deutsches forschungsnetz

Upgrade auf Shibboleth IdP 5.x

DFN-AAI

Doreen Liebenau (liebenau@dfn.de)
Andreas Borm (borm@dfn.de)

Agenda

- Allgemeine Neuerungen im IdP 5.x
- Vorbereitungen für das Upgrade (Schulungs-VM)
- Vorgehensweise beim Upgrade

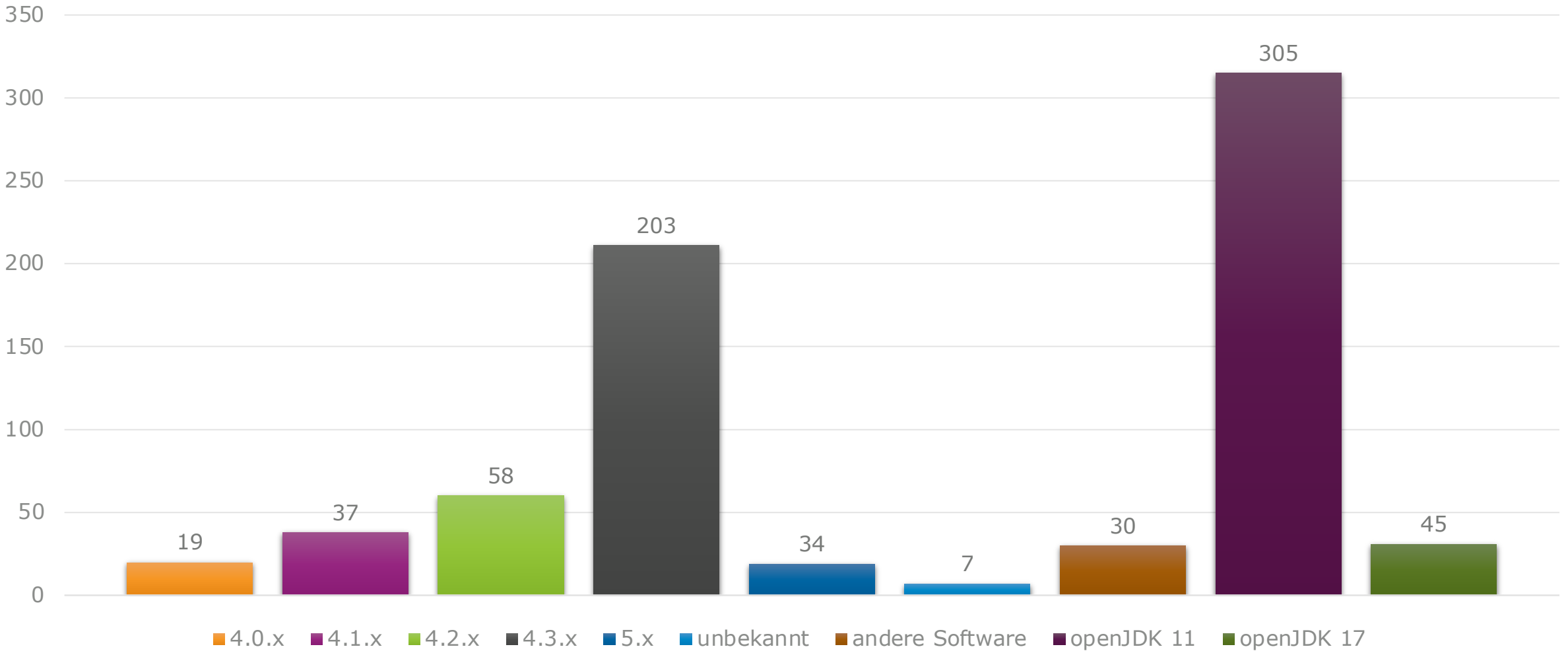
Intro

- Support für Shibboleth IdP 4.3.x läuft September 2024 aus
- IdPs mit dem Entity Attribut Sirtfi müssen bis dahin auf 5.x laufen
- IdPs ohne Sirtfi: Bitte bis Ende Juni 2025 upgraden
  - DFN-AAI kann nicht langfristig mehrere Versionen unterstützen
  - Sicherheitslücken lassen sich durch Einspielen eines Minor Updates auf einem aktuellen IdP schnell beheben
- Vortrag richtet sich an IdP-Betreiber*innen

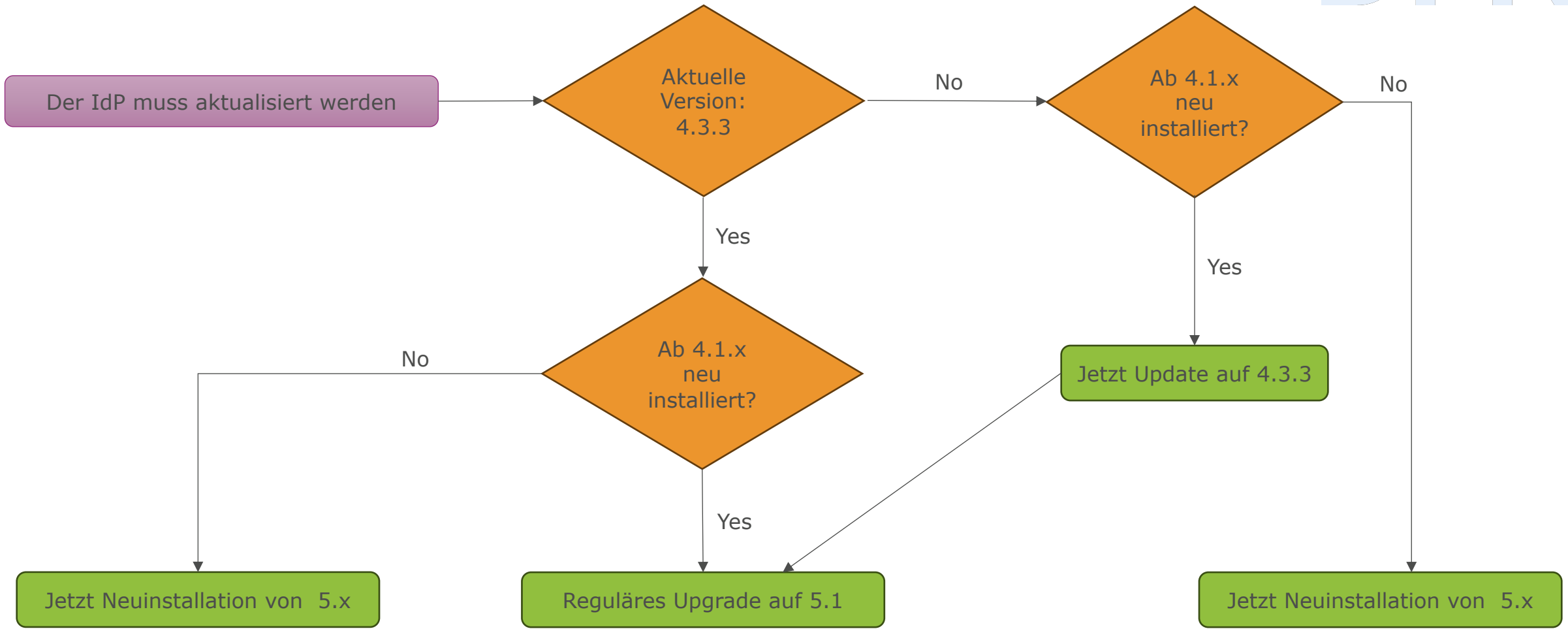
Die Schulungs-VM

- Debian 12
- Vorkonfiguriert:
  - Tomcat9, Apache 2.4
  - OpenLDAP mit Testaccounts
  - 2 Service Provider
  - Installation Shibboleth IdP unter /opt
- Credentials: shibboleth

High Score 12. Juni 24



Vorgehen beim Upgrade



Systemanforderungen

- Java 17 (Amazon Corretto, OpenJDK, ähnliche Distributionen)
- Servlet Container mit Servlet API 5.0 (Jetty 11+, Tomcat 10.1+)
- Bei Installation aus Paketquellen debianbasierter Linuxsysteme:
  - Debian 12
- ggf. ist der erste Schritt ein Betriebsystem-Upgrade

Plugins und Module

- Zusätzliche Funktionalitäten für den IdP, inkl. einheitlicher Routinen zur Wartung (./bin/module.sh)
- Aktivierung von Modulen (Hinterlegen spezifischer Konfigurationsdateien im Dateibaum)
  - bin/module.sh -- eanable module-ID
- Deaktivieren von Modulen (vorhandene Konfigurationsdateien = enabled)
  - /bin/module.sh -- disable module-ID --clean
- Bei Upgrade
  - Filename.idpnew-idpversion: Default-Configs von geänderten Dateien
  - Filename.idpsave: Konfigs, die bei Deinstallation gesichert wurden

Module I

- Module kapseln eine optionale Funktion der Software
- Beinhalten die Möglichkeit, optionale Dateien zu installieren, aktualisieren oder zu entfernen, die zu dieser Funktion gehören
- Also note that after upgrading from an older version, you will find that most/all modules will claim to be "enabled". This because in most cases, that status depends on the existence of the configuration files that the module is managing, and most of those files existed prior to the module system's development.
- If you're not using it, none of those files are needed. So, if you're not using the feature, having those files installed and in the way is just annoying and confusing.
- Module enthalten: views, properties, xml-Dateien
- Module werden mit dem IdP versioniert (anders als die Plugins)

- Quelle: https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199510765/ModuleConfiguration

Module II

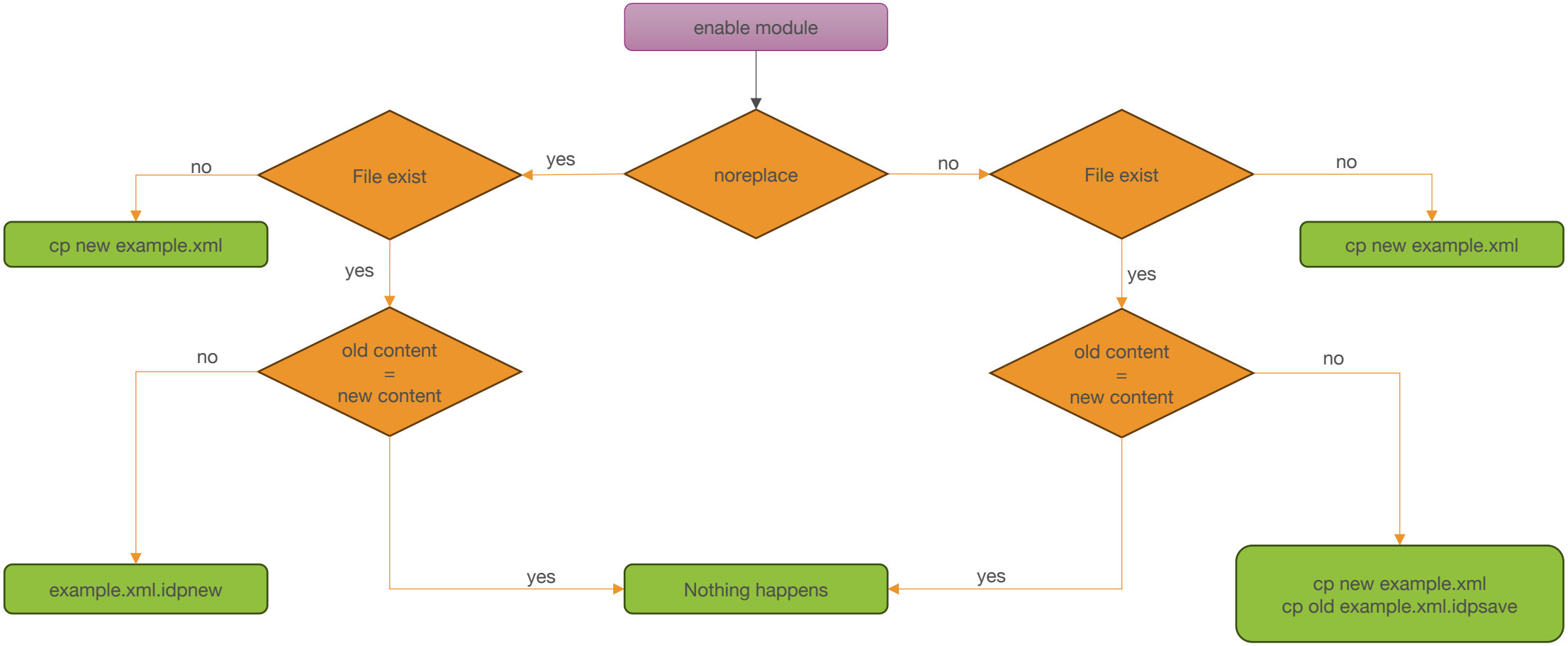
- Alle für den Benutzer sichtbaren oder änderbaren Dateien werden von einem der drei neuen Module (idp.Core, idp.CommandLine und idp.EditWebApp) kontrolliert, d.h. lokale Änderungen werden fast immer beibehalten

```
# bin/module.sh -l

Module: idp.Core [ENABLED]

Module: idp.CommandLine [ENABLED]

Module: idp.EditWebApp [ENABLED]
```

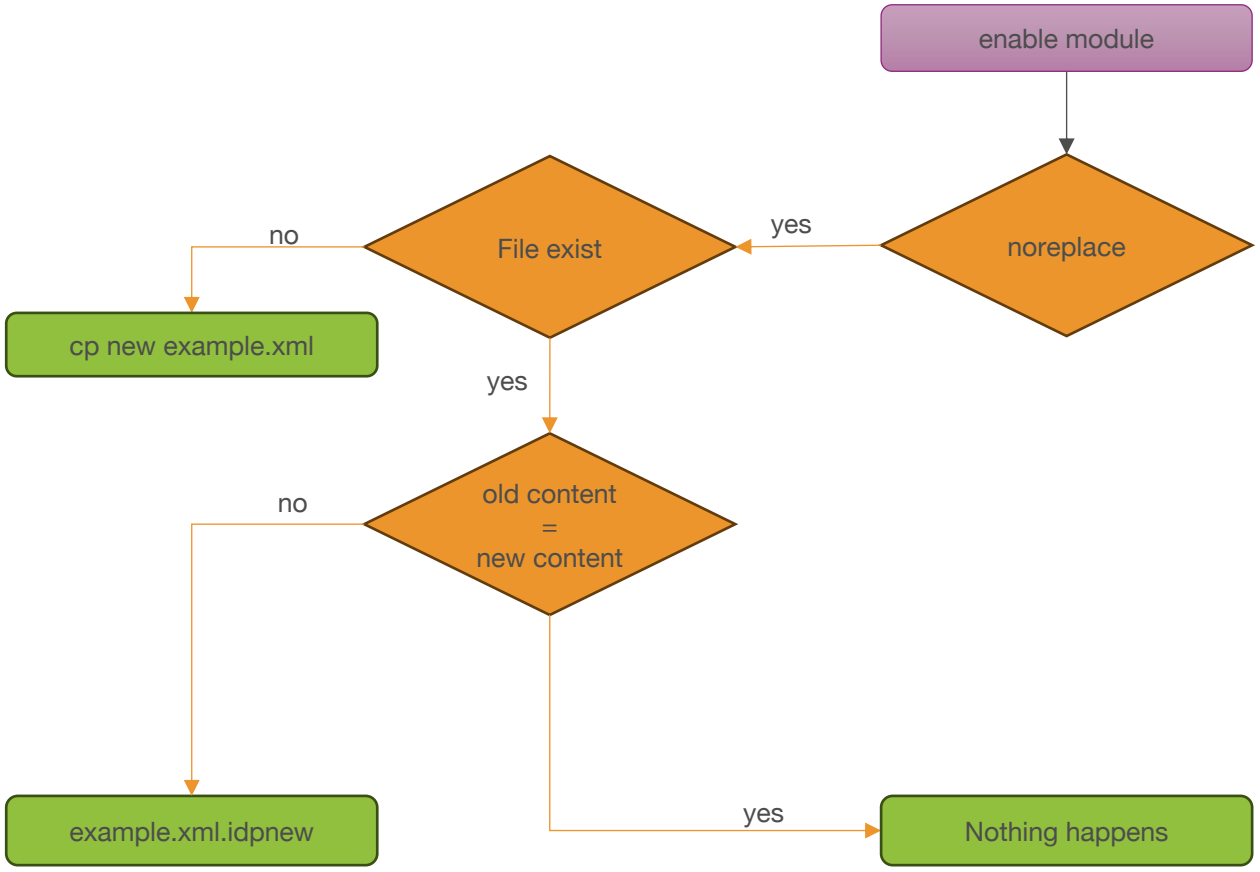
- Detaillierte Informationen zum Modul & dazugehörigen Config-Dateien

```
$ bin/module.sh -i module-ID
```

Module III


enable module
noreplace
File exist
no
cp new example.xml
yes
old content
=
new content
no
example.xml.idpnew
yes
Nothing happens
yes
File exist
no
cp new example.xml
yes
old content
=
new content
no
cp new example.xml
cp old example.xml.idpsave
yes

Module IV



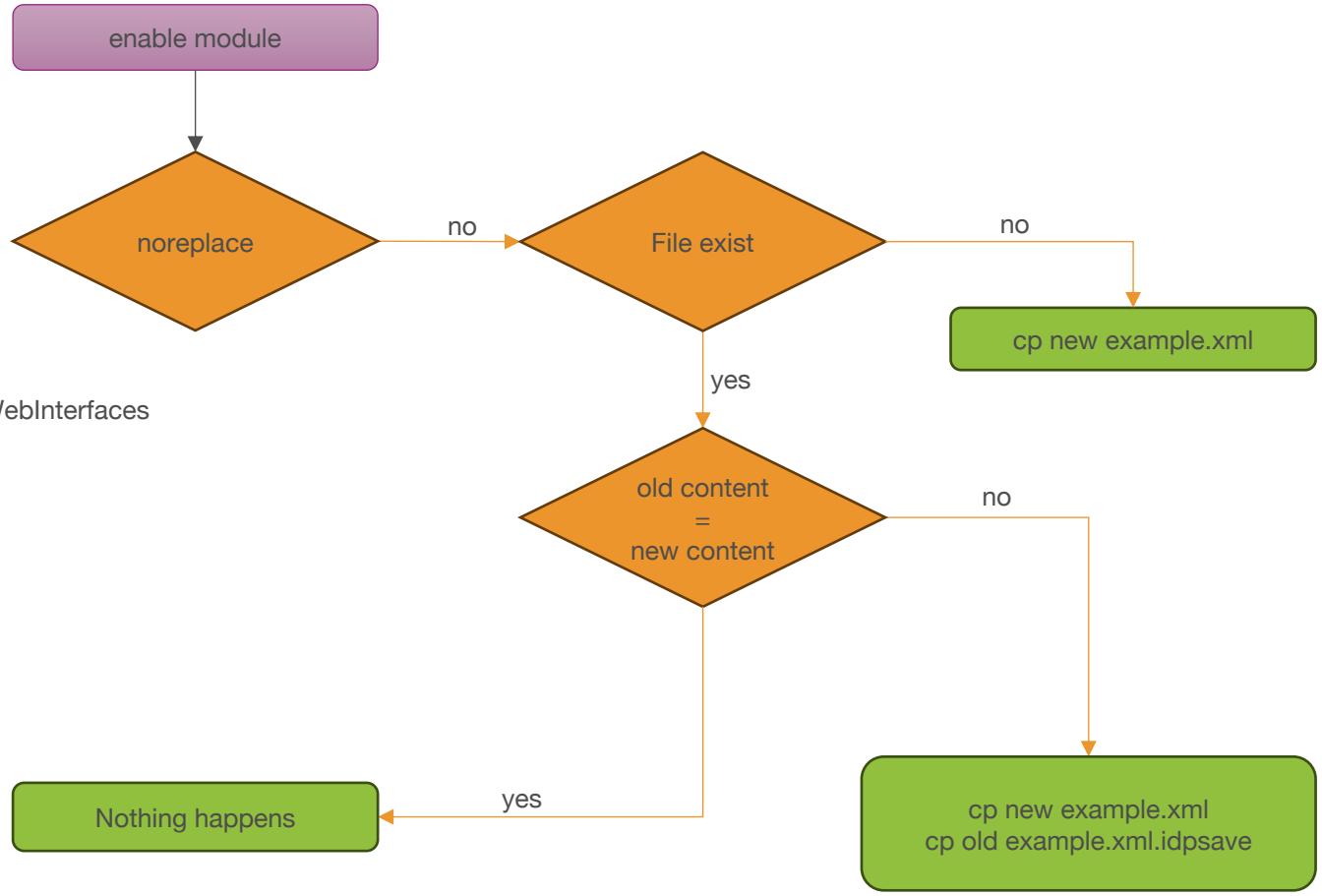

```
$ bin/module.sh -i idp.Core

Module: idp.Core
Name: Core IdP Functions (Required)
Desc: Module that provides built-in IdP functionality
Help: https://shibboleth.atlassian.net/wiki/spaces/IDP5/
Status: ENABLED

Resource: (noreplace) views/error.vm
Resource: (noreplace) views/logout.vm
..
Resource: (noreplace) conf/access-control.xml
Resource: (noreplace) conf/attribute-filter.xml
Resource: (noreplace) conf/attribute-registry.xml
Resource: (noreplace) conf/attribute-resolver.xml
Resource: (noreplace) conf/idp.properties
Resource: (noreplace) conf/ldap.properties
```

Nach Update:

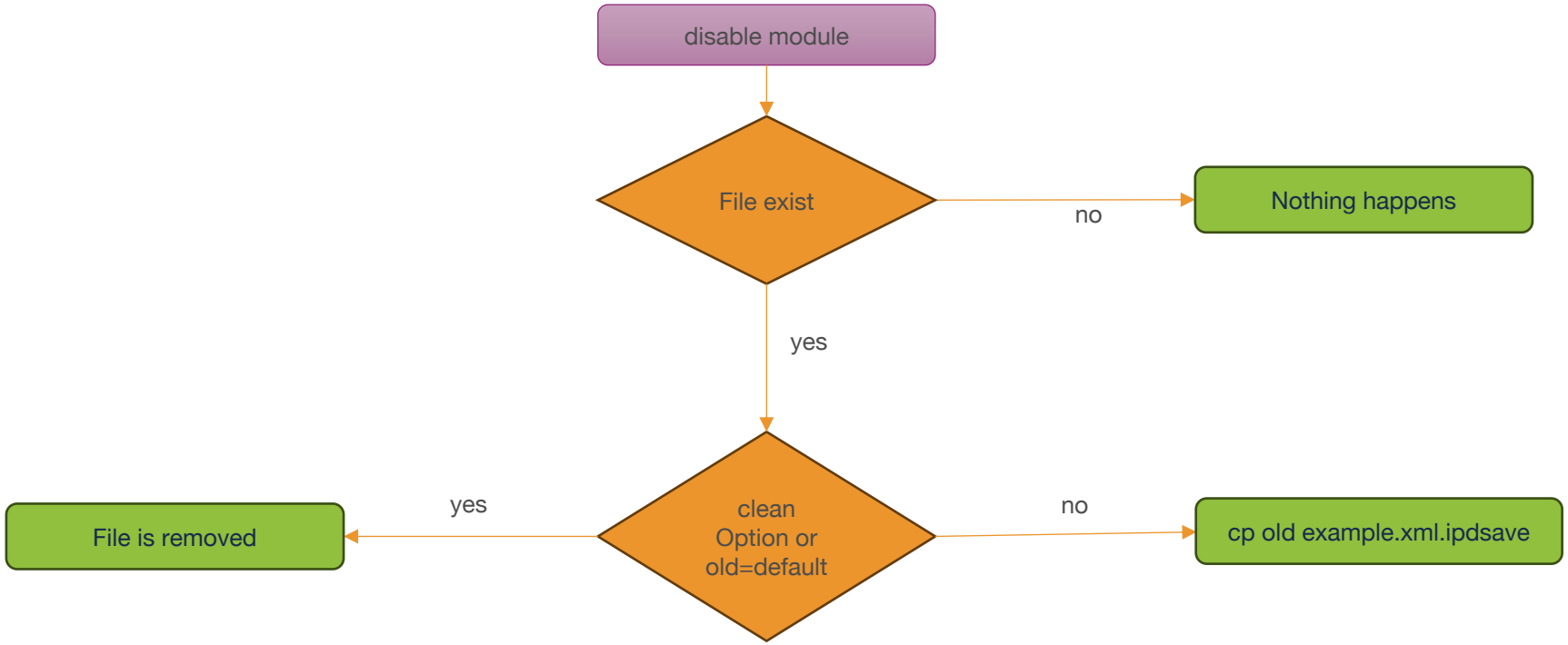
```
$ ls -la /opt/shibboleth-idp/conf/
..
idp.properties
idp.properties.idpnew-511
..
```

Module V

```
$ bin/module.sh -i idp.CommandLine

Module: idp.CommandLine
Name: Command Line Scripts
Desc: Command line scripts for managing services or rebuilding the warfile
Help: https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199511365/WebInterfaces
Status: ENABLED
…
Resource: ( replace) bin/keygen.sh
Resource: ( replace) bin/keygen.bat
Resource: ( replace) bin/mdquery.sh
Resource: ( replace) bin/mdquery.bat
Resource: ( replace) bin/plugin.sh
Resource: ( replace) bin/plugin.bat
…
Resource: ( replace) bin/status.sh
Resource: ( replace) bin/status.bat
Resource: ( replace) bin/update.sh
Resource: ( replace) bin/update.bat
Resource: ( replace) bin/version.sh
Resource: ( replace) bin/version.bat
…
```



Module VI


disable module
File exist
no
Nothing happens
yes
clean
Option or
old=default
yes
File is removed
no
cp old example.xml.ipdsave

Plugins I

- Zusatzpakete, die Funktionalität hinzufügen
- Upgrade IdP und Plugin werden unabhängig voneinander entwickelt & aktualisiert
- Können direkt aus dem Internet installiert & aktualisiert warden
- Müssen signiert sein
- Installation aus einer im Internet gehosteten Datei oder lokal möglich
- Hat keine Konfiguration
- Plugin-Entwickler gibt vor, ob automatisch ein Modul bei Installation aktiviert wird

Plugins II

- `/opt/shibboleth-idp/bin/plugin.sh -fl`

```
…

Plugin: net.shibboleth.idp.plugin.nashorn Current Version: 2.0.0
Plugin Versions
1.0.0: Min=4.1.0 Max=5.0.0 Support level: Withdrawn
1.1.0: Min=4.1.0 Max=5.0.0 Support level: Current
2.0.0: Min=5.0.0 Max=6.0.0 Support level: Current
```

- Support Level
  - OutOfDate: funktioniert, neue Version verfügbar
  - Secadv: es gibt Sicherheitswarnung für dieses Plugin
  - Withdrawn: zurück gezogen
  - Current: aktuell
- Weitere Optionen: https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199500688/PluginInstallation#Operation-Qualifiers

Verzeichnisstruktur

`bin`	• CLI-Tools & während der Installation benötigte Java-Bibliotheken • Distributions-Dateien werden bei Updates überschrieben • Zusätzlich hinzugefügte Dateien bleiben erhalten
`conf`[1]	• Hauptkonfiguration
`credentials`[1]	• Schlüssel, Zertifikate, Schlüsselspeicher und Anmeldeinformationen, z.B. Validierung v. Metadatensignaturen • Soll nur für das den IdP ausführende Benutzerkonto lesbar sein
`dist`	• Originalversion des Inhalts von *conf*, flows, *messages* & *views* • Verzeichnis wird bei jeder Installation gelöscht und neu erstellt
`edit-webapp`[1]	• Anpassungen an Stylesheets, Grafiken, zus. `.jar`-Files → nach Änderungen IdP-Servlet neubauen: `./bin/build.sh`
`flows`[1]	• vom User editierbare Spring Web Flow Definitionen
`logs`	• Default-Verzeichnis für Diagnose- & Audit-Logs
`messages`[1]	• sprachspezifische Beschriftungen
`metadata`	• SAML-Metadaten • Bei Erstinstallation wird *idp-metadata.xml* erzeugt (Einstiegsbeispiel, keine echte Metadatenquelle!)
`views`[1]	• Velocity-Templates für HTML-Seiten (Login, User Consent)
`war`	• gepackte IdP-War-Datei für das Deployment

[1] Hinzufügen von Dateien bei Upgrades, Keine Ersetzung bei Installation od. Upgrades

LDAP Änderungen

- **ldap-authn-config.xml (V4.0)** wird nicht mehr funktionieren
- stattdessen: **ldap.properties & password-authn-config.xml**
  - Vor V 4.1 verschiedene LDAP-Pooling-Eigenschaften → numerische Werte in Sekunden, z.B: 300== 5 Min
  - Ab V 4.1 Interpretation in Millisekunden → übermäßig häufige Pool Validierung
- Empfehlung: Nach dem Upgrade diese Dateien neu anlegen
- Bleibt die alte Datei bestehen, kommt es zur Fehlermeldung -->veraltete ldap-authn-config.xml

Removed or Deprecated

- Removed Properties
  - Modul idp.duo.* entfernt; ersetzt durch Plugin **DuoOIDC**
  - idp.httpclient.filecaching.cacheDirectory entfernt
- Removed Features
  - EntityRoleWhiteList; ersetzt durch EntityRole
- Deprecated Objects
  - Liberty.SSOS & Liberty.SSOS.MDDriven
  - shibboleth.SameSiteCookieFilter & shibboleth.ResponseHeaderFilter (referenced in older *web.xml*)
- Deprecated Java Class
  - net.shibboleth.idp.profile.context.RelyingPartyContext, ersetzt durch: net.shibboleth.profile.context.RelyingPartyContext
- (eduPersonTargetedID bleibt bestehen)
- Vollständige Liste: https://shibboleth.atlassian.net/wiki/spaces/IDP5/pages/3199500367/ReleaseNotes

Vorbereitungen für das Upgrade

Upgrade OpenJDK 11 auf 17

- Ab IdP 4.1 unterstützt OpenJDK 17
  - Vorarbeit: Installation Java 17
  - IdP 4.1 ist damit weiter lauffähig
- Javascript Scripting Engine Nashorn wird nicht mehr ausgeliefert
  - Stattdessen: Nashorn-Plugin installieren (ab IdP 4.2)
- Datenbank-Verbindung wird im IdP 5.x nicht mehr über den JPA Storage Service hergestellt
  - Stattdessen: JDBC-Plugin installieren (ab IdP 4.2)
- https://doku.tid.dfn.de/de:shibidp:upgrade_openjdk_11_auf_openjdk_17

Vorgehen beim Upgrade

Vorgehen beim Upgrade I

- *“V5 is a simple upgrade from V4 for the vast majority of people”*
- *“So far the upgrade process has been very smooth, and this appears to be the least impactful major upgrade in the project’s history”*
- *Quelle:* Shibboleth Development Center
- Datensicherung von idp.home und Datenbank
- nicht überschrieben werden ./conf, ./flows, ./metadata, ./credentials, ./messages und ./edit-webapp

Vorgehen beim Upgrade II

- Deprecation Warnings?
  - $ tail –f idp-process.log bzw.
  - $ tail –f idp-warn.log
  - $ tail –f /var/log/tomcat10/Catalina-date.log
- Aktualisierung auf IdP 4.3.3
- Gewohnte Upgrade-Routine:
  - Download und Entpacken des IdP 4.x
  - Aufruf des Installers (Linux: ./bin/install.sh -Didp.conf.filemode=644), Angabe des Zielverzeichnisses der alten Installation
  - IdP-Logs beobachten und testen
  - neue Deprecation Warnings abarbeiten

Upgrade

- Ab hier weiter mit https://doku.tid.dfn.de/de:shibidp:upgrade5

Handler

- Sie können über URLs bestimmte Handler direkt aufrufen. Hier ein paar Beispiele:
- **Identity Provider**
  - Logout (Session am IdP beenden): https://hostname/idp/profile/Logout
- **Service Provider**
  - Metadata-Handler eines SP aufrufen: https:// hostname /Shibboleth.sso/Metadata (im Browser öffnen, Seitenquelltext anzeigen)
  - Session-Handler am SP aufrufen: https:// hostname /Shibboleth.sso/Session
  - Logout-Handler am SP aufrufen: https:// hostname /Shibboleth.sso/Logout

Dokumentation & Support

- Shibboleth-Wiki: https://shibboleth.atlassian.net/wiki/spaces/IDP5/overview
- DFN-AAI-Wiki: https://doku.tid.dfn.de/en:dfnaai:start
  - Troubleshooting allgemein: https://doku.tid.dfn.de/de:shibidp:troubleshooting
  - Troubleshooting IdP 5: https://doku.tid.dfn.de/de:shibidp:troubleshooting_idp_5
- Mailinglisten DFN: dfn-aai-users@listserv.dfn.de & dfn-aai-announce@listserv.dfn.de
- Mailinglisten Shibboleth: users@shibboleth.net & announce@shibboleth.net
- DFN-AAI: hotline@aai.dfn.de
- Funktionstest (IdP & SP): https://doku.tid.dfn.de/de:functionaltest

Vielen Dank! Gibt‘s Fragen?

- Kontakt
  - DFN-AAI Team

    E-Mail: hotline@aai.dfn.de
    Tel.: +49-30-884299-9124
    Fax: +49-30-884299-370

    Anschrift:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz 1
    10178 Berlin