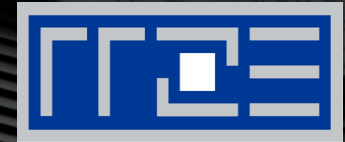


REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Windows-Betriebssysteme

Systemausbildung – Grundlagen und Aspekte von
Betriebssystemen und System-nahen Diensten

Sebastian Zenger, RRZE, 31.05.2017

Dieser Vortrag wird aufgezeichnet.

**Die ersten beiden Sitzreihen
befinden sich im Kameraradius.**

Agenda

- Server- und Client-Betriebssysteme
- Benutzerverwaltung
- Registry
- Gruppenrichtlinien-Objekte (GPOs)
- Windows-Updatebezug
- Windows-Firewall
- Windows-Aufgabenplanung
- Ereignisanzeige
- Terminalserver

Server- und Client-Betriebssysteme

- Trennung zwischen Server- und Client-Betriebssystemen
- Server
 - Zentraler Betrieb von Diensten (z.B. Fileserver, Druckserver, etc.)
- Client
 - Arbeitsstation für Endbenutzer
- Server- und Client-Versionen aus einer Generation
 - Windows Server 2008 R2 / Windows 7 SP1
 - Windows Server 2012 R2 / Windows 8.1
 - Windows Server 2016 / Windows 10



DIE BENUTZERVERWALTUNG



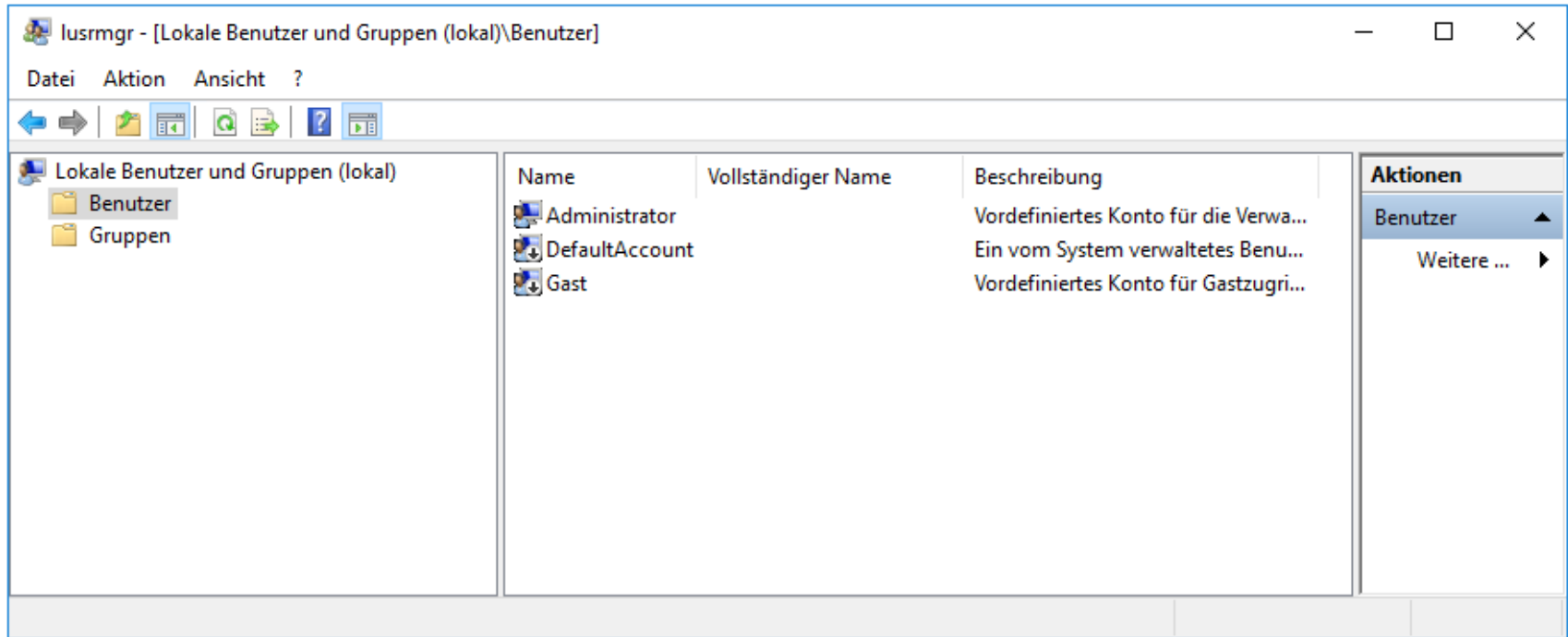
Einführung Benutzerverwaltung

- Benutzerkonto (SID)
- Access Token für den Benutzer
- Security Account Manager (SAM)
- Lokale- und zentrale Benutzerverwaltung

Benutzerverwaltung

- Anlegen und Verwalten von Benutzern
- Vereinfachte Benutzerverwaltung
 - Erweiterung der Systemsteuerung
 - Eingeschränkter Funktionsumfang
- Erweiterte Benutzerverwaltung
 - lusrmgr.msc
 - vorkonfigurierte Management-Konsole

lusrmgr.msc – Benutzer



Benutzereigenschaften

- Benutzername
- Vollständiger Name
- Beschreibung
- Kennwort
- Weitere Einstellungen

Neuer Benutzer

Benutzername: Testuser

Vollständiger Name: Sebastian Zenger

Beschreibung: Arbeitsgruppe Windows

Kennwort:

Kennwort bestätigen:

☐ Benutzer muss Kennwort bei der nächsten Anmeldung ändern

☐ Benutzer kann Kennwort nicht ändern

☐ Kennwort läuft nie ab

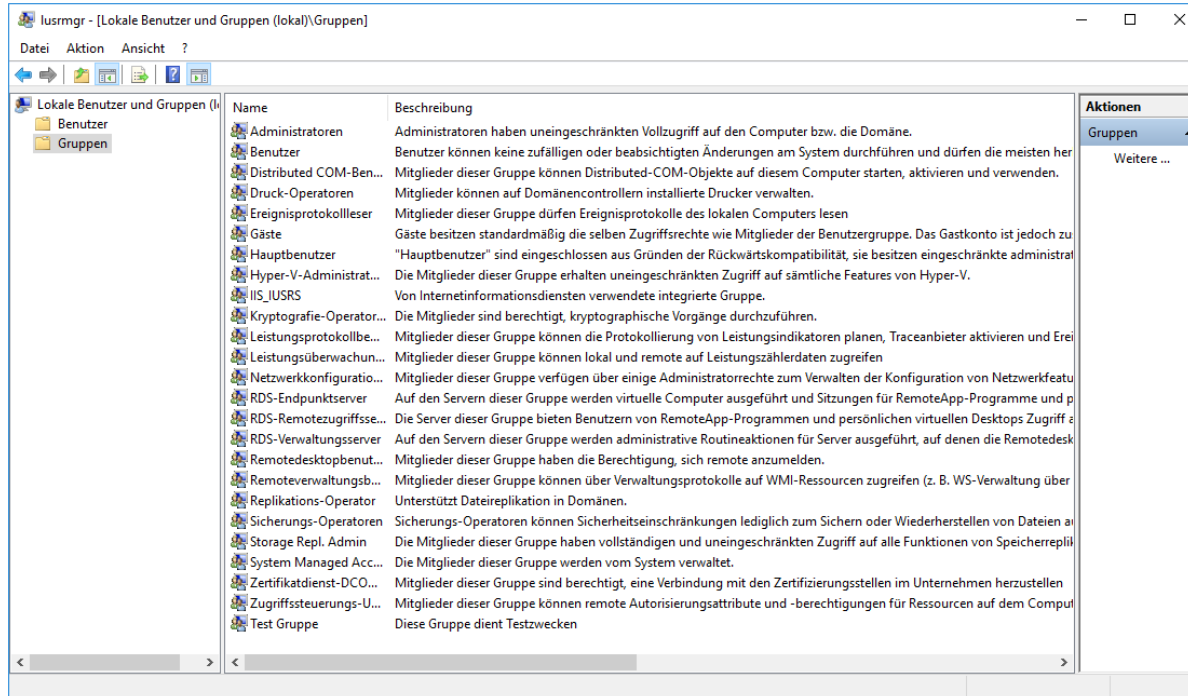
☐ Konto ist deaktiviert

Hilfe Erstellen Schließen

Gruppenmitgliedschaften

- Benutzer muss mind. einer Gruppe angehörig sein
- Standardgruppe ist „Benutzer“ bzw. „Domänen Benutzer“
- Benutzer in Gruppe aufnehmen bzw. entfernen
- Rechtesteuerung sollte über Gruppen realisiert werden

Iusrmgr.msc - Gruppen



Benutzerprofil

- Das Benutzerprofil speichert Einstellungen des Benutzers
- Profiltypen (C:\Users\...)
 - Default: Kopiervorlage für neue Profile
 - Öffentlich: Startmenü- und Desktoplink für alle Benutzer
 - <Benutzername>: Dateien des Benutzers (u.a. NTUSER.DAT)
- Erweiterte Profiltypen
 - Roaming Profile (abgekündigt)
 - Mandatory Profile (Veränderungen werden nicht gespeichert)

Richtlinien für die Benutzerkonten

- Gemeinsame Eigenschaften für Benutzerkonten
- Lokale Sicherheitsrichtlinien (secpol.msc)
 - Maximales Kennwortalter
 - Kennwortchronik erzwingen
 - Minimales Kennwortalter
 - Minimale Kennwortlänge
 - Kennwort muss Komplexitätsvoraussetzungen entsprechen
 - Kontosperrungsschwelle
 - › Kontosperrdauer
 - › Zurücksetzdauer des Kontosperrzählers



REGISTRY



Registry – Speicherung der Konfigurationen

- Zentraler Speicherort für Konfigurationen
 - Benutzereinstellungen
 - Anwendungseinstellungen
 - Hardwareprofile
 - Information zum Ablauf der interaktiven Anmeldung
 - Treiberinformationen
 - Informationen zu den Partitionen des Datenträgers
 - usw.

Darstellung der Registry

- Besteht aus mehreren Dateien (Hives)
- Hierarchischer Aufbau
 - Hauptschlüssel
 - Schlüssel und Unterschlüssel
 - Teilbäume
 - Schlüsseleinträge
 - Werte
- Darstellung Registry-Pfad
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\...

Die Gliederung der Registry (1)

- HKEY_LOCAL_MACHINE
 - Konfigurationsinformationen des OS und seiner Module
 - Bsp. Gerätetreiber, Partitionierung, Benutzerdatenbank, etc.
- HKEY_USERS
 - Benutzerspezifischen Einstellungen
 - Bsp. Abweichungen der Standardeinstellungen von Software
 - Unterschiedliche BT werden über SID des Benutzer repräsentiert

Die Gliederung der Registry (2)

- HKEY_CLASSES_ROOT
 - Zuordnung der Dateitypen zu Anwendungen
 - Speicherung von sog. Objekt-ID zur Identifizierung
 - Verzweigter HKEY (HKEY_LOCAL_MACHINE\Software\Classes
- HKEY_CURRENT_USER
 - Benutzerspezifische Einstellungen des aktuellen Benutzers
 - Benutzerteilbaum (BT) aus HKEY_USERS wird geladen

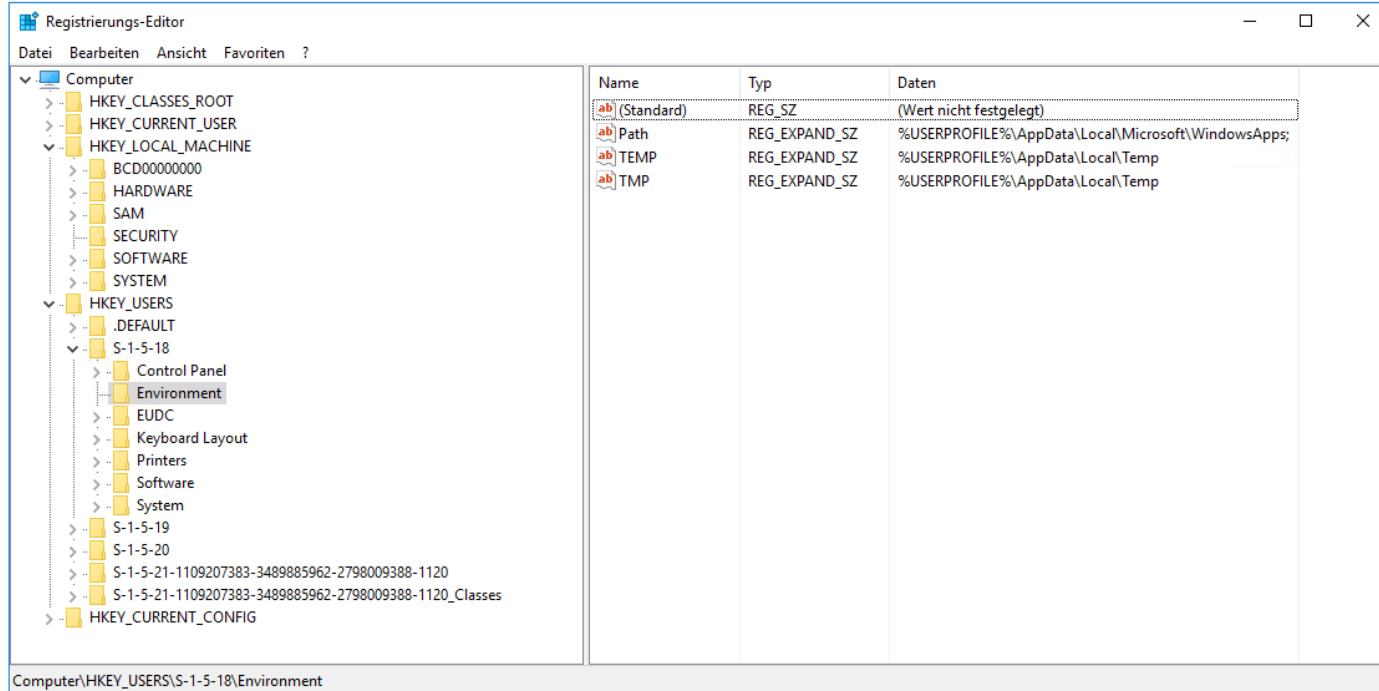
Die Gliederung der Registry (3)

- HKEY_CURRENT_CONFIG
 - Einstellungen des aktuellen Hardwareprofils
 - Verzweigter HKEY (HKEY_LOCAL_MACHINE\SYSTEM\Current Control Set\Hardware-Profiles\Current)

Registry-Editor

- Betrachtung und Bearbeitung „REGEDIT.EXE“
- Suche nach Schlüsseln, Einträgen und Werten
- Exportieren als TXT-, ASCII-, und Reg-File
- Importieren
- Inaktive Hives bearbeiten

REGEDIT.EXE



Registry-Dateien

- Maschinenbezogene Hives
 - %windir%\system32\config
 - SAM, Security, Software, System und Default
 - Einbinden beim Systemstart
- Benutzerbezogener Hive
 - C:\Users\<Benutzername>
 - NTUSER.DAT
 - Einbinden bei der Anmeldung



GRUPPENRICHTLINIEN-OBJEKTE (GPOs)



FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

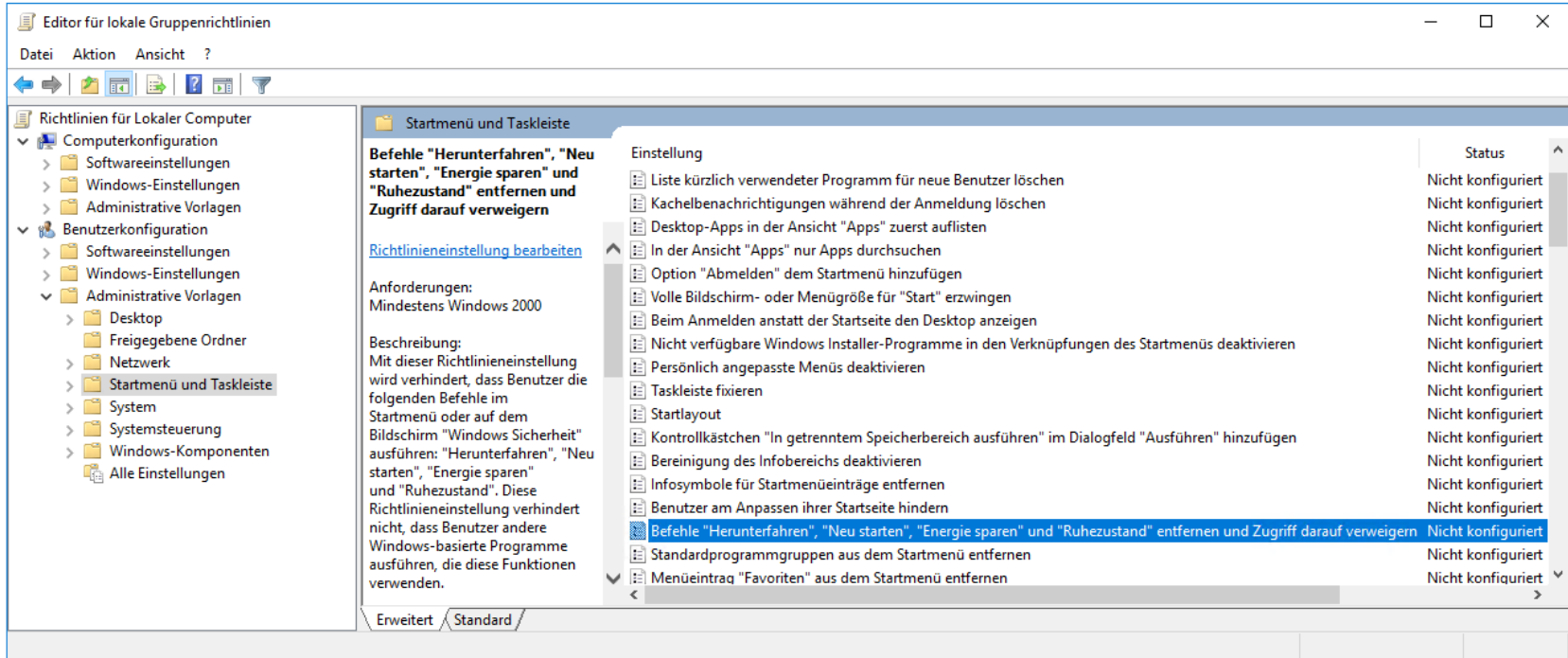
Gruppenrichtlinien (1)

- Vorkonfiguration von Anwendungen / Betriebssystem
- Lokal verwaltete und über das AD verwaltete GPOs
- Einträge in die Registry
- Gpupdate.exe / Gpresult.exe

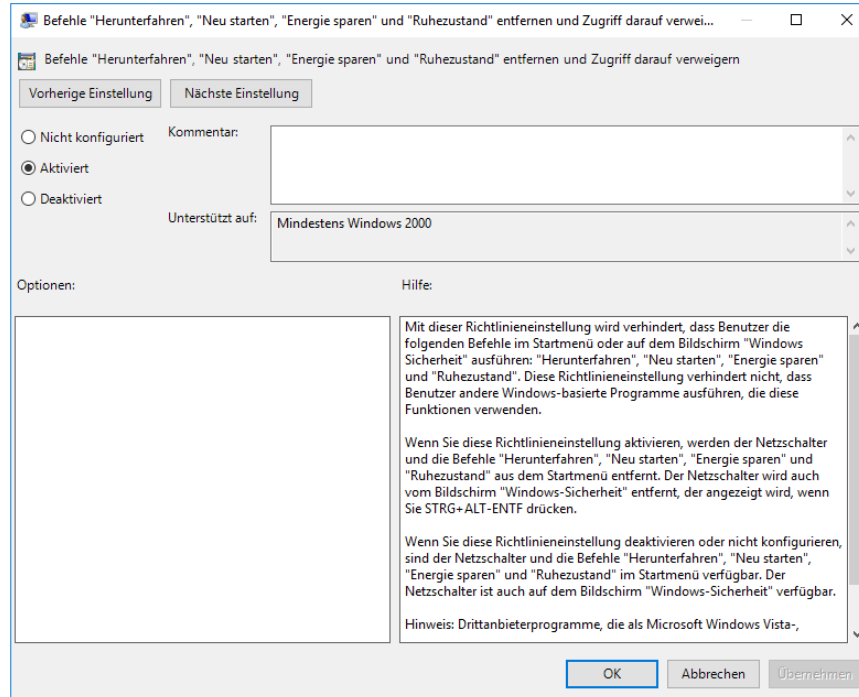
Gruppenrichtlinien (2)

- Computerkonfiguration
 - Einstellungen die den Rechner betreffen
- Benutzerkonfiguration
 - Einstellungen die den Benutzer betreffen
- Administrative Vorlagen
 - Vorlagen für bestimmte Regeln
 - Erweiterbar

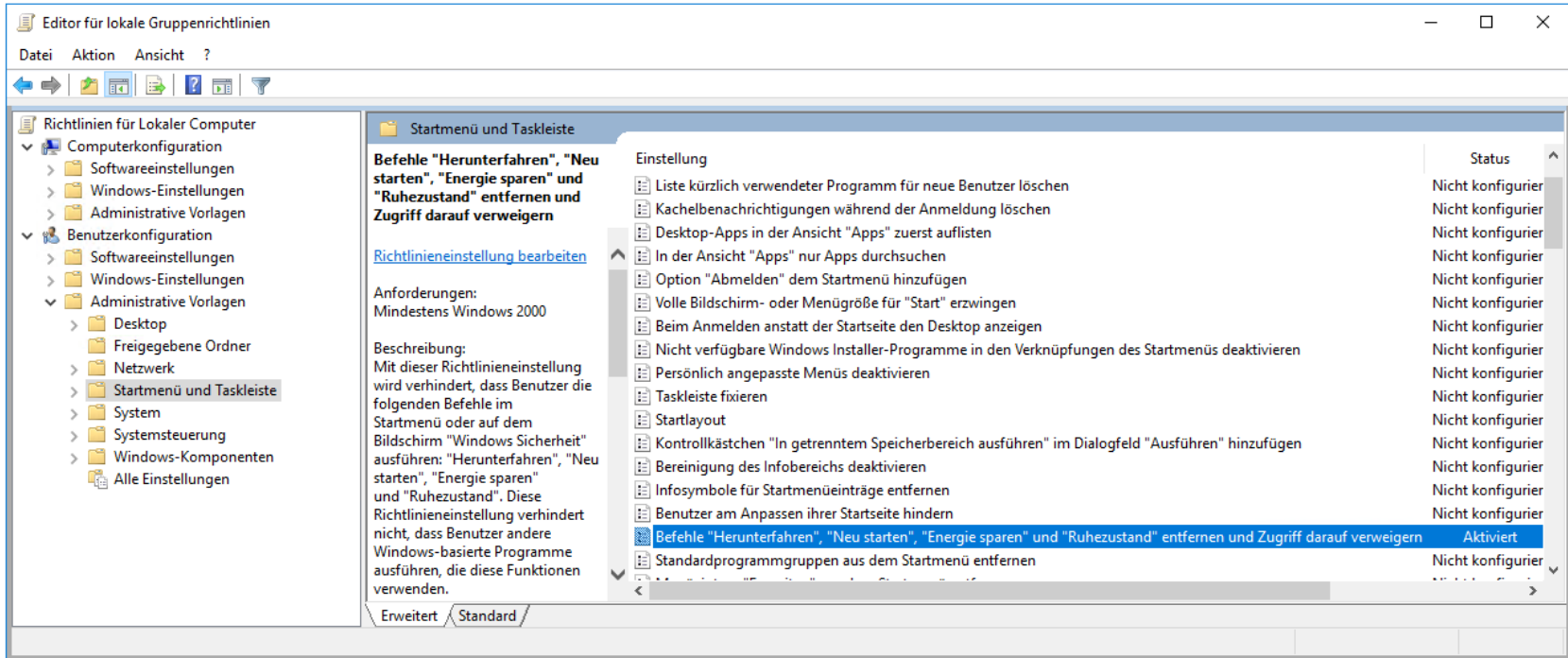
Editor für lokale Gruppenrichtlinien (1)



Editor für lokale Gruppenrichtlinien (2)



Editor für lokale Gruppenrichtlinien (3)





WINDOWS-UPDATEBEZUG



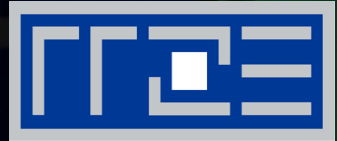
Windows-Updatebezug

- Windows-Updates dienen zum
 - Schließen von Sicherheitslücken
 - Beheben von Fehlern
 - Erweiterung von Funktionen
- Bezugsarten
 - Betrieb eines „Windows Server Update Service“ (WSUS)
 - › Zentrale Bereitstellung von Windowsupdates im eigenen Netzwerk
 - › Flexible Veröffentlichung und Bereitstellung
 - Direkter Bezug von Microsoft

Windows-Updatebezug am RRZE

- Betrieb eines „Windows Server Update Service“ (WSUS)
- FAU-Current 0, 1, 2 (keine Unterscheidung des OS)
- FAU-Next 0,1, 2 (nur Windows 10)
- Weitere Fragen beantworten die Folien des Campustreffens
<https://www.video.uni-erlangen.de/clip/id/6956.html>

WINDOWS-FIREWALL



FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

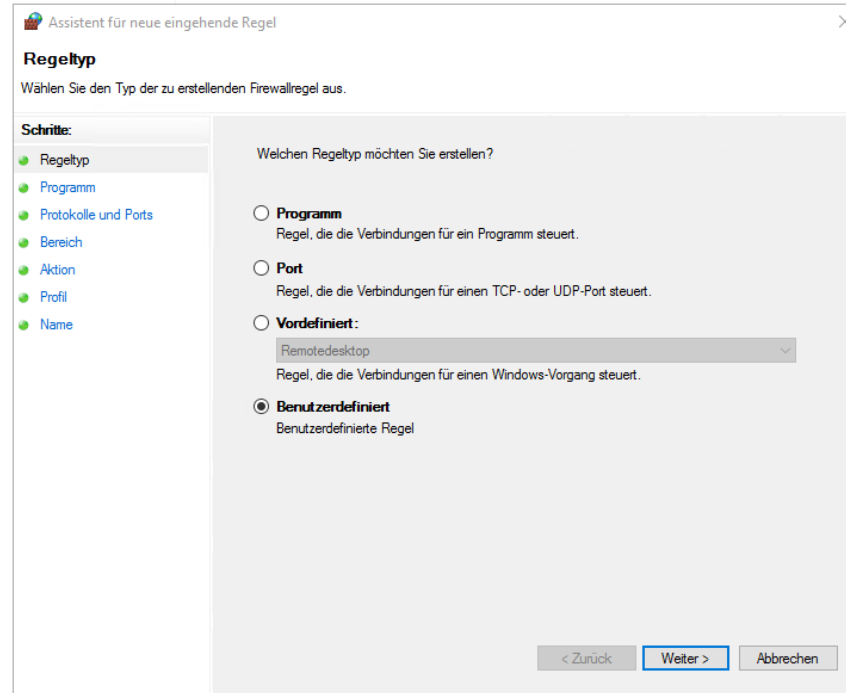
Windows-Firewall (1)

- Systemsteuerung / MMC-Snap-In (wf.msc)
- Firewall != Antivirus-Software
- Reglementierung auf Netzworkebasis möglich
- Ein- und ausgehende Regeln
- Profile der Windows-Firewall
 - Domäne
 - Privat
 - Öffentlich

Windows-Firewall (2)

- Standardverhalten für ein- und ausgehende Verbindungen
- Protokollierung
- Regeltypen
 - Programm
 - Port (UDP/TCP)
 - Vordefiniert (z.B. iSCSI-Dienste, Remotedesktopdienste, usw.)
 - Benutzerdefiniert

Windows-Firewall – Regeltyp



Windows-Firewall – Programm

Assistent für neue eingehende Regel

Programm

Geben Sie den vollständigen Programmpfad und den Namen der ausführbaren Datei des Programms an, dem diese Regel entspricht.

Schritte:

- Regeltyp
- Programm**
- Protokolle und Ports
- Bereich
- Aktion
- Profil
- Name

Betrifft diese Regel alle oder nur ein bestimmtes Programm?

☒ **Alle Programme**
Die Regel wird auf alle Computerverbindungen angewendet, die mit anderen Regeleigenschaften übereinstimmen.

☐ **Dieser Programmpfad:**

Beispiel: c:\Pfad\Programm.exe
%ProgramFiles%\Browser\Browser.exe

Dienste

Legen Sie die Dienste fest, die diese Regel betrifft.

< Zurück Weiter > Abbrechen

Windows-Firewall – Protokolle und Ports

Assistent für neue eingehende Regel

Protokolle und Ports

Geben Sie die Protokolle und Ports an, für die diese Regel gilt.

Schritte:

- Regeltyp
- Programm
- Protokolle und Ports**
- Bereich
- Aktion
- Profil
- Name

Für welche Ports und Protokolle gilt diese Regel?

Protokolltyp: TCP

Protokollnummer: 6

Lokaler Port: Bestimmte Ports

80

Beispiel: 80, 443, 5000-5010

Remoteport: Alle Ports

Beispiel: 80, 443, 5000-5010

ICMP-Einstellungen: Anpassen...

< Zurück Weiter > Abbrechen

Windows-Firewall – Bereich

Assistent für neue eingehende Regel

Bereich

Geben Sie die lokalen IP-Adressen und die Remote-IP-Adressen an, auf die diese Regel angewendet wird.

Schritte:

- Regeltyp
- Programm
- Protokolle und Ports
- Bereich**
- Aktion
- Profil
- Name

Für welche lokalen IP-Adressen gilt diese Regel?

☒ Beliebige IP-Adresse

☐ Diese IP-Adressen:

Hinzufügen...
Bearbeiten...
Entfernen

Passen Sie Schnittstellentypen an, für die die Regel angewendet wird:

Für welche Remote-IP-Adressen gilt diese Regel?

☐ Beliebige IP-Adresse

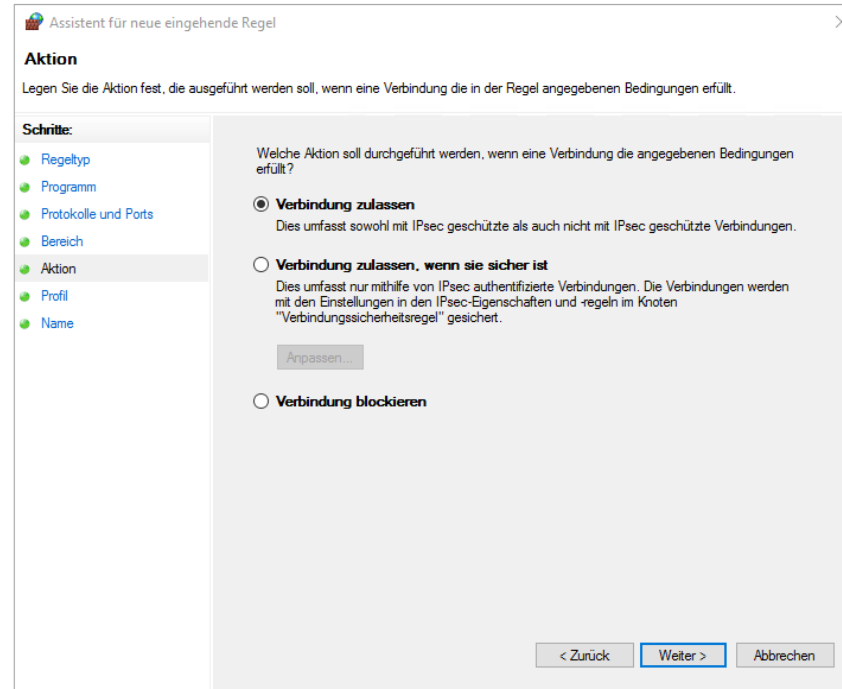
☒ Diese IP-Adressen:

192.168.1.10
10.10.10.0/24

Hinzufügen...
Bearbeiten...
Entfernen

< Zurück Weiter > Abbrechen

Windows-Firewall – Aktion



Windows-Firewall – Profil

Assistent für neue eingehende Regel

Profil

Geben Sie die Profile an, für die diese Regel zutrifft.

Schritte:

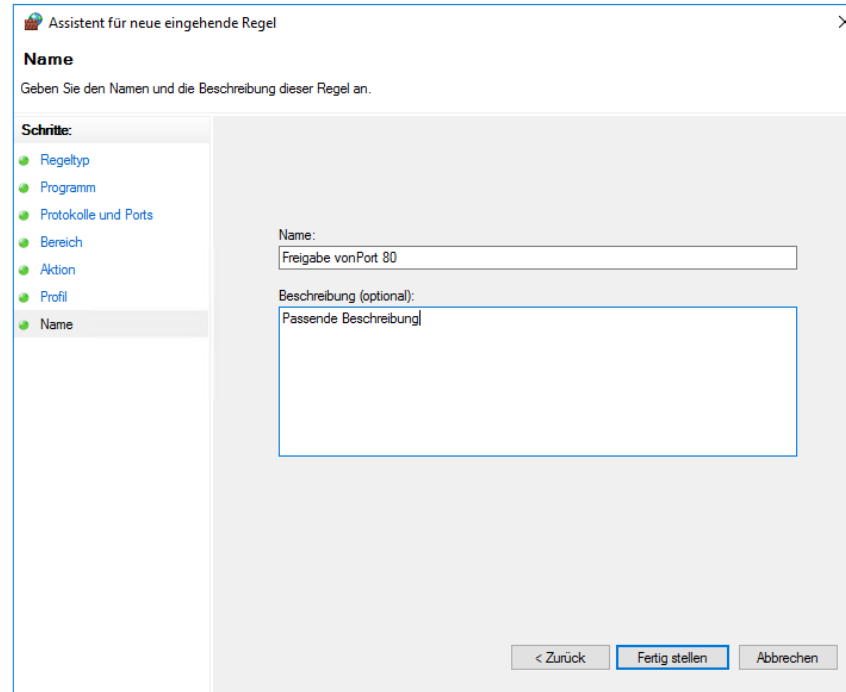
- Regeltyp
- Programm
- Protokolle und Ports
- Bereich
- Aktion
- Profil**
- Name

Wann wird diese Regel angewendet?

- ☒ **Domäne**
Wird angewendet, wenn ein Computer mit der Firmendomäne verbunden ist.
- ☒ **Privat**
Wird angewendet, wenn ein Computer mit einem privaten Netzwerk (z.B. zu Hause oder am Arbeitsplatz) verbunden ist.
- ☒ **Öffentlich**
Wird angewendet, wenn ein Computer mit einem öffentlichen Netzwerk verbunden ist.

< Zurück Weiter > Abbrechen

Windows-Firewall – Name



Assistent für neue eingehende Regel

Name

Geben Sie den Namen und die Beschreibung dieser Regel an.

Schritte:

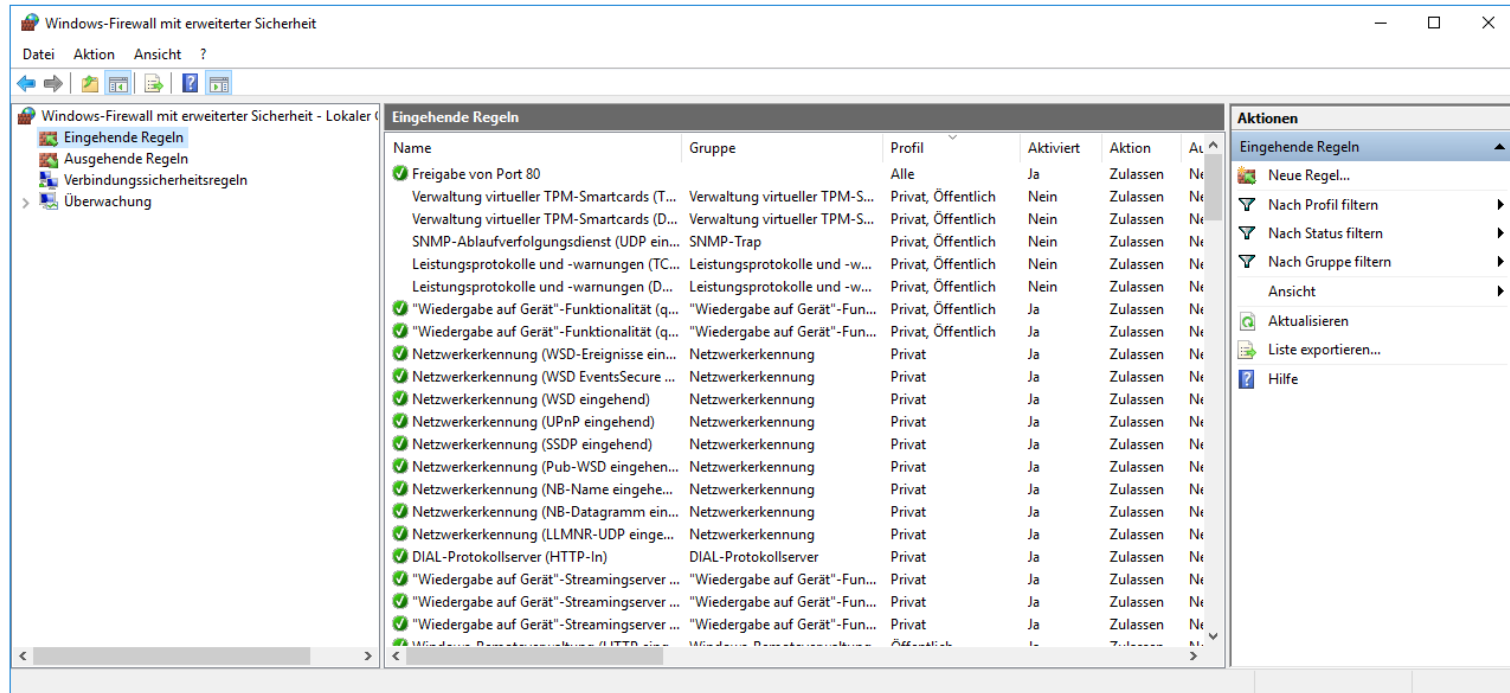
- Regeltyp
- Programm
- Protokolle und Ports
- Bereich
- Aktion
- Profil
- Name**

Name:
Freigabe von Port 80

Beschreibung (optional):
Passende Beschreibung

< Zurück Fertig stellen Abbrechen

Windows-Firewall erstellte Regel





WINDOWS-AUFGABENPLANUNG

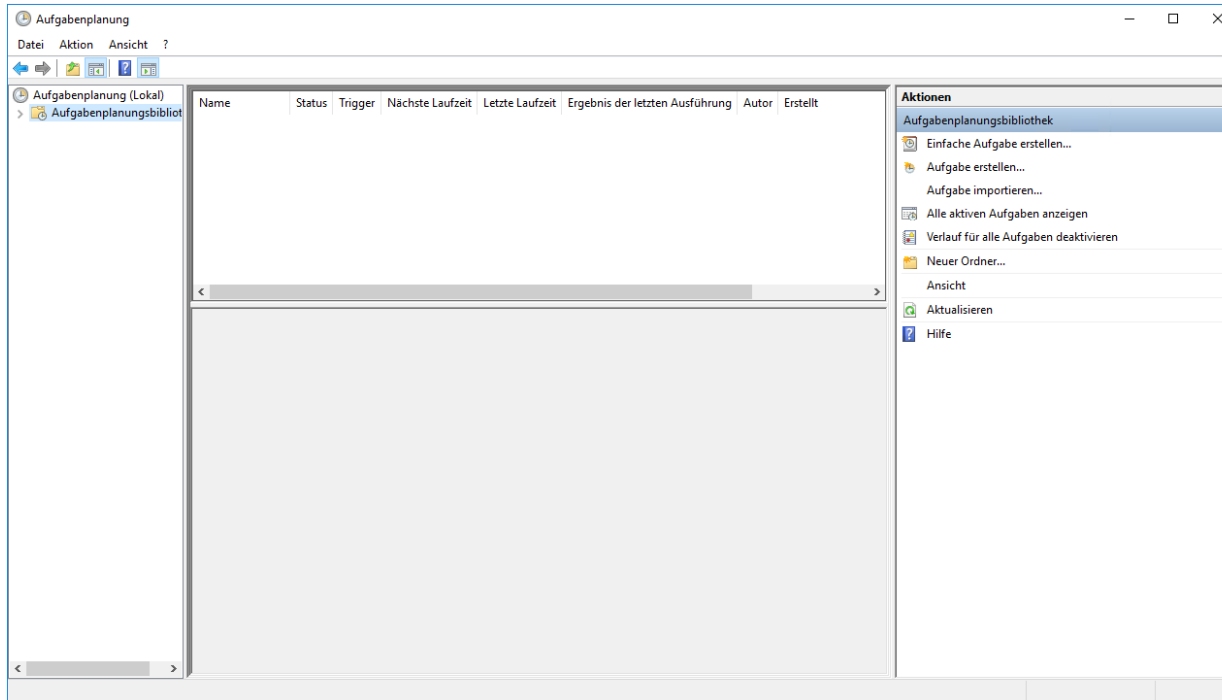


FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Windows-Aufgabenplanung

- Aufgabenplanungs-Editor (taskschd.msc)
- Terminierte Aufgaben erstellen
- Aufgabe exportieren und importieren
- Verbindung mit einem anderen Computer herstellen

Windows-Aufgabenplanung



Aufgabe erstellen – Allgemein

The screenshot shows the 'Aufgabe erstellen' (Create Task) dialog box in Windows Task Scheduler. The 'Allgemein' (General) tab is selected. The 'Name' field contains 'Test-Aufgabe'. The 'Speicherort' (Location) field is empty. The 'Autor' (Author) field contains 'TESTAD\adszenger'. The 'Beschreibung' (Description) field is empty. Under 'Sicherheitsoptionen' (Security options), the text 'Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden:' (When running the task, use the following user account:) is followed by 'NT-AUTORITÄT\SYSTEM'. A button 'Benutzer oder Gruppe ändern...' (Change user or group...) is next to it. Below this, there are three radio buttons: 'Nur ausführen, wenn der Benutzer angemeldet ist' (Run only when the user is logged on), 'Unabhängig von der Benutzeranmeldung ausführen' (Run regardless of the user's login state), and 'Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu.' (Do not save password. The task can only use local computer resources.). There are also two checkboxes: 'Mit höchsten Privilegien ausführen' (Run with highest privileges) and 'Ausgeblendet' (Hidden). At the bottom, there is a dropdown menu 'Konfigurieren für:' (Configure for:) set to 'Windows Server 2016'. The 'OK' and 'Abbrechen' (Cancel) buttons are at the bottom right.

Aufgabe erstellen

Allgemein | Trigger | Aktionen | Bedingungen | Einstellungen

Name: Test-Aufgabe

Speicherort: \

Autor: TESTAD\adszenger

Beschreibung:

Sicherheitsoptionen

Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden:

NT-AUTORITÄT\SYSTEM [Benutzer oder Gruppe ändern...](#)

☒ Nur ausführen, wenn der Benutzer angemeldet ist

☐ Unabhängig von der Benutzeranmeldung ausführen

☐ Kennwort nicht speichern. Die Aufgabe greift nur auf lokale Computerressourcen zu.

☐ Mit höchsten Privilegien ausführen

☐ Ausgeblendet Konfigurieren für: Windows Server 2016

OK Abbrechen

Aufgabe erstellen – Trigger

Neuer Trigger

Aufgabe starten: Nach einem Zeitplan

Einstellungen

☐ Einmal
☐ Täglich
☐ Wöchentlich
☒ Monatlich

Start: 25.04.2017 14:15:37 ☐ Zeitzoneübergreifende Synch.

Monate: Januar, Februar, März, April...

☐ Tage:

☒ Am: Letzter Dienstag

Erweiterte Einstellungen

☐ Aufgabe verzögern für maximal: 1 Stunde

☐ Wiederholen jede: 1 Stunde für die Dauer von: 1 Tag

☐ Alle ausgeführten Aufgaben am Ende der Wiederholungsdauer beenden

☐ Aufgabe beenden nach: 3 Tage

☐ Ablaufen: 25.04.2018 14:15:43 ☐ Zeitzoneübergreifende Synch.

☒ Aktiviert

OK Abbrechen

Aufgabe erstellen – Aktion

Neue Aktion

Geben Sie die Aktion an, die von der Aufgabe ausgeführt werden soll.

Aktion: Programm starten

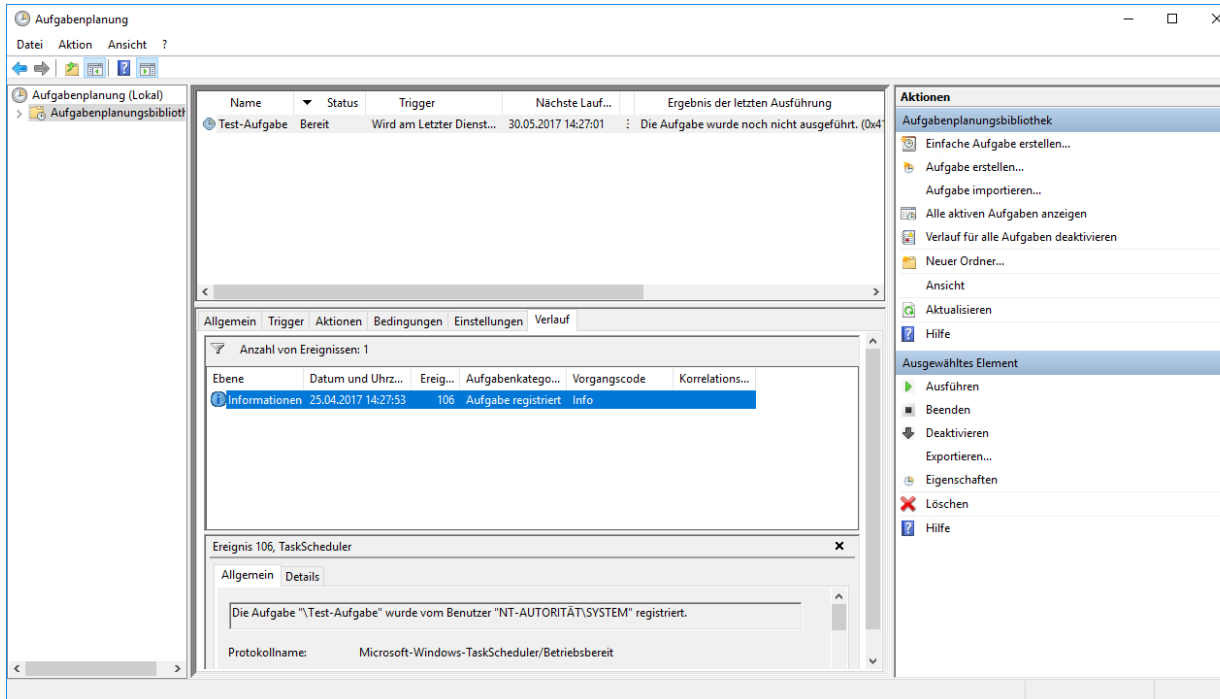
Einstellungen

Programm/Skript:
ows\System32\WindowsPowerShell\v1.0\powershell.exe

Argumente hinzufügen (optional):

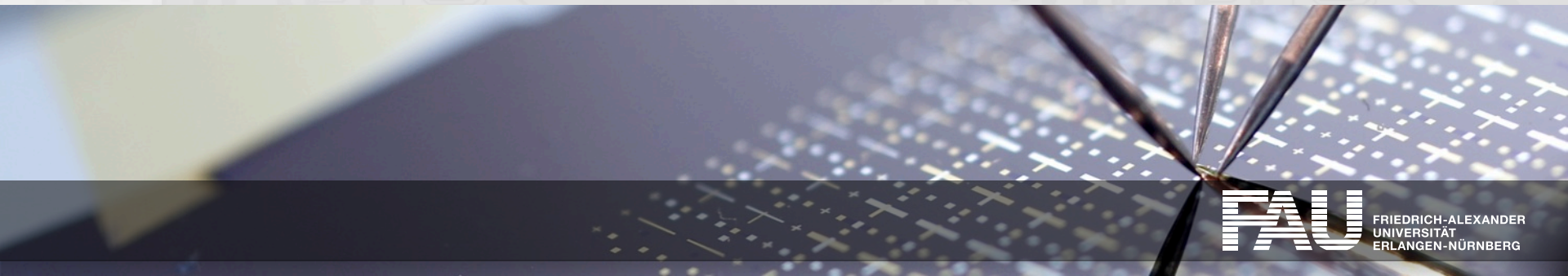
Starten in (optional):

Aufgabe erstellt





EREIGNISANZEIGE



Ereignisanzeige (Event Viewer)

- „eventvwr.msc“
- Ereignisebenen
 - Fehler, Information und Warnung
- Windows-Protokolle
 - Anwendungen, Sicherheit, Installation und System
 - Weitergeleitete Ereignisse
- Benutzerdefinierte Ansichten

eventvwr.msc

The screenshot shows the Windows Event Viewer window titled 'Ereignisanzeige'. The left pane shows the tree view with 'Ereignisanzeige (Lokal)' expanded, and 'Installation' selected under 'Windows-Protokolle'. The main pane displays a list of events under the 'Installation' category, with 58 events in total. The selected event is a 'Warning' (Warnung) with ID 4, titled 'Ereignis 4, WUSA'. The details pane shows the event description: 'Das Windows-Update Update für Windows (KB4010672) erfordert einen Neustart des Computers, um die Installation abzuschließen. (Befehlszeile: ""C:\Windows\system32\wusa.exe" "C:\Users\... Desktop \windows10.0-kb4010672-x64_(Server1703).msu")'. Below the description, the event properties are listed: Protokollname: Installation, Quelle: WUSA, Ereignis-ID: 4, Ebene: Warnung, Benutzer: ..., Vorgangscode: Info, and Weitere Informationen: [Onlinehilfe](#). The right pane shows the 'Aktionen' (Actions) menu with options like 'Gespeicherte Protokolldatei öffnen...', 'Benutzerdefinierte Ansicht erstellen...', and 'Ereigniseigenschaften'.

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkate...
Informationen	11.05.2017 15:06:46	Servicing	1 (1)	
Informationen	11.05.2017 15:06:21	Servicing	1 (1)	
Informationen	11.05.2017 15:03:15	Servicing	2 (1)	
Informationen	11.05.2017 14:44:56	Servicing	4 (1)	
Informationen	11.05.2017 14:37:34	WUSA	2 Keine	
Warnung	11.05.2017 14:37:34	WUSA	4 Keine	
Informationen	11.05.2017 13:34:24	Servicing	1 (1)	
Informationen	03.05.2017 08:23:37	Servicing	3 (1)	
Informationen	03.05.2017 07:49:26	Servicing	1 (1)	

Ereignis 4, WUSA

Allgemein Details

Das Windows-Update Update für Windows (KB4010672) erfordert einen Neustart des Computers, um die Installation abzuschließen. (Befehlszeile: ""C:\Windows\system32\wusa.exe" "C:\Users\... Desktop \windows10.0-kb4010672-x64_(Server1703).msu")

Protokollname: Installation
Quelle: WUSA
Ereignis-ID: 4
Ebene: Warnung
Benutzer: ...
Vorgangscode: Info
Weitere Informationen: [Onlinehilfe](#)

Protokolliert: 11.05.2017 14:37:34
Aufgabenkategorie: Keine
Schlüsselwörter: ...
Computer: ...



TERMINALSERVER (REMOTE DESKTOP SERVICES)



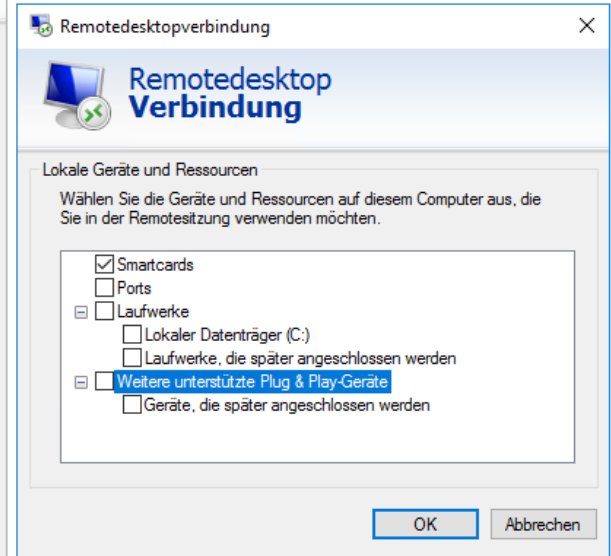
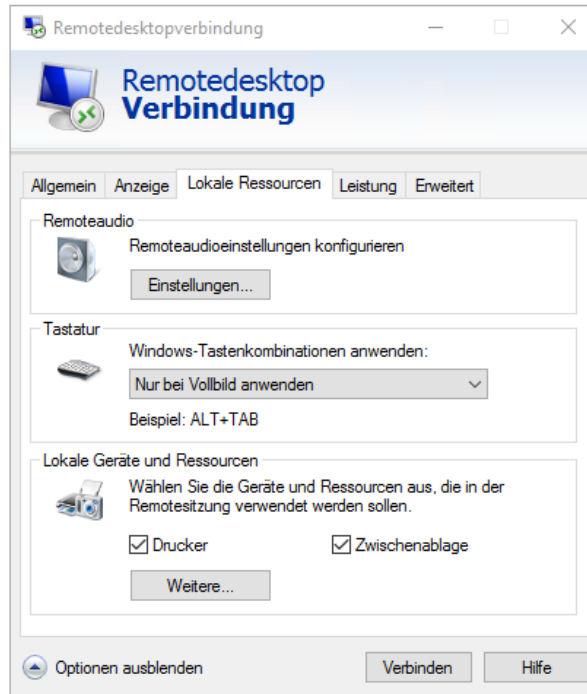
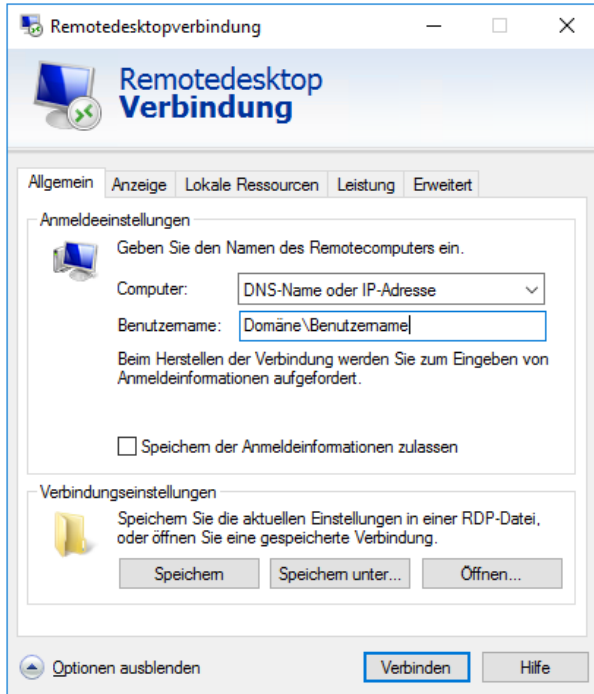
Terminalserver (Remote Desktop Services)

- Zentralbetriebener Windows-Server mit installierten RDS
 - Zentrale Bereitstellung und Administration
 - Keine Begrenzung von zeitgleichen Benutzersitzungen
- Dimensionierung je nach Benutzeranzahl
- Sitzungsbasiert, RemoteApps und VDI
- Lizenzierung
 - RDS User CALs
 - RDS Device CALs

Remoteverbindung mit Windows-Systemen

- RDP (Remote Desktop Protocol)
- Zielseitige Einrichtung der RDP-Kommunikation
- RDP-Client
 - Einbinden von lokalen Ressourcen
 - „.rdp-Dateien“

RDP-Client





ORGANISATORISCHES



- Die Vorträge im Überblick
- Andere Vortragsreihen des RRZE
- Ablageorte Vortragsfolien
- RRZE-Veranstaltungskalender / Mailingliste abonnieren
- Themenvorschläge & Anregungen

Weitere Vorträge zur „Systemausbildung“

26.04.2017 – Geschichte der Betriebssysteme

03.05.2017 – Unixoiden Betriebssysteme (Unix, Linux, OS X)

10.05.2017 – Systemüberwachung / Monitoring

17.05.2017 – Storage & Filesysteme

31.05.2017 – Windows-Betriebssysteme

21.06.2017 – High Performance Computing

28.06.2017 – Benutzerverwaltung: MS Active Directory

05.07.2017 – Virtualisierung

12.07.2017 – Backup / Archiv

19.07.2017 – Kerberos

26.07.2017 – IT-Sicherheit

- Immer mittwochs (ab 14 c.t.),
- Raum 2.049 im RRZE

Andere Vortragsreihen des RRZE

Campustreffen

- immer donnerstags ab 15 Uhr c.t.
- vermittelt Informationen zu den Dienstleistungen des RRZE
- befasst sich mit neuer Hard- & Software, Update-Verfahren sowie Lizenzfragen
- ermöglicht den Erfahrungsaustausch mit Spezialisten

Netzwerkausbildung „Praxis der Datenkommunikation“

- immer mittwochs in den Wintersemestern, ab 14 Uhr c.t.
- Vorlesungsreihe, die in die Grundlagen der Netztechnik einführt
- stellt die zahlreichen aktuellen Entwicklungen auf dem Gebiet der (universitären) Kommunikationssysteme dar

Vortragsfolien

Die Vortragsfolien werden nach der Veranstaltung auf der Webseite des RRZE abgelegt:

<http://www.rrze.fau.de/news/systemausbildung.shtml>

RRZE-Veranstaltungskalender & Mailinglisten

- Kalender abonnieren oder bookmarken
 - Alle Infos hierzu stehen auf der Webseite des RRZE unter:
<http://www.rrze.fau.de/news/kalender.shtml>
- Mailingliste abonnieren
 - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste [RRZE-Aktuelles](#) gesendet.
 - Auch diese Liste kann man abonnieren:
<https://lists.fau.de/mailman/listinfo/rrze-aktuelles>

Themenvorschläge & Anregungen

Themenvorschläge und Anregungen nehmen wir gerne entgegen!

Bitte schreiben Sie uns einfach eine E-Mail an:
rrze-zentrale@fau.de (Betreff: Systemausbildung)

REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Vielen Dank für Ihre Aufmerksamkeit!

Regionales RechenZentrum Erlangen [RRZE]

Martensstraße 1, 91058 Erlangen

<http://www.rrze.fau.de>