "Tab" for the space between the entries in one line.
4. Press `Ctrl` + `X` and confirm with `Y` or `Enter` to save the changes made.
5. Configure or disable the local firewall according to your needs.

5 AlmaLinux Tests

To confirm, that the installation and configuration has been finished successfully, perform following steps:

1. To display the hostname execute the following command:
   `# hostname`
   This command should only display the hostname of the Linux server (e.g.: `fscbackend`).
2. To display the fully qualified domain name, execute the following command:
   `# hostname -f`
   This command should display the hostname and the domain (e.g.: `fscbackend.sub.comp.com`).
3. `localhost` has to be resolved. Execute the following command:
   `# ping localhost`
   Note: Press `Ctrl` + `C` to end the command `ping`.

4. `localhost.localdomain` has to be resolved. Execute the following command:
   ```
   # ping localhost.localdomain
   ```
   Note: Press `Ctrl` + `C` to end the command `ping`.
5. `ping <computer name>` has to work. Execute the following command:
   ```
   # ping fscbackend
   ```
   Note: Press `Ctrl` + `C` to end the command `ping`.
6. `ping <computer name>.<domain name>` has to work. Execute the following command:
   ```
   # ping fscbackend.sub.comp.com
   ```
   Note: Press `Ctrl` + `C` to end the command `ping`.

The AlmaLinux installation has been tested on hostname and domain.

6 Kerberos Authentication

On nodes intended for Fabasoft Folio Web Services, SPNEGO authentication for the Apache Web Server as an extension module is provided. SPNEGO authentication allows single sign on via Kerberos and Active Directory even from a Fabasoft Folio Web Client (similar and compatible to integrated login on the Microsoft platform).

Additionally, configure `/etc/krb5.conf` to use the Active Directory domain as Kerberos realm and its domain controller as Kerberos Key Distribution Centre.

To configure `/etc/krb5.conf`, perform the following steps:

1. Open the `/etc/krb5.conf` file in an editor.
2. Configure `krb5.conf` as follows.
   Replace the values in `<>` with the appropriate values for the domain. In case of troubles consult the Kerberos documentation.
   ```
   [libdefaults]
     default_realm = <SUB.COMP.COM>
     dns_fallback = false
     forwardable = true
     proxiable = true
   [realms]
     <SUB.COMP.COM> = {
       kdc = <IP address of the Domain Controller>[:<port>, [options]]
       admin_server = <IP address of the Domain Controller>[: <port>, [options]]
     }
   [domain_realm]
     <.company.com> = <SUB.COMPANY.COM>
   ```
   Note: Attend to entries written in uppercase (e.g. `<SUB.COMP.COM>`).

The Kerberos authentication has been configured basically on the newly installed server.

6.1 Key Creation for Fabasoft Folio Backend Services

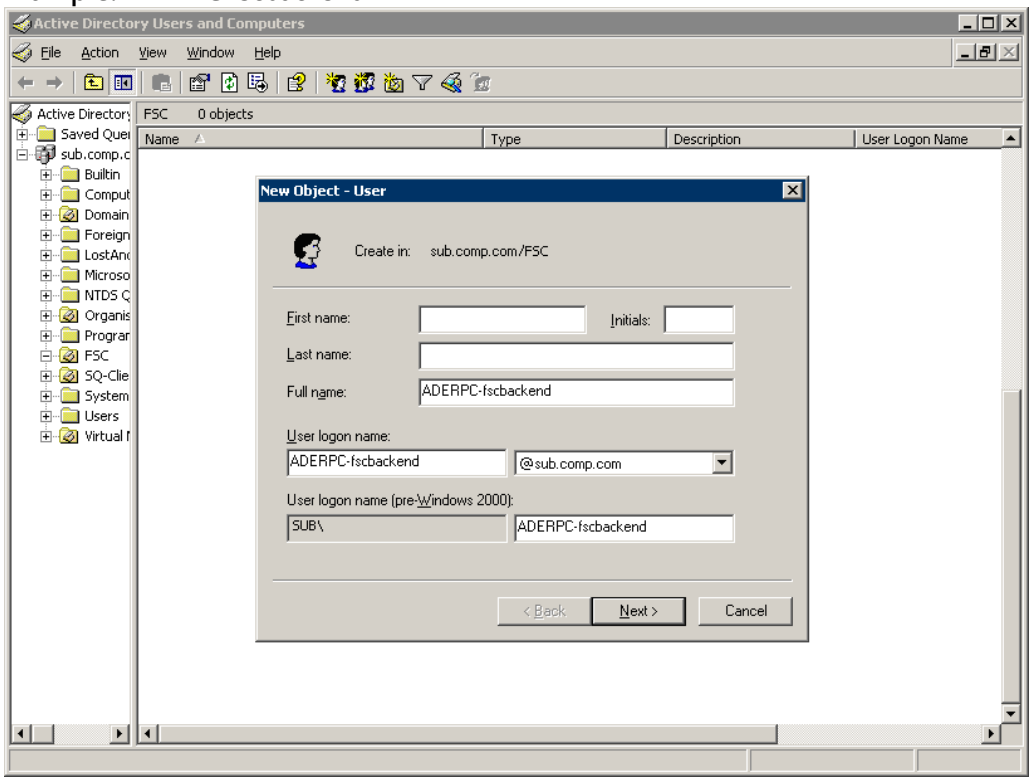
6.1.1 ADERPC Key Creation

For each Linux server running kerberized Fabasoft Folio Services, a distinct ADERPC key has to be exported.

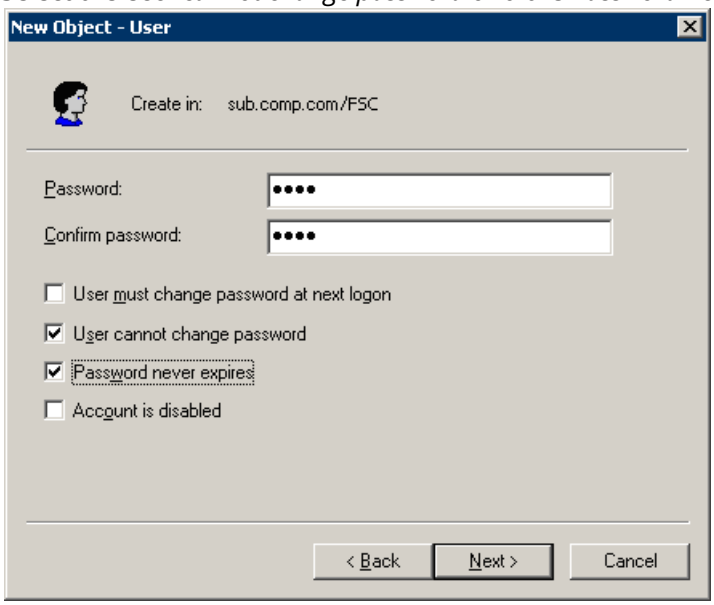
To create an ADERPC key for Fabasoft Folio Backend Services, perform the following steps:

1. Log on to the primary Active Directory domain controller.
2. Open the MMC snap in „Active Directory Users and Computers" (`dsa.msc`).

3. Add a user with an arbitrary logon name of your choice for each Fabasoft Folio Server.
   A common prefix is recommended.
   Example: ADERPC-fscbackend

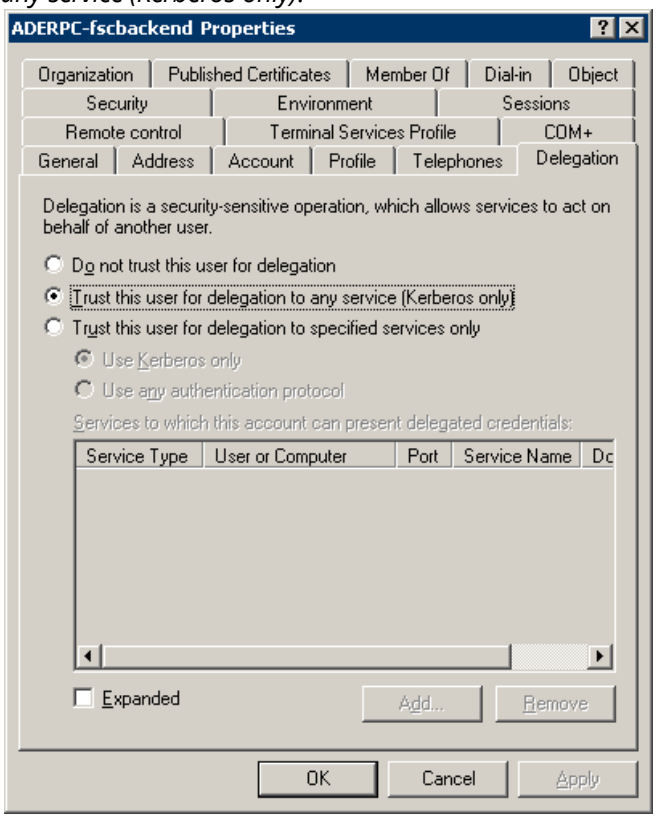


4. Click “Next”.
5. Select the *User cannot change password* and the *Password never expires* check boxes.



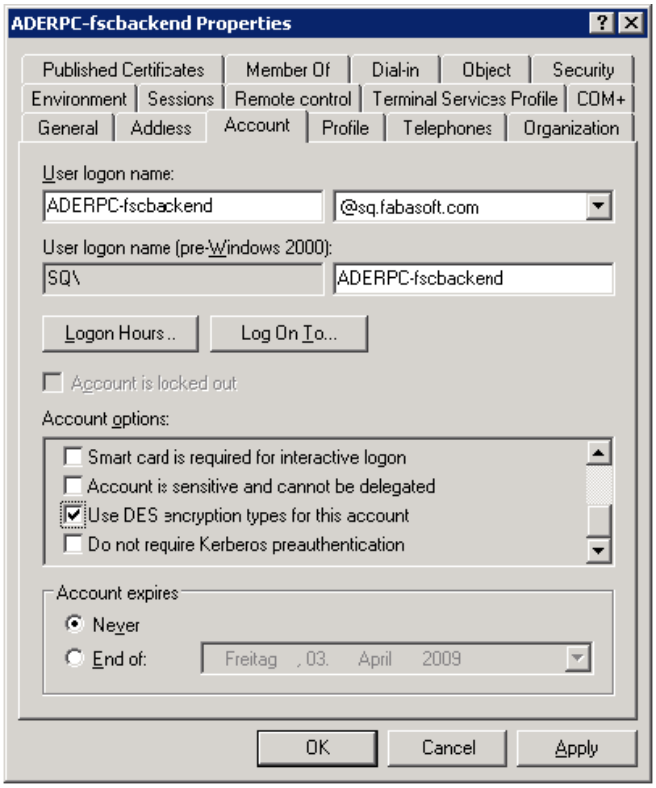
6. To create the user click “Next“.
   A Kerberos user has been created.
7. Execute the following command:
   `setspn -A ADERPC/<fqdn> <user account>`
   Example:
   `setspn -A ADERPC/fscbackend.sub.comp.com ADERPC-fscbackend`

8. On the “Delegation” tab of the user’s properties dialog box click *Trust this user for delegation to any service (Kerberos only)*.

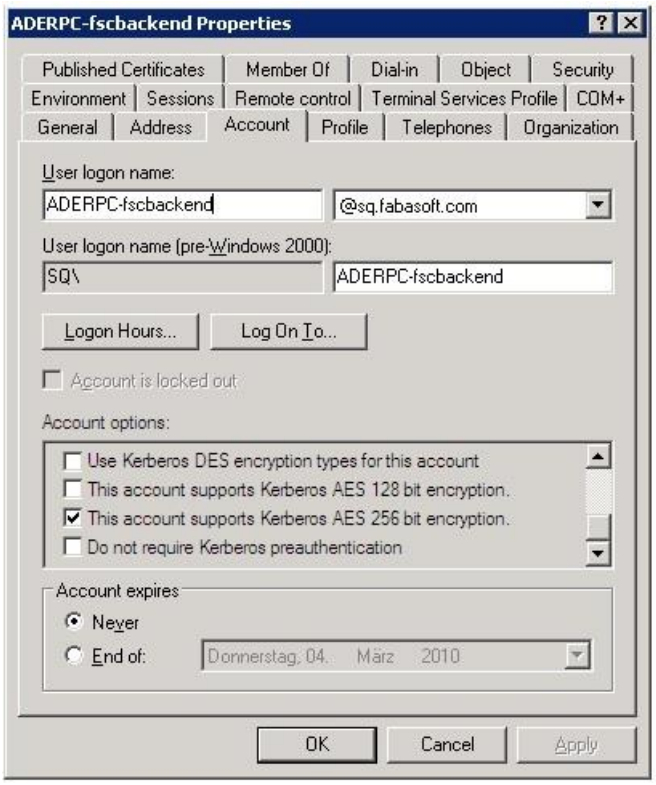


9. On the „Account“ tab of the users’s properties dialog box click *Use DES encryption types for this account* or select *This account supports Kerberos AES 256 bit encryption.*

`DES-CBC-MD5`:



`AES256-SHA1`:



Now a Kerberos key needs to be transferred to the according Linux computer. To export the key from Active Directory, the `ktpass` utility is required.

Execute the following command:

```
ktpass -crypto <crypto-typ> -princ ADERPC/<fqdn>@<REALM> -ptype KRB5_NT_PRINCIPAL
-mapuser <user account> -pass <password of the user account> -out <filename>
```

Possible crypto types:

- `DES-CBC-MD5` (Active Directory 2000/2003)
- `AES256-SHA1` (Active Directory 2008/2008 R2)

Note:

- AES support is limited by some combinations of Microsoft operating systems.
  For details see the Microsoft TechNet article "Kerberos Enhancements".
  http://technet.microsoft.com/en-us/library/cc749438(WS.10).aspx

Example:

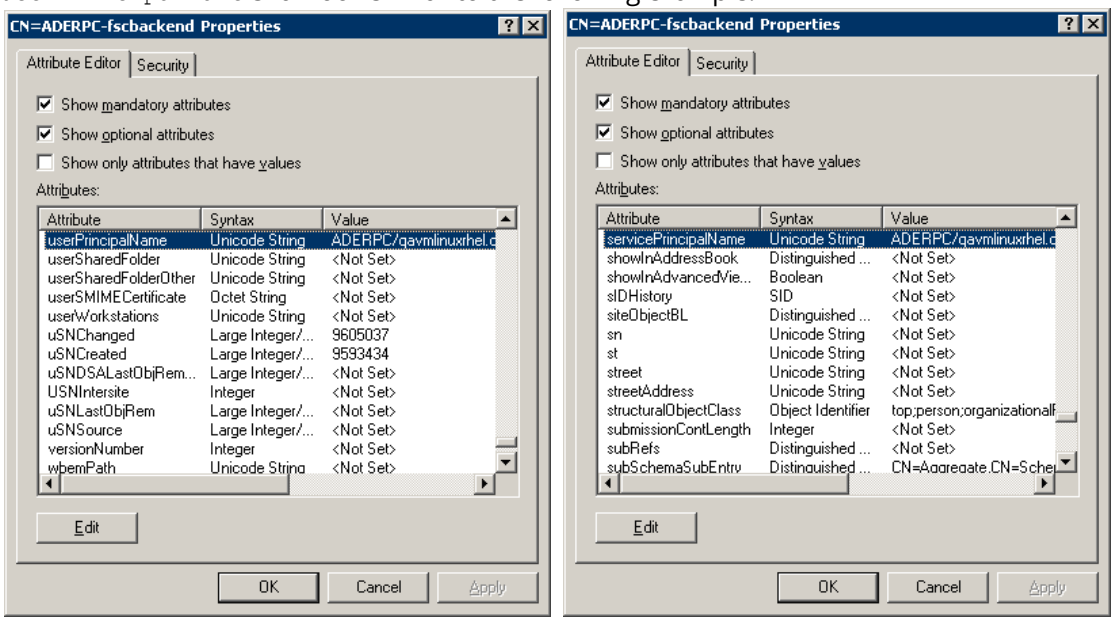
```
ktpass -crypto DES-CBC-MD5 -princ ADERPC/fscbackend.sub.comp.com@SUB.COMP.COM -
ptype KRB5_NT_PRINCIPAL -mapuser ADERPC-fscbackend -pass <your password> -out
fscbackendADERPC.key
```

Via secure channel (e.g. using `ssh`) transfer the key file to the Linux server, where it needs to be imported in the Kerberos key tab as described in chapter 6.2 "Import of Keys on Linux Servers".

Note:

- `<REALM>` is always all-upper-case.
- It is imperative that `<fqdn>` matches the Linux server's hostname in DNS and the entries in Active Directory exactly, `<fqdn>` is also case-sensitive.

- DNS entries for each Linux machine must exist for forward (type A) as well as for reverse (type PTR) lookups.
- The Active Directory user entries can be validated with “ADSI Edit”. Execute `adsiedit.msc` and view the properties of the corresponding user. The attributes `servicePrincipalName` and `userPrincipalName` shall look similar to the following example:



6.1.2 HTTP Key Creation

For each machine intended for Fabasoft Folio Web Services as well as all nodes running Fabasoft Folio Web Management, a HTTP Kerberos key is required.

Perform the steps of chapter 6.1.1 ”ADERPC Key Creation” and replace “ADERPC” with “HTTP”. Name the output file `<hostname>HTTP.key`, which would result in `qavmlinuxrhelHTTP.key` for our example host.

6.2 Import of Keys on Linux Servers

First create a subdirectory `fabasoft` in `/etc`. In the terminal type:

```
mkdir /etc/fabasoft.
```

Run the utility `/usr/kerberos/sbin/ktutil`.

Execute the following commands:

- Read the specified Kerberos key file (created on the Microsoft Windows Server and subsequently transferred to the Linux machine) into the current key list.
  `rkt /path/to/keyfile`
- Write that key into the Kerberos `keytab` file utilized by all Fabasoft Folio Services:
  `wkt /etc/fabasoft/krb5.keytab`
- Do the same for the HTTP key.
  `rkt /path/to/keyfile`
  `wkt /etc/fabasoft/krb5.keytab`
- Type `quit` and press `Enter` to exit `ktutil`.

Note: The ownership and permissions of the file `/etc/fabasoft/krb5.keytab` need to be changed later on (user `fscsrv`, group `fsc`, permissions `0600`). This can be done only after the basic Fabasoft Folio software packages have been installed as these packages will create all required users and groups. Do not create the user (or group) yourself!
See white paper "Installation of Fabasoft Folio Services on Linux".

6.3 Kerberos Tests

If one of the tests fails it is necessary to fix the problem before Fabasoft Folio is installed.

6.3.1 First test

Execute the following command and enter the user's password when prompted:

```
kinit <Microsoft Windows user>
```

If no error message is returned, view the ticket cache with the following command:

```
klist
```

Verify the output (the default principal must correspond to the provided user):

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: <Microsoft Windows user>@<SUB.COMPANY.COM>

Valid starting     Expires            Service principal
11/15/04 09:16:36  11/16/04 19:16:38  krbtgt/<SUB.COMPANY.COM>@<SUB.COMPANY.COM>
```

6.3.2 Second test

Issue the following command to acquire a ticket using the key in the Kerberos key tab file instead of an interactive password:

```
kinit -k -t /etc/fabasoft/krb5.keytab <principalname>
```

Example:

```
kinit -k -t /etc/fabasoft/krb5.keytab \
   ADERPC/<hostname>.<sub.company.com>@<SUB.COMPANY.COM>
```

Note: '\' denotes line continuation.

If no error message is returned, view the ticket cache with the following command:

```
klist
```

Verify the output (the default principal must correspond to the provided user):

```
[root@fscbackend ~]# /usr/kerberos/bin/klist
Ticket cache: FILE: /tmp/krb5cc_0
Default principal: ADERPC/fscbackend.qa.fabasoft.com@QA.FABASOFT.COM

Valid Starting     Expires              Service principal
01/29/09 09:45:34  01/30/09 19:43:57    krbtgt/QA.FABASOFT.COM@QA.FABASOFT.COM
        renew until 01/30/09 09:45:34


Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
[root@fscbackend ~]#
```

Along the same lines, try the HTTP key.

```
kinit -k -t /etc/fabasoft/krb5.keytab \
   HTTP/<hostname>.<sub.company.com>@<SUB.COMPANY.COM>
```

Note: '\' denotes line continuation.

If no error message is returned, view the ticket cache with the following command:

```
klist
```

```
[root@fscbackend ~]# /usr/kerberos/bin/klist
Ticket cache: FILE: /tmp/krb5cc_0
Default principal: HTTP/fscbackend.qa.fabasoft.com@QA.FABASOFT.COM

Valid Starting     Expires              Service principal
01/29/09 09:58:23  01/30/09 19:58:23    krbtgt/QA.FABASOFT.COM@QA.FABASOFT.COM
        renew until 01/30/09 09:58:23


Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
[root@fscbackend ~]#
```

On any errors, please consult the extensive Kerberos documentation.

If no errors occur the installation and configuration of Kerberos has been successful.