

Verschlüsselte Backups mit Bareos

Zusammenfassung

Beschreibung für die Einstellung eines Verschlüsselten Backups mit Bareos.

⚠️ Wenn dies nicht korrekt eingestellt wird, kann unter Umständen auch kein Restore mehr gemacht werden.

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Mitarbeitende**

Transport-Verschlüsselung

Bei einem aktuellen Client (ab Version 19) ist die Transportverschlüsselung der Backups automatisch aktiviert. Damit wird die komplette Kommunikation zwischen Client und Server verschlüsselt.

Daten-Verschlüsselung

Wenn die gesicherten Daten verschlüsselt werden müssen, ist besondere Vorsicht geboten, damit diese auch wieder gelesen werden können. Sinnvoll ist eine Datenverschlüsselung nur, wenn diese auf dem Client passiert und somit weiß der Server nur noch die Metadaten (Dateinamen, Größe, ...). Eine Wiederherstellung ist dann nur auf Clients möglich, an denen der entsprechend passende Private Schlüssel eingebunden ist. Somit muss der öffentliche und private Schlüssel gesondert gesichert werden.

<https://docs.bareos.org/TasksAndConcepts/DataEncryption.html#dataencryption>

Client Konfiguration

Damit die Daten vom Client verschlüsselt werden, muss dort ein Zertifikat existieren. Da es bei der DFN-CA nur noch Zertifikate mit 1 Jahr Laufzeit gibt, was sich für Verschlüsselung für Backups nicht so gut eignet wird nun doch die Verwendung von selbstsignierten Zertifikaten empfohlen. Es müssen dann der öffentliche (public) und der geheime (private) Schlüssel (Key) in einer Datei gespeichert werden, wobei nur root-Leserechte benötigt:

```
openssl genrsa -out fd-example.priv.key 2048
openssl req -new -key fd-example.priv.key -x509 -out fd-example.pub.key -days 1826
# DE, Thuringen, Jena, Friedrich-Schiller-Universitaet Jena, URZ, example.rz.uni-jena.de
cat fd-example.priv.key fd-example.pub.key >/etc/bareos/fd-example.pem

cd /etc/bareos/
chmod 400 example-fd.pem
ls -l example-fd.pem
# -r----- 1 root root 3814 May 20 2016 example-fd.pem

curl https://repo.rz.uni-jena.de/backupmaster.pem >backupmaster.pem
```

Wenn nur der public-Key gespeichert wird geht der Restore logischerweise nicht. Wir sorgen dafür, dass der (private) Backup-Master-Key entsprechend geschützt ist, der public-Key des Backup-Masters liegt hier: <https://repo.rz.uni-jena.de/backupmaster.pem>
/etc/bareos/bareos-fd.d/client/myself.conf

```
Client {
...
  ## encryption configuration
  PKI Signatures = Yes                # Enable Data Signing
  PKI Encryption = Yes                # Enable Data Encryption
  PKI Keypair = "/etc/bareos/fd-myclient.pem" # Public and Private Keys
  PKI Master Key = "/etc/bareos/backupmaster.pem" # ONLY the Public Key
  PKI Cipher = aes256                 # specify desired PKI Cipher
here
}
```

⚠️ **Achtung!** Wer seine Daten verschlüsselt, dem kann bei Schlüsselverlust nur geholfen werden, wenn der Master-Key **Backupmaster-Key** mit eingetragen wird. ⚠️

Backupmaster Zertifikat

Da die Zertifikate vom DFN nur noch 1 Jahr gültig sind, wird nun ein unabhängiges mit langer Laufzeit für den Backup-Master erzeugt.
Eigenschaften des Backupmaster Keys

```
openssl x509 -in backupmaster-2021.pem -text

Certificate:
...
    Serial Number:
        3d:d0:61:b4:91:6b:6b:2e:5f:ff:a7:f1:83:f3:da:64:64:b4:44:aa
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = DE, ST = Thuringen, L = Jena, O = Friedrich-Schiller-Universitaet Jena, OU = URZ, CN = back
upmaster.rz.uni-jena.de, emailAddress = thomas.otto@uni-jena.de
    Validity
        Not Before: Apr  7 13:08:47 2021 GMT
        Not After : Apr  5 13:08:47 2031 GMT
    Subject: C = DE, ST = Thuringen, L = Jena, O = Friedrich-Schiller-Universitaet Jena, OU = URZ, CN = bac
kupmaster.rz.uni-jena.de, emailAddress = thomas.otto@uni-jena.de
...
```

backupmaster-2021.pem

```
-----BEGIN CERTIFICATE-----
MIIEWzCCA0OgAwIBAgIUPdhtJFray5f/6fxg/PaZGS0RKowDQYJKoZIhvcNAQEL
BQAwgbwxCzAJBgNVBAYTAkRFMRMwEQYDVQQIDApUaHVlcmluZ2VuMQ0wCwYDVQQH
DARKZ5hMS0wKwYDVQQKDCRGCml1ZHZpY2gtU2NoaWxsZXItVW5pdmVyc2l0YWV0
IEplbmExDDAKBgNVBAsMA1VSWjEkMCIGA1UEAwwbYmFja3VwbWZzdGVyLnJ6LnVu
aSlqZW5hLmRlMSYwJAYJKoZIhvcNAQkBFhd0aG9tYXMuY291b3R0b0B1bmktaWVuYS5k
ZTAeFw0yMTA0MDcxMzA4NDdaFw0zMTA0MDUxMzA4NDdaMIG8MQswCQYDVQQGEwJE
RTETMBEGA1UECAwKVGH1ZXJpbmdlbjJENMAsGA1UEBwwESmVuYXV0eTEtMCsGA1UECgwk
RnJpZWRYaWNoLVNjaGlsbGVyLWVuaXZ1cnNpdGFldCBKZW5hMQwwCgYDVQQQLDANV
UloxJDAiBgNVBAMMG2JhY2t1cG1hc3R1ci5yei51bmktaWVuYS5kZTEtMCQGCsG
S1b3DQEQJARYXGhvbWZzLm90dG9AdW5pLWplbmEuZGUwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC787UEC0dQJIVjCJVR2CqDqVIR0WmI0LPvAS+2g+1n
LYhiwZ89CzVV2JaD5w+V0cElonitpQ3arqJW4X1wrrLrKNEXcy8WyrTgsLh3z2nx
UVnmu6jNFv7rq7VF6uALbAx+Sp+2WCH1SauLlcIMr/ZD+yv1Hrg80wanMAkBXAbY
3JDpW2tFk5s6a9XE7zyawrpNooUZ238rPAyP9rD7FMxuxZGzrC2W4XQOFQEj5cPo
UsInWJGiOCStUzTCPwTCfRSnveF2QBWgQeo7Ypm8pXtY6IoUwFfsFSw33/Q7EOBR
kjITs11DfGgCpc8RIJg9zVLSn08Q09i9asJbvgSciedRagMBAAGjUzBRMB0GA1Ud
DgQWBBS7EXMuWa/e1V+bMv9Y3/yi804/aTafBgNVHSMEGDAWgBS7EXMuWa/e1V+b
Mv9Y3/yi804/aTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQCx
VbUqqmRDRJ3vzpNW64aUpRgyNF1M5cIwBh6VhJ1tcY1FWrR19FQSCw1JP67v5NDk
OBW01pi3Vyg927cs7QTm3bNoeDSYTx0iqN2V8PjzWPen6/ZHondcpSsLmMRqv50E
eGdlUwuYZEzP2hzkzG3+IdJU6gp9RU+8g0yWFC0c3TDgOzB8BSZtaboQACbKUBuU
pJ39FYjGwbotzfkZzUBTi/bWQ10FuJDD3zR8VbZSqrftXLDg+XvwwvP2pZ919XG8
nz2hGhNbHtjQvRDdw6e/DX4nno+MgE6TskhG110pmlbNoc0x57StDe7g6V3WWkyF
DxzmIp1JKTL/xBN7Ty8s
-----END CERTIFICATE-----
```

Titel: "Verschlüsselte Backups mit Bareos"

Stand: 23.11.2021

