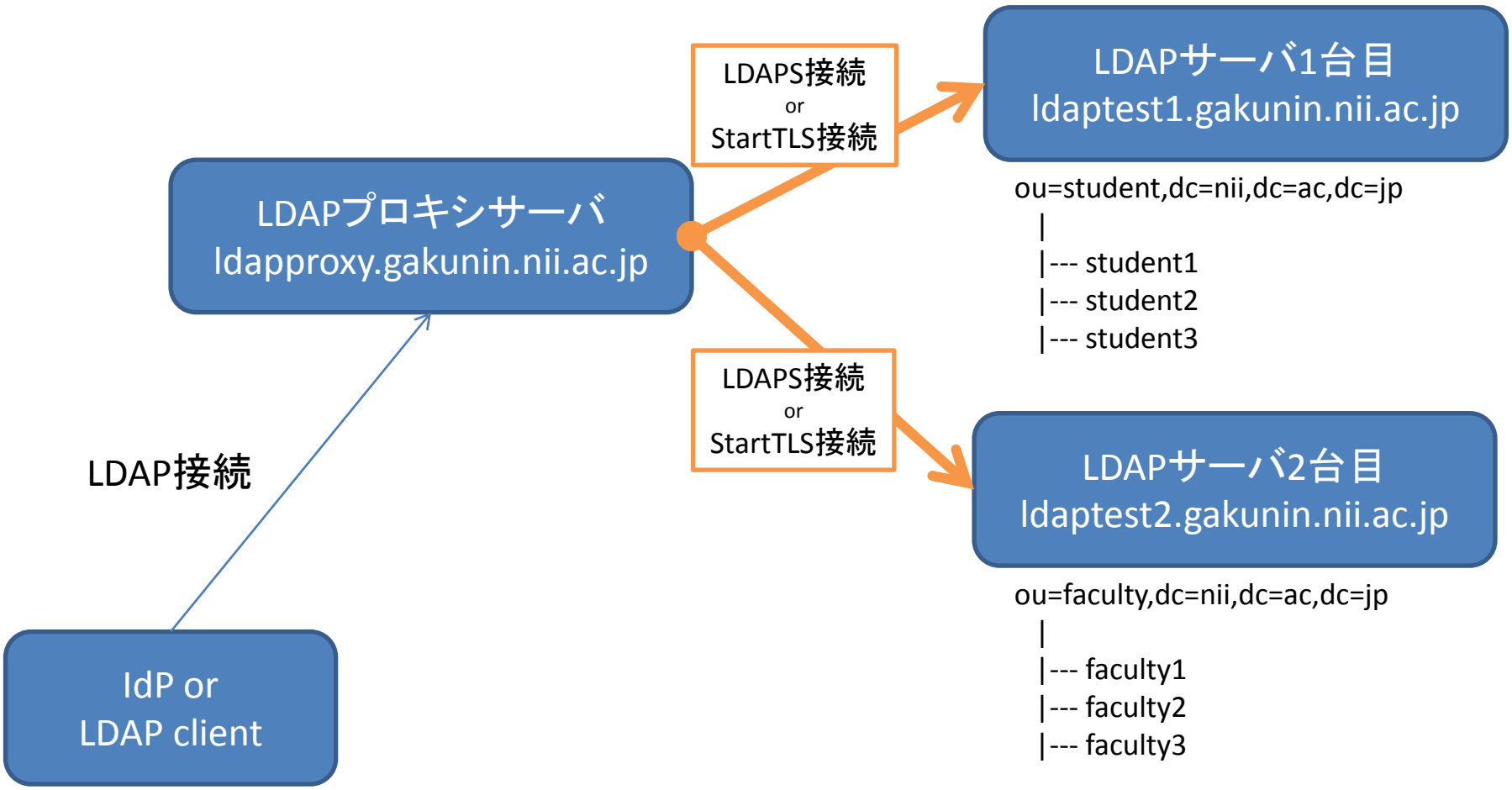
LDAPサーバ2台 + LDAPプロキシ間のLDAPS接続調査

目次

全体構成



ou=student,dc=nii,dc=ac,dc=jp
|
|--- student1
|--- student2
|--- student3

ou=faculty,dc=nii,dc=ac,dc=jp
|
|--- faculty1
|--- faculty2
|--- faculty3

各サーバの構成
OS　　：CentOS 5.7
LDAPサーバ：CentOS標準のOpenLDAPパッケージを使用
(openldap-servers-2.3.43-12.el5_7.10)

LDAPサーバ設定(ldaptest1)

- /etc/openldap/slapd.confの設定

  ### LDAPS用証明書の設定
  TLSCACertificateFile /etc/pki/tls/certs/gakuninca.pem
  TLSCertificateFile /etc/pki/tls/certs/ldaptest1.gakunin.nii.ac.jp.pem
  TLSCertificateKeyFile /etc/pki/tls/private/ldaptest1.gakunin.nii.ac.jp.key
  ### LDAPデータベース設定
  database bdb
  suffix “dc=nii,dc=ac,dc=jp”

SSLサーバ証明書	/etc/pki/tls/certs/ldaptest1.gakunin.nii.ac.jp.pem •issuer=/C=JP/O=NII/OU=GakuNin •subject=/C=JP/O=NII/OU=GakuNin/CN=ldaptest1.gakunin.nii.ac.jp
秘密鍵	/etc/pki/tls/private/ldaptest1.gakunin.nii.ac.jp.key
CA証明書	/etc/pki/tls/certs/gakuninca.pem

LDAPサーバ設定(ldaptest2)

- /etc/openldap/slapd.confの設定

  ### LDAPS用証明書の設定
  TLSCACertificateFile /etc/pki/tls/certs/gakuninca.pem
  TLSCertificateFile /etc/pki/tls/certs/ldaptest2.gakunin.nii.ac.jp.pem
  TLSCertificateKeyFile /etc/pki/tls/private/ldaptest2.gakunin.nii.ac.jp.key
  ### LDAPデータベース設定
  database bdb
  suffix “dc=nii,dc=ac,dc=jp”

SSLサーバ証明書	/etc/pki/tls/certs/ldaptest2.gakunin.nii.ac.jp.pem •issuer=/C=JP/O=NII/OU=GakuNin •subject=/C=JP/O=NII/OU=GakuNin/CN=ldaptest2.gakunin.nii.ac.jp
秘密鍵	/etc/pki/tls/private/ldaptest2.gakunin.nii.ac.jp.key
CA証明書	/etc/pki/tls/certs/gakuninca.pem

LDAPプロキシサーバ設定(LDAPS接続の場合)(ldapproxy)

- /etc/openldap/slapd.confの設定

```
### 証明書検証の設定
TLSVerifyClient demand
TLSCACertificateFile /etc/openldap/cacerts/gakuninca.pem

### LDAPプロキシの設定
database meta
suffix “dc=nii,dc=ac,dc=jp”
uri “ldaps://ldaptest1.gakunin.nii.ac.jp/ou=student,dc=nii,dc=ac,dc=jp”
uri “ldaps://ldaptest2.gakunin.nii.ac.jp/ou=faculty,dc=nii,dc=ac,dc=jp”
```

CA証明書	/etc/pki/tls/certs/gakuninca.pem

LDAPプロキシサーバ設定(StartTLS接続の場合)(ldapproxy)

- /etc/openldap/slapd.confの設定

```
### 証明書検証の設定
TLSVerifyClient demand
TLS_CACERT /etc/openldap/cacerts/gakuninca.pem

### LDAPプロキシの設定
database meta
suffix “dc=nii,dc=ac,dc=jp”
tls start
uri “ldap://ldaptest1.gakunin.nii.ac.jp/ou=student,dc=nii,dc=ac,dc=jp”
uri “ldap://ldaptest2.gakunin.nii.ac.jp/ou=faculty,dc=nii,dc=ac,dc=jp”
```

CA証明書	/etc/pki/tls/certs/gakuninca.pem

注意 : metaバックエンドとStartTLSの組み合わせでは、接続時の証明書検証で問題があることがわかっています。詳細は LDAPプロキシサーバの証明書検証について をご覧ください。

LDAPプロキシサーバの証明書検証について

- ldapproxyからldaptest{1,2}への接続方法により、証明書検証の挙動が変わります
  - LDAPS接続の場合
    - LDAPプロキシサーバslapd.conf内のTLSCACertificateFileで指定したCA証明書を用いて、LDAPサーバのサーバ証明書がそのCAから発行されたものか検証が行なわれます。正しく検証が行なえない場合はそのサーバとのコネクションが遮断されます。
    - uriで指定したサーバ名と、接続先のLDAPサーバから提供されるサーバ証明書のCommonName(CN)の検証が行なわれます。サーバ名とCNと違う場合にはコネクションが遮断されます。
  - StartTLS接続の場合
    - LDAPプロキシサーバslapd.conf内のTLSCACertificateFileで指定したCA証明書を用いて、LDAPサーバのサーバ証明書がそのCAから発行されたものか検証が行なわれます。正しく検証が行なえない場合はそのサーバとのコネクションが遮断されます。
    - uriで指定したサーバ名と、接続先のLDAPサーバから提供されるサーバ証明書のCommonName(CN)の検証が行なわれます。サーバ名とCNと違う場合でもコネクションは遮断されません。

LDAPプロキシサーバからLDAPサーバへの接続試験 (LDAPS接続)

- ldapproxy ---(LDAPS接続)---> ldaptest1

```
$ LDAPTLS_CACERT=/etc/openldap/cacerts/gakuninca.pem ldapsearch -x -H
    "ldaps://ldaptest1.gakunin.nii.ac.jp" -b "dc=nii,dc=ac,dc=jp" '(uid=*)' dn
    # student1, student, nii.ac.jp
    dn: uid=student1,ou=student,dc=nii,dc=ac,dc=jp

    # student2, student, nii.ac.jp
    dn: uid=student2,ou=student,dc=nii,dc=ac,dc=jp

    # student3, student, nii.ac.jp
    dn: uid=student3,ou=student,dc=nii,dc=ac,dc=jp
```

- ldapproxy ---(LDAPS接続)--> ldaptest2

```
$ LDAPTLS_CACERT=/etc/openldap/cacerts/gakuninca.pem ldapsearch -x -H
    "ldaps://ldaptest2.gakunin.nii.ac.jp" -b "dc=nii,dc=ac,dc=jp" '(uid=*)' dn
    # faculty1, faculty, nii.ac.jp
    dn: uid=faculty1,ou=faculty,dc=nii,dc=ac,dc=jp

    # faculty2, faculty, nii.ac.jp
    dn: uid=faculty2,ou=faculty,dc=nii,dc=ac,dc=jp

    # faculty3, faculty, nii.ac.jp
    dn: uid=faculty3,ou=faculty,dc=nii,dc=ac,dc=jp
```

LDAPTLS_CACERTで設定しているCA証明書は、/etc/openldap/ldap.conf内のTLS_CACERTとして定義することも可能です。

LDAPプロキシサーバからLDAPサーバへの接続試験 (StartTLS接続)

- ldapproxy ---(StartTLS接続)---> ldaptest1

```
$ LDAPTLS_CACERT=/etc/openldap/cacerts/gakuninca.pem ldapsearch -x -ZZ –H
    "ldap://ldaptest1.gakunin.nii.ac.jp" -b "dc=nii,dc=ac,dc=jp" '(uid=*)' dn
        # student1, student, nii.ac.jp
        dn: uid=student1,ou=student,dc=nii,dc=ac,dc=jp

        # student2, student, nii.ac.jp
        dn: uid=student2,ou=student,dc=nii,dc=ac,dc=jp

        # student3, student, nii.ac.jp
        dn: uid=student3,ou=student,dc=nii,dc=ac,dc=jp
```

- ldapproxy ---(StartTLS接続)--> ldaptest2

```
$ LDAPTLS_CACERT=/etc/openldap/cacerts/gakuninca.pem ldapsearch -x -ZZ -H
    "ldap://ldaptest2.gakunin.nii.ac.jp" -b "dc=nii,dc=ac,dc=jp" '(uid=*)' dn
        # faculty1, faculty, nii.ac.jp
        dn: uid=faculty1,ou=faculty,dc=nii,dc=ac,dc=jp

        # faculty2, faculty, nii.ac.jp
        dn: uid=faculty2,ou=faculty,dc=nii,dc=ac,dc=jp

        # faculty3, faculty, nii.ac.jp
        dn: uid=faculty3,ou=faculty,dc=nii,dc=ac,dc=jp
```

LDAPTLS_CACERTで設定しているCA証明書は、/etc/openldap/ldap.conf内のTLS_CACERTとして定義することも可能です。

LDAPクライアントからLDAPSプロキシサーバへの接続試験

- LDAP client ---(LDAP接続)---> ldapproxy

```
$ ldapsearch -x -H "ldap://ldapproxy.gakunin.nii.ac.jp" -b "dc=nii,dc=ac,dc=jp" '(uid=*)' dn
```

```
# student1, student, nii.ac.jp
dn: uid=student1,ou=student,dc=nii,dc=ac,dc=jp

# faculty1, faculty, nii.ac.jp
dn: uid=faculty1,ou=faculty,dc=nii,dc=ac,dc=jp

# student2, student, nii.ac.jp
dn: uid=student2,ou=student,dc=nii,dc=ac,dc=jp

# faculty2, faculty, nii.ac.jp
dn: uid=faculty2,ou=faculty,dc=nii,dc=ac,dc=jp

# student3, student, nii.ac.jp
dn: uid=student3,ou=student,dc=nii,dc=ac,dc=jp

# faculty3, faculty, nii.ac.jp
dn: uid=faculty3,ou=faculty,dc=nii,dc=ac,dc=jp
```