A Admin-Toolbox

Als Systemadmin möchte man alle wichtigen Werkzeuge zur Systemverwaltung gerne an einer Stelle haben. Man kann unter Windows mit der *Microsoft Management Console*, ähnlich einem Baukastensystem, sein eigenes Konfigurationstool bauen (die MMC-Technologie wird nämlich von zahlreichen Microsoft-Verwaltungswerkzeugen verwendet).

In dieser Übung stellen Sie sich Ihre eigene "Admin-Toolbox" für Windows 11 (das funktioniert seit vielen Windows Versionen, dh. auch unter Windows 10), erkunden eine Reihe nützlicher Werkzeuge und lernen, wie man wichtige Meldungen des Systems in der Ereignisanzeige (Systemprotokoll – *Event Log*) nachlesen kann. Bitte beantworten Sie alle Fragen und schreiben Sie alle relevanten Schritte in Ihr Protokoll und fügen Sie ggf. Screenshotsein!

Tipp: Mit dem Windows-*Snipping-Tool* können Sie sehr einfach einen Bildschirm-Ausschnitt "abfotografieren". Dieser *Screenshot* wird automatisch in der Zwischenablage gespeichert und steht sofort auch außerhalb der virtuellen Maschine auf Ihrem Linux-Host zur Verfügung.

B Inbetriebnahme der VM und Kennenlernen des Windows 11 *User Interfaces*

Erstellen Sie wenn notwendig eine neue virtuelle Windows 11-Maschine (ein virtueller PC als *Linked Clone*, siehe Anleitung) und melden Sie sich mit Admin-Rechten (User/Passwort: `junioradmin`) an!

(1) Ändern Sie den Namen des Computers auf UE01-*IhrFamiliennname-IhrVorname (Tipp: Systemsteuerung → Kleine Symbole → System → Erweiterte Systemeinstellungen* oder schneller: Tastenkombination `Windows+Pause)`! Wie lautete der Standardname? Was ist notwendig, damit die Änderung des Computernamens tatsächlich durchgeführt wird? Dokumentieren Sie hier anhand eines Screenshots[1], dass Ihr Rechner erfolgreich umbenannt wurde!

(2) Jetzt ist ein guter Zeitpunkt um einen *Snapshot* zu erstellen. VMware speichert den Zustand der virtuellen Maschine (Festplatte und Einstellungen), man kann jederzeit zu diesem Zustand *zurückkehren*. Machen Sie den Snapshot mit dem Namen "init" am besten bei heruntergefahrener VM!

Dokumentieren Sie die Schritte, um einen Snapshot zu erstellen!

(3) Machen Sie sich mit dem Windows 11 *User Interface* vertraut. Dokumentieren und merken Sie sich, wie man folgende Werkzeuge möglichst *schnell* aufrufen kann! (*Tipp*: Nutzen Sie das Handout über Windows-Tastenkombinationen!)

a) Erweitertes Kontextmenü (*Quicklink* zu den wichtigsten Verwaltungswerkzeugen im *Desktop*)
b) Explorer -Fenster öffnen Hauptfenster
c) Einstellungen (Modern UI Style)
d) Systemsteuerung (klassisch)
e) Task-Manager
f) Systemeigenschaften (*Info-Feld "System"*)
g) Geräte-Manager
h) Terminal = Kommandozeile: ist seit Windows 10 1703 (Creators + Update) nicht mehr CMD sondern die *Powershell*
i) Snipping-Tool, um einen Screenshot in die Zwischenablage zu kopieren
j) Bonus: Fügen Sie 2 virtuelle Desktops hinzu, starten Sie im ersten der neuen virtuellen Desktops den Taschenrechner `calc.exe` und im anderen den Task-Manager. Wozu sind virtuelle Desktops nützlich?

[1] Im Linux Desktop können Sie mit der Tastenkombination `STRG + Shift + Druck` einen rechteckigen Bildschirmbereich in die Zwischenablage kopieren!

(4) Welche Windows-Version (mit genauer *Build-Nummer*) haben Sie installiert? Mit welchem Programm (das Sie mit Windows-R starten können) haben Sie das ermittelt?

C Microsoft Management Console

C.1 Allgemeines zu MMC

(5) Beantworten Sie z.B. durch Internet-Recherche die folgenden Fragen zur MMC:

a. Wozu dient die MMC?
b. Was ist ein *Snap-in*?
c. Nennen Sie zwei Beispiele vorgefertigter System-Tools, welche die MMC nutzen!

C.2 Anlegen einer eigenen MMC

(6) Rufen Sie eine leere MMC-Konsole auf und fügen Sie die folgenden Snap-Ins (bzw. "Ordner") hinzu (alle für den lokalen Computer), damit folgende Baumstruktur entsteht (lesen):

Achtung: Die Untergruppen von "Ereignisanzeige" sind als Teil des Snap-Ins bereits vordefiniert, also vorhanden! Die "Ordner" `Hardware` `hrFamilienname_System` und `Netzwerk25` müssen Sie aber selbst anlegen!

Tipp: Wo notwendig, erst den Ordner mit dem vorläufigen Namen `Ordner` hinzufügen, dann den Ordner entsprechend umbenennen, etwa `Hardware`, `IhrFamilienname_System` ... Sodann fügen Sie das gewünschte Snap-In dem Ordner hinzu, indem Sie als `Übergeordnetes Snap-In` den Ordnernamen (*nicht* `Konsolenstamm`) angeben!

```
- Konsolenstamm
  - Ereignisanzeige
     |- Benutzerdefinierte Ansichten
     |- Windows-Protokolle
     |- Anwendungs- und Dienstprotokolle
     |- Abonnements
  - Hardware
     |- Geräte-Manager
     |- Datenträgerverwaltung
  - IhrFamilienname_System
     |- Lokale Benutzer und Gruppen
     |- Freigegebene Ordner
     |- Dienste
     |- Leistung(-süberwachung)
  - Netzwerk25
     |- Windows Defender Firewall mit erweiterter Sicherheit
```

Fügen Sie ein Screenshot in Ihr Protokoll!

(7) Speichern der Konsole: Geben Sie Ihrer Konsole den Namen `Die traumhafte Konsole von IhrVorname IhrFamilienname anno 2025` und speichern Sie Ihre Konsole mit dem Dateinamen `dtk.msc` (unter dem vorgeschlagenen Standardpfad) ab!

a. *Wo* ist die Datei `dtk.msc` im Dateisystem abgelegt? *(Absoluter Pfad gesucht, also* `C:\Users\...\dtk.msc`*- Tipp : Speichern unter → Eigenschaften → Ort)*

b. Wie können Sie diese angepasste Konsole also wieder aufrufen *(zum Testen vorher alle Fenster schließen)*?

C.3 MMC Snap-Ins

(8) Erkunden Sie die einzelnen Snap-Ins:

a. *Geräte-Manager:*

i. Wie kann man den Netzwerkzugriff über einen bestimmten Netzwerkadapter gänzlich unterbinden (ohne ihn ganz zu entfernen/deinstallieren)?

ii. Probieren Sie das aus – wie testen Sie das?

b. *Freigaben:*

Man kann einzelne Ordner anderen Computern im Netzwerk über sogenannte *Freigaben* verfügbar machen – Benutzer von anderen Computern können dann auf diese Ordner über ein sogenanntes *Netzwerklaufwerk* zugreifen, sofern sie die nötigen Freigabe und Dateisystem-(NTFS)-Rechte haben.

i. Was kann man mit Hilfe des Snap-ins "Freigegebene Ordner" so alles machen (zum Beispiel ansehen)?

ii. *(Daraus:)* Welche Ordner werden automatisch (aber nur für Administratoren) im Netzwerk freigegeben? *Zum Nachdenken:* Ist das ein Sicherheitsproblem?

c. *Dienste:*

Dienste (*Services*) sind Programme, die vom Betriebssystem meist automatisch gestartet werden und "im Hintergrund werken", d.h. normalerweise nicht mit dem Benutzer interagieren:

i. Welche vier Einstellungen zum Starttyp kann man zu den einzelnen Diensten(*Service*) im Snap-in *Dienste* vornehmen?

ii. Starten Sie den Drucker-Spooler (`Druckwarteschlange`) neu!
   1. Wie haben Sie das gemacht?
   2. Wann/Warum wird man das in der Praxis evtl. machen?

iii. Verhindern Sie, dass Windows-Media-Player in der Lage ist, über das Netzwerk Audio/Video-Dateien an *Universal-Plug-and-Play-(UPnP)*-Media-Streaming-Geräte (wie z.B. die Xbox) weiterzugeben!

iv. *Bonusaufgabe für Sicherheitsbewusste*: Schalten Sie die Windows-Telemetrie-Dienst (Benutzererfahrungen und Telemetrie im verbundenen Modus) dauerhaft ab!

d. *Leistung:*

Starten Sie den *Ressourcen-Monitor* aus dem Leistungs-Snap-In! Wie vergleicht sich der Informationsgehalt mit dem (Ihnen vermutlich bekannten) *Task Manager*?

(9) Schnellzugriff auf Snap-Ins:

Mit welchem tatsächlichen Namen kann man die folgenden Snap-Ins (mitsamt einer MMC-Instanz) **direkt** ausführen (mit der Tastenkombination `Windows + R`)?

Tipp: Suchen Sie Dateien namens `*.msc` unter `C:\Windows\System32` mit der Explorer-Suchfunktion!

Beispiel: Ereignisanzeige ⟶ `eventvwr.msc` *(Testen!)*

Geräte-Manager ⟶ …

Datenträgerverwaltung ⟶ …

Lokale Benutzer und Gruppen ⟶ …

Lokale Sicherheitsrichtlinie → …

D Systemüberwachung und Protokolle

In diesem Teil der Übung werden Sie sich mit der Verwendung des MMC-*Snap-In Ereignisanzeige (Event Log)* zur Fehlererkennung und Systemüberwachung auseinandersetzen – ein mächtiges Werkzeug, um Fehlfunktionen und Störungen des Windows-Computers auf die Schliche zu kommen!

In der Ereignisanzeige protokolliert Windows alles, was es für erwähnenswert hält. Dazu gehören nicht nur schwere Systemfehler, Probleme bei fehlerhaft konfigurierter Hardware, Ereignisse wie z.B. Updates oder jeden Start von Windows. Selbst wenn Windows völlig einwandfrei konfiguriert wurde, werden in der Ereignisanzeige zahlreiche Einträge über Warnungen und Fehler protokolliert. Windows stuft nämlich viele harmlose Ereignisse als Fehler oder Warnung ein. Um nicht die "Nadel im Heuhaufen" suchen zu müssen, sollten Sie daher die Log-Einträge gezielt durchforsten.

D.1 Benutzerdefinierte Ansicht der Ereignisanzeige

(10) Es gibt zahlreiche Ereignisprotokolle – mit einer *Benutzerdefinierten Ansicht* können Sie Log-Einträge aus den verschiedenen Quellen kombinieren, nur bestimmte Ereignisse betrachten und filtern:

Legen Sie eine benutzerdefinierte Ansicht "Wichtige Sachen von IhrName 2025" an, die kritische/wichtige Fehler sowie Warnungen aus den Logs (Windows-Protokollen) für "Anwendungen", "System", "Sicherheit" sowie "Hardware-Ereignisse" zusammenfasst.

(11) Wählen Sie eines der nun angezeigten Ereignisse aus und dokumentieren Sie exemplarisch den Fehler/die Warnung. Verwenden Sie zur besseren Klärung des Ereignisses evtl. auch die Informationsseite www.eventid.net. Kopieren Sie einen Screenshot des Ereignisses in Ihr Protokoll.

(12) Leeren (= Löschen der Einträge) Sie die Protokolle *(Logs)* "Anwendung", "Sicherheit" und "System" als Vorbereitung für unseren Bonus-Übungspunkt.

(13) Welche Auswahl haben Sie, wenn Sie die Ereignisse löschen?

D.2 Bonus: Lokale Sicherheitsrichtlinie und Sicherheitsprotokollierung

(14) Öffnen Sie aus der Systemsteuerung unter "Verwaltung" das *Snap-In* "Lokale Sicherheitsrichtlinie".

a. Wie heißt eigentlich die `.msc`-Datei? *Tipp:* Das haben Sie vorhin bereits ermittelt! ;-)

b. Aktivieren Sie die Überwachungsrichtlinie für

   i. Anmeldeereignisse (erfolgreich und fehlgeschlagen),
   ii. Anmeldeversuche (fehlgeschlagen) und
   iii. Kontenverwaltung (erfolgreich).

c. Schließen Sie diese Konsole und wechseln Sie zu Ihrer MMC.

(15) Anlegen von Benutzerkonten:

a. Erzeugen Sie ein neues Benutzerkonto für sich. Verwenden Sie als Kontonamen Ihren Vornamen (klein geschrieben). Das Kennwort soll zunächst gleichlautend mit dem Kontonamen sein. Aktivieren Sie aber die Option "Benutzer muss Kennwort bei der nächsten Anmeldung ändern".

b. Schließen Sie alle Fenster, melden Sie sich ab, dann mit Ihrem neu erstellten Benutzer an *(Sie sollten Ihr Passwort ändern müssen).*

c. Melden Sie sich anschließend wieder als `junioradmin` an. Öffnen Sie Ihre MMC und kontrollieren Sie die Protokollierungen, indem Sie Einträge finden für …

i. die Erstellung des neuen Kontos,
ii. die Passwortänderung,
iii. den Login durch den neuen Benutzer!

(Tipp: Suchen Sie im Sicherheitsprotokoll z.B. nach `ändern`, `erstellt` usw.).

→ Kopieren Sie die wesentlichen Infos (nach Ihrer Einschätzung) aus den Ereignisprotokolleinträgen in Ihr Laborprotokoll!

Viel Spaß!