Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Informatikdienste

nethz Web Service

Gruppenverwaltung

Benutzerhandbuch

Dateiname:	nethz Web Service - Groupmgr.docx
Version und Datum:	0.3 – 28.11.2014
Dokumentstatus:	
Autor(en):	Lange Gunter (ID SWS)
Departement/Direktion:	ID Software Services

Änderungsnachweis

Version	Datum	Autor	Bemerkung / Änderung(en)
0.1	31.10.2014	Gunter Lange (ID SWS)	Erste Version
0.2	14.11.2014	Gunter Lange (ID SWS)	aktualisiert
0.3	28.11.2014	Gunter Lange (ID SWS)	Korrekturen aus Rückmeldungen

Inhaltsverzeichnis

1 Einleitung

Der *nethz Web Service* ermöglicht es, die Funtionalität der Gruppenverwaltung, die die Web Applikation *nethz Admin-Tool* zur Verfügung stellt, für den Gruppentyp 'Custom' remote über HTTPS auszuführen.

```
Die wesentlichen Funktionen sind
 - C reate : eine Gruppe neu erstellen, Provisioning der ausgeführten Mutationen in
             die ausgewählten Zielsysteme AD, LDAPS oder CQ5
 - R read  : Gruppeninformationen lesen
 - U pdate : Personen zu einer bestehenden Gruppe hinzufügen, Gruppenbeschreibung
             ändern oder ein Provisioning Zielsystem setzen
 - D elete : eine Gruppe, ein Gruppenmitglied oder das Provisioning Zielsystem löschen
```

1.1 Hinweis zur IAM Migration

Das aktuell produktive Identity and Access Management System (IAM) der ETHZ wird in der nächsten Zeit durch ein neues System abgelöst. Das Projekt ist bereits gestartet und die Migration des bestehenden Systems in das neue Zielsystem wird anfangs nächsten Jahres beginnen.

Nach aktuellem Kenntnisstand wird das neue IAM auf der DirX Suite Technologie der Firma Atos basieren. DirX ist eine Java Struts Technologie. Web Services sind als SOA Services zu realisieren.

Was bedeutet dies für die Spezifikation der Web Services? Die Spezifikation der Web Services gilt für das aktuelle IAM. Mit der Systemumstellung kann nicht ausgeschlossen werden, dass Änderungen in der Schnittstelle des Web Service vorgenommen werden müssen.

1.2 Allgemeines Verhalten des Web Service

Der Web Service zum Lesen der nethz Custom Gruppeninformationen erfolgt in einem einzigen Aufruf.

Modifizierende Aktionen (Create, Update, Delete) erfolgen stets zweistufig:

- zuerst werden die Mutation(en) einer Gruppe ausgeführt (bei erfolgreicher Ausführung sind die Änderungen in der nethz DB persistiert).
- anschliessend erfolgt das Provisoning der Zielsysteme (AD, LDAPS oder CQ5).

Der Request und Response Datentransport erfolgt im Json Format. Weitere Datenformate sind nicht vorgesehen. Ausgenommen sind die Daten, die als Query parameters übermittelt werden.

1.3 HTTP basic auth over HTTPS

Für die Web Services mit mutierenden Charakter (Create, Update, Delete) ist eine Authentisierung zwingend. Mit den im Request Header gesendeten credentials wird geprüft, ob die Durchführung der Aktion zulässig ist. Die credentials werden Base64 encoded übermittelt.

2 Web Service API

2.1 nethz Web Service URL

Eine kurze (saloppe) Definition von

- URI identifiziert die Resource
- URL fügt dieei Information hinzu, wie die Resource zu erreichen ist

Der Web Service URL der nethz Gruppenverwaltung lautet:

https://idn.ethz.ch/cgi-bin/Groupmgr/public/nethz

2.2 Übersicht

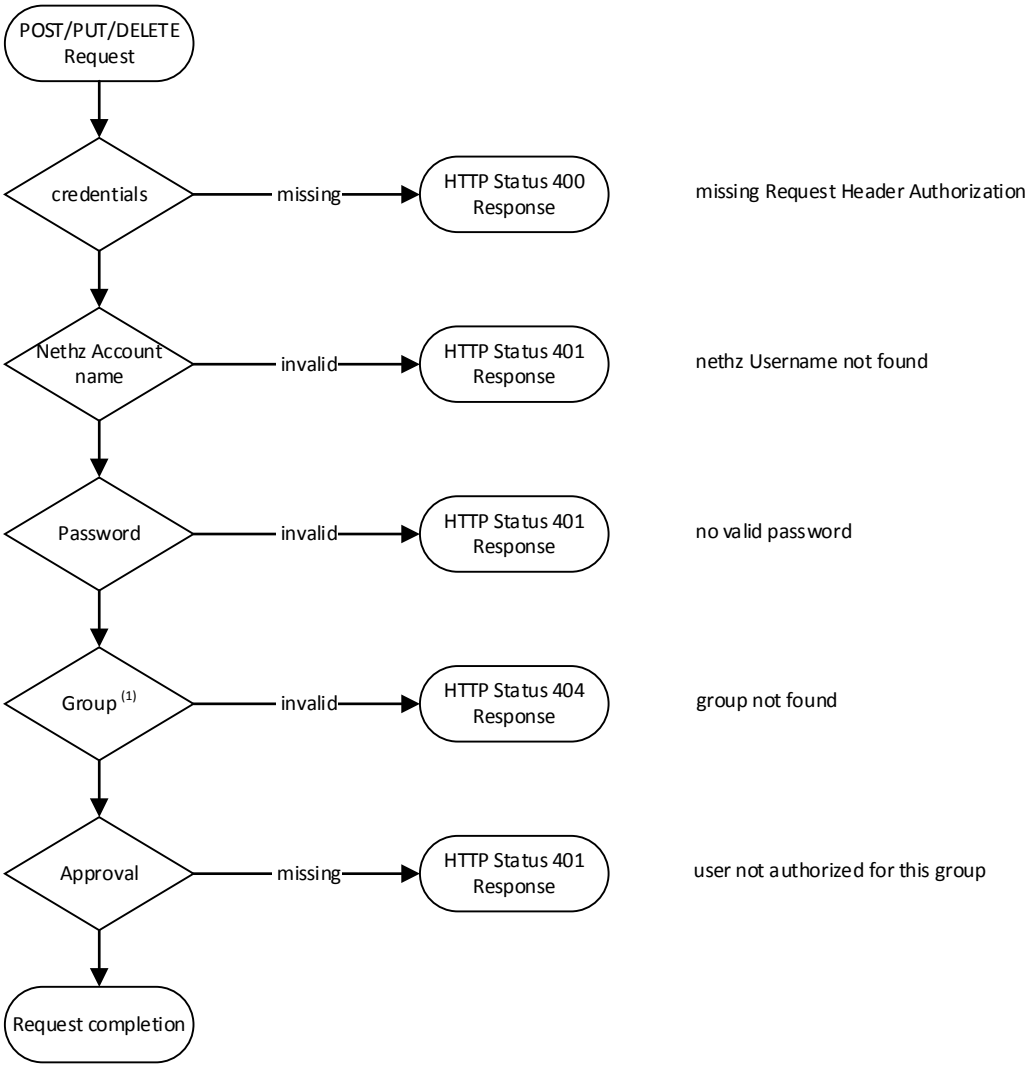
HTTP verb	Auth	URI	Body	Beschreibung
GET		/group/:name		Gruppeninformation
GET		/groups		Namensliste aller vorhandenen Gruppen
GET		/groups?name=<group>&name=<group>		Gruppeninformation(en)
POST	X	/group	X	neue Gruppe erstellen
POST	X	/group/provisioning	X	Provisioning(en) ausführen
PUT	X	/group/users	X	Gruppenmitglied(er) hinzufügen
PUT	X	/group/description	X	Beschreibung aktualisieren
PUT	X	/group/provisioning	X	Provisioning Ziele setzen/aktualisieren
DELETE	X	/group/:name		Gruppe löschen
DELETE	X	/group/:name/user/:name		Gruppenmitglied löschen
DELETE	X	/group/:name/ provisioning/:name		Provisioning Ziel löschen

Zur Parameter Übergabe

- wenn der Request ein GET oder DELETE ist, werden zusätzlich Parameter in den *Query params* der URI erwartet
- wenn der Request ein POST oder PUT ist, werden zusätzliche Parameter in den *body params* erwartet

2.3 Authentifikation - Autorisierung

Das folgende Flussdiagramm zeigt den Authentifikation und Autorisierung Ablauf bei Web Service Aufrufen mit modifizierenden Charakter (POST/PUT/DELETE).



(1) diese Prüfung erfolgt nur bei bereits existierenden Gruppen, nicht aber beim Erzeugen einer neuen Gruppe

2.4 GET

2.4.1 Gruppeninformation einer bestimmten nethz Custom Gruppe

```
Synopsis: Informationen einer nethz Custom Gruppe lesen

          Joker/wildcards sind nicht zulässig

HTTP method   : GET
URI  Resource : group/:name
Content-Type  : application/x-www-form-urlencoded

Returns (HTTP Status Code):
- 200 OK          : die Gruppe wurde gefunden und die Informationen wurden ausgelesen
- 400 Bad request : Aufrufparameter nicht korrekt
- 404 Not Found   : die Gruppe konnte nicht gefunden werden
```

- Beispiel

```
Request    <url>/group/06065

Response   {
              "group" : {
                 "subgroups" : [],
                 "members" : [
                    "farnungc",
                    "fcroci",
                    "glange",
                    "kdavor",
                    "meierret",
                    "mruepp",
                    "spamin",
                    "vermeul"
                 ],
                 "name" : "06065",
                 "export" : [
                    "AD",
                    "LDAPS",
                    "CQ5"
                 ],
                 "description" : "ID Identity / Access Management & eServ"
              }
           }
```

2.4.2 Gruppeninformation zu einer Liste von nethz Custom Gruppen

- ohne weitere Angabe von Gruppen

```
Synopsis: Namensliste aller nethz Custom Gruppen lesen



HTTP method   : GET
URI  Resource : groups
Content-Type  : application/x-www-form-urlencoded

Returns (HTTP Status Code):
- 200 OK          : die Liste der Namen wurde ausgelesen
- 400 Bad request : Aufrufparameter nicht korrekt
```

➢ Beispiel

```
Request    <url>/groups
Response   {
              "groups" : [
                 "AGRL-ISG-GUESTS",
                 "AGRL-ISG-WIKI",
                 "AGRL-test-test",
                 "BAUG-IFU-SWW-MM",
                 "BAUG-IT-alle",
                 ...
                 "service-inf-drz",
                 "spinoff-gimalon",
                 "uplinknetz",
                 "usys",
                 "zo-sec"
              ]
           }
```

- mit Angabe von Gruppennamen

```
Synopsis: Informationen der spezifizierten nethz Custom Gruppen lesen

          wildcards (Jokerzeichen ist '*') sind zulässig

HTTP method   : GET
URI  Resource : groups?name=<gruppe>&name=<gruppe>&name= ...
Content-Type  : application/x-www-form-urlencoded

Returns (HTTP Status Code):
- 200 OK          : die Liste der Namen wurde ausgelesen
- 400 Bad request : Aufrufparameter nicht korrekt
```

➢ Beispiel

```
Request    <url>/groups?name=06065&name=itet-staff*
```

Response


```
{
   "groups" : [
      {
         "subgroups" : [],
         "members" : [
            "fcroci",
             ...
            "vermeul"
         ],
         "name" : "06065",
         "export" : [
            "AD",
            "LDAPS"
         ],
         "description" : "ID Identity / Access Management & eServ"
      },
      {
         "subgroups" : [],
         "member" : [
            "bonaccos",
            "eggerju",
            "hgiger",
            "maegger",
            "mreimers",
            "szekely",
            "thaler",
            "vangool"
         ],
         "name" : "itet-staff",
         "export" : [
            "Realm"
         ],
         "description" : "selfmanaged Laptops, VLAN ETx::788,
129.132.40.0"
      },
      {
         "subgroups" : [],
         "member" : [
            "morari",
            "nguyenr",
            "thaler"
         ],
         "name" : "itet-staff-2",
         "export" : [
            "Realm"
         ],
         "description" : "Selfmanaged Laptops, VLAN ETx::786,
129.132.29.0"
      }
   ]
}
```

2.5 POST

2.5.1 nethz Custom Gruppe erzeugen

```
Synopsis: eine neue nethz Custom Group erzeugen

          obligatorsiche Parameter (JSON, body)
                name        : Name der nethz Custom Gruppe
                description : Beschreibung der Gruppe
                admingroup  : Name der übergeordneten nethz Admin Gruppe

HTTP method   : POST
URI  Resource : group
Content-Type  : application/json

Returns (HTTP Status Code):
- 201 Created     : Gruppe erfolgreich erzeugt
- 400 Bad request : Aufrufparameter nicht korrekt
- 404 Not found   : - Admin Gruppe nicht gefunden
                    - Nickname der Admin Gruppe nicht gefunden
- 409 conflict    : - eine Gruppe mit dem selben Namen existiert bereits
                    - Präfix der Custom Gruppe und Nickname der Admin Gruppe
                      passen nicht überein
```

- Beispiel

```
Request    <url>/group

- Params   {
               "group": {
                   "name": "ENTWU-Groupmgr-Test",
                   "description": "Hello World Test Group",
                   "admingroup": {
                       "name": "Entwurmer"
                   }
               }
           }

Response   {
               "grid": "4945508",
               "group": "ENTWU-Groupmgr-Test",
               "status": "[SUCCESS] created"
           }
```

2.5.2 Provisioning

```
Synopsis: Provisoning der Zielsysteme (modifizierte Gruppeninformationen werden nach AD,
          LDAPS oder CQ5 exportiert)

          obligatorsiche Parameter (JSON, body)
                group.name  : Name der nethz Custom Gruppe
                target.name : Zielsystem (AD, LDAPS, CQ5)
```

```
          Der Web Service Request startet nur den Prozess, wartet aber nicht das Pro-
          zessende des Provisioning ab

HTTP method   : POST
URI  Resource : group/provisioning
Content-Type  : application/json

Returns (HTTP Sttus Code):
- 202 Accepted    : Provisioning erfolgreich gestartet
- 400 Bad request : Aufrufparameter nicht korrekt
- 500 Internal Server Error
```

➢ Beispiel

```
Request    <url>/group/provisioning

- Params   {
               "group": {
                   "name": "ENTWU-Groupmgr-Test",
                   "targets": [
                       { "name": "AD" },
                       { "name": "LDAPS" }
                    ]
                }
           }

Response   {
              "target" : "AD, LDAPS",
              "group" : "ENTWU-Groupmgr-Test",
              "status" : "[ACCEPTED] start provisioning"
           }
```

2.6 PUT

2.6.1 Mitglieder einer nethz Custom Gruppe hinzufügen

```
Synopsis: Person(en) zu einer nethz Custom Gruppe hinzufügen

          obligatorsiche Parameter (JSON, body)
                group.name : Name der nethz Custom Gruppe
                user.name  : nethz Account Name

HTTP method   : PUT
URI  Resource : group/users
Content-Type  : application/json

Returns (HTTP Sttus Code):
- 200 OK          : die Person(en) wurden der Gruppe hinzugefügt
- 400 Bad request : Aufrufparameter nicht korrekt
- 409 Conflict    : nethz Account Name wurde nicht gefunden
- 500 Internal Server Error
```

➢ Beispiel

```
Request    <url>/group/users

- Params   {
             "group": {
               "name": "ENTWU-Groupmgr-Test",
               "users": [
                 { "name": "glange" },
                 { "name": "mreimers" },
                 { "name": "davidsch" }
               ]
             }
           }

Response   {
              "group" : "ENTWU-Groupmgr-Test",
              "status" : "[SUCCESS] created",
              "users" : [
                 "glange",
                 "mreimers",
                 "davidsch"
               ]
           }
```

2.6.2 Beschreibung der nethz Custom Gruppe ändern

```
Synopsis: Die Beschreibung einer existierenden nethz Custom Gruppe ändern

          obligatorsiche Parameter (JSON, body)
                group.name        : Name der nethz Custom Gruppe
                group.description : Beschreibung der nethz Custom Gruppe

HTTP method   : PUT
URI  Resource : group/description
Content-Type  : application/json

Returns (HTTP Sttus Code):
- 200 OK          : die Person(en) wurden der Gruppe hinzugefügt
- 400 Bad request : Aufrufparameter nicht korrekt
- 404 Not found   : - nethz Account der Person(en) wurde nicht gefunden
                    - Nickname der Admin Gruppe nicht gefunden
- 500 Internal Server Error
```

- Beispiel

```
Request    <url>/group/description

- Params   {
             "group": {
               "name": "ENTWU-Groupmgr-Test",
               "description": "aktualisierte Beschreibung"
             }
           }
```

```
Response   {
              "group" : "ENTWU-Groupmgr-Test",
              "status" : "[SUCCESS] updated",
              "description" : "aktualisierte Beschreibung"
           }
```

2.6.3 Provisioning Ziel setzen/aktualisieren

```
Synopsis: Provisioning Ziel einer existierenden nethz Custom Gruppe setzen oder
          aktualisieren.

          obligatorsiche Parameter (JSON, body)
                group.name  : Name der nethz Custom Gruppe
                target.name : Zielsystem (AD, LDAPS, CQ5)

HTTP method   : PUT
URI  Resource : group/provisioning
Content-Type  : application/json

Returns (HTTP Sttus Code):
- 200 OK          : Provisioning Ziel(e) wurden der Gruppe hinzugefügt
- 400 Bad request : Aufrufparameter nicht korrekt
- 500 Internal Server Error
```

- Beispiel

```
Request    <url>/group/provisioning

- Params   {
             "group": {
               "name": "ENTWU-Groupmgr-Test",
               "targets": [
                 { "name": "AD" },
                 { "name": "LDAPS" }
               ]
             }
           }

Response   {
              "target" : "AD, LDAPS",
              "group" : "ENTWU-Groupmgr-Test",
              "status" : "[SUCCESS] updated"
           }
```

2.7 DELETE

2.7.1 nethz Custon Gruppe löschen

```
Synopsis: Eine existierende nethz Custom Gruppe löschen.


HTTP method   : DELETE
URI  Resource : group/:name
Content-Type  : application/json

Returns (HTTP Sttus Code):
- 200 OK          : nethz Gruppe gelöscht
- 400 Bad request : Aufrufparameter nicht korrekt
- 500 Internal Server Error
```

- Beispiel

```
Request    <url>/group/ ENTWU-Groupmgr-Test

Response   {
              "group" : "ENTWU-Groupmgr-Test",
              "status" : "[SUCCESS] deleted"
           }
```

2.7.2 Mitglied einer nethz Custom Gruppe löschen

```
Synopsis: Ein Mitglied einer existierenden nethz Custom Gruppe löschen.

          obligatorsiche Parameter (query params)
                group/:name        : nethz Custom Gruppename
                user/:name         : nethz Account Name

HTTP method   : DELETE
URI  Resource : group/:name/user/:name
Content-Type  : application/json

Returns (HTTP Sttus Code):
- 200 OK          : die Person(en) in der Gruppe gelöscht
- 400 Bad request : Aufrufparameter nicht korrekt
- 404 Not found   : nethz Account der Person(en) wurde nicht gefunden
- 500 Internal Server Error
```

- Beispiel

```
Request    <url>/group/:name/user/:name

Response   {
              "group" : "ENTWU-Groupmgr-Test",
              "status" : "[SUCCESS] deleted"
           }
```

2.7.3 Provisioning Ziel löschen

```
Synopsis: Die Provisioning Ziel einer existierenden nethz Custom Gruppe löschen.

          obligatorsiche Parameter (query params)
                group/:name        : nethz Custom Gruppename
                provisioning /:name: Zielsystem (AD, LDAPS oder CQ5)

HTTP method   : DELETE
URI  Resource : group/:name/provisioning/:name
Content-Type  : application/json

Returns (HTTP Sttus Code):
- 200 OK          : die Person(en) wurden der Gruppe hinzugefügt
- 400 Bad request : Aufrufparameter nicht korrekt
- 404 Not found   : - nethz Account der Person(en) wurde nicht gefunden
                    - Nickname der Admin Gruppe nicht gefunden
- 500 Internal Server Error
```

- Beispiel

```
Request    <url>/group/ENTWU-Groupmgr-Test/provisioning/AD

Response   {
              "target" : "AD",
              "group" : "ENTWU-Groupmgr-Test",
              "status" : "[SUCCESS] deleted"
           }
```