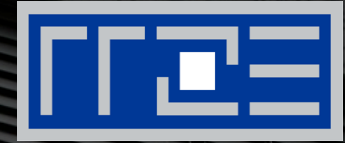


REGIONALES RECHENZENTRUM ERLANGEN [RRZE]



Windows-Betriebssysteme

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

Andrea Kugler, Sonja Schmidt, RRZE, 13.05.2020

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 2019 / Windows 10 18xx
 - Windows Server 2016 / Windows 10 16xx
 - Windows Server 2012R2 / Windows 8.1

Windows Versionsverlauf

Extended Support Windows Server-Generationen

- Windows Server 2008 R2 (01/2020)
- Windows Server 2012 R2 (10/2023)
- Windows Server 2016 (01/2027)
- Windows Server 2019 (01/2029)

Windows Versionsverlauf

Extended Support Windows Client-Generationen

- Windows 7 (01/2020)
- Windows 8.1 (01/2023)
- Windows 10 1709 (04/2020)
- Windows 10 1803 (11/2020)
- Windows 10 1809 (05/2021)
- Windows 10 1903 (12/2020)
- Windows 10 1909 (05/2022)

<https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet>



DIE BENUTZERVERWALTUNG



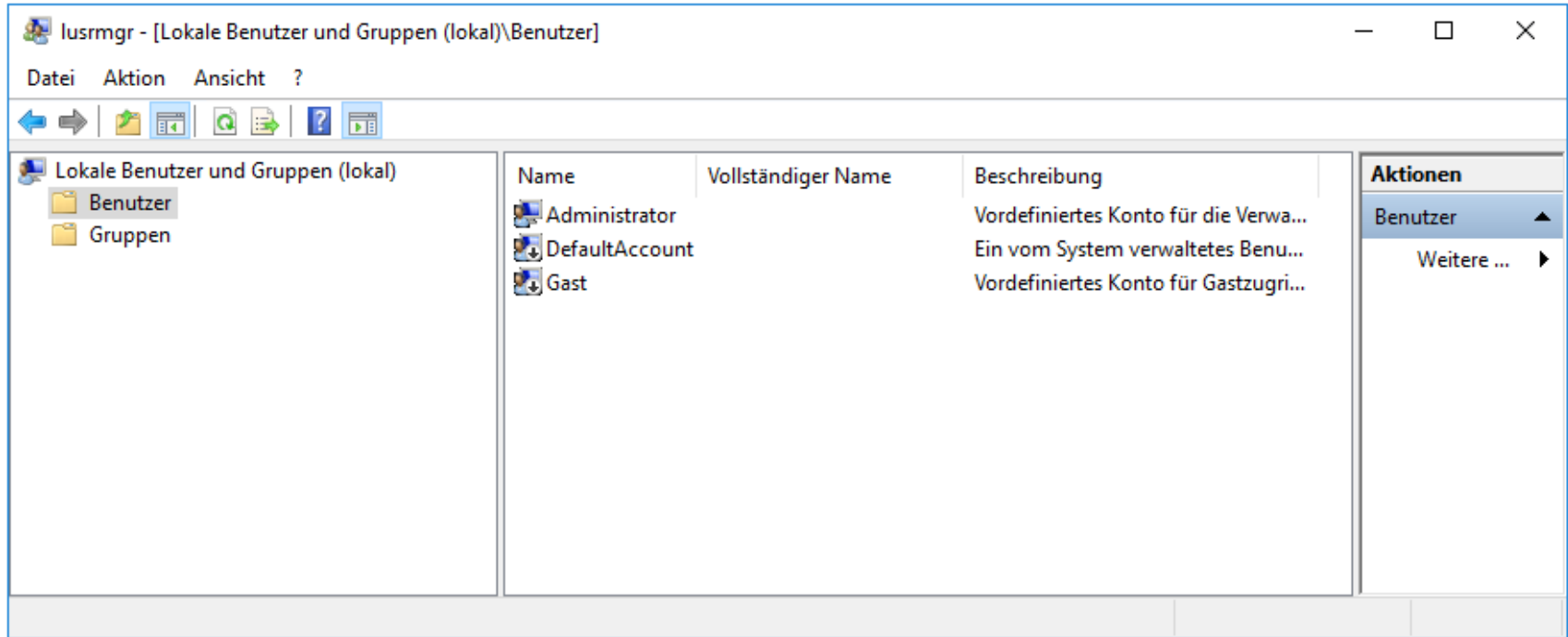
Einführung Benutzerverwaltung

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

Lokale 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

Sicherheitsrichtlinien für Benutzerkonten

Lokaler Sicherheitsrichtlinien Editor (secpol.msc)

Gemeinsame Einstellungen für alle













- Maximales Kennwortalter
- Kennwortchronik erzwingen
- Minimales Kennwortalter
- Minimale Kennwortlänge
- Kennwort muss Komplexitätsvoraussetzungen entsprechen
- Kontosperrungsschwelle
 - › Kontosperrdauer
 - › Zurücksetzdauer des Kontosperrzählers







Gruppenmitgliedschaften

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

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)

 Administratoren	Administratoren haben uneingeschränkten Vo
 Benutzer	Benutzer können keine zufälligen oder beabsic
 Distributed COM-Ben...	Mitglieder dieser Gruppe können Distributed-C
 Druck-Operatoren	Mitglieder können auf Domänencontrollern im
 Ereignisprotokollleser	Mitglieder dieser Gruppe dürfen Ereignisproto
 Gäste	Gäste besitzen standardmäßig die selben Zugr
 Hauptbenutzer	"Hauptbenutzer" sind eingeschlossen aus Grün
 Hyper-V-Administrat...	Die Mitglieder dieser Gruppe erhalten uneinge
 IIS_IUSRS	Von Internetinformationsdiensten verwendete
 Kryptografie-Operator...	Die Mitglieder sind berechtigt, kryptographisc
 Leistungsprotokollbe...	Mitglieder dieser Gruppe können die Protokoll
 Leistungsüberwachun	Mitglieder dieser Gruppe können lokal und re

 Netzwerkkonfiguratio...	Mitglieder dieser Gruppe verfügen über einige Adminis
 RDS-Endpunktserver	Auf den Servern dieser Gruppe werden virtuelle Compu
 RDS-Remotezugriffsse...	Die Server dieser Gruppe bieten Benutzern von Remote
 RDS-Verwaltungsserver	Auf den Servern dieser Gruppe werden administrative F
 Remotedesktopbenut...	Mitglieder dieser Gruppe haben die Berechtigung, sich
 Remoteverwaltungs...	Mitglieder dieser Gruppe können über Verwaltungspro
 Replikations-Operator	Unterstützt Dateireplikation in Domänen.
 Sicherungs-Operatoren	Sicherungs-Operatoren können Sicherheitseinschränku
 Storage Repl. Admin	Die Mitglieder dieser Gruppe haben vollständigen und
 System Managed Acc...	Die Mitglieder dieser Gruppe werden vom System verw
 Zertifikatdienst-DCO...	Mitglieder dieser Gruppe sind berechtigt, eine Verbindu
 Zugriffssteuerungs-U...	Mitglieder dieser Gruppe können remote Autorisierung
 Test Gruppe	Diese Gruppe dient Testzwecken



REGISTRY



Registry – Speicherung der Konfigurationen

Zentraler Speicherort für Konfigurationen

- Benutzereinstellungen
- Anwendungseinstellungen
- Hardwareprofil
- 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
 - Bootinfo, Benutzerdatenbank, Softwareeinstellungen, etc.
- HKEY_USERS
 - Benutzerspezifischen Einstellungen
 - Abweichungen der Standardeinstellungen von Software, etc.
 - Ein Teilbaum pro Benutzer, Schlüssel ist SID des Benutzers

Die Gliederung der Registry (2)

- HKEY_CLASSES_ROOT
 - Zuordnung der Dateitypen zu Anwendungen
 - Speicherung von sog. Objekt-ID zur Identifizierung
 - Zeigt auf HKEY_LOCAL_MACHINE\Software\Classes
- HKEY_CURRENT_USER
 - Benutzerspezifische Einstellungen des aktuellen Benutzers
 - Zeigt auf HKEY_USERS\S-1-5-21-...

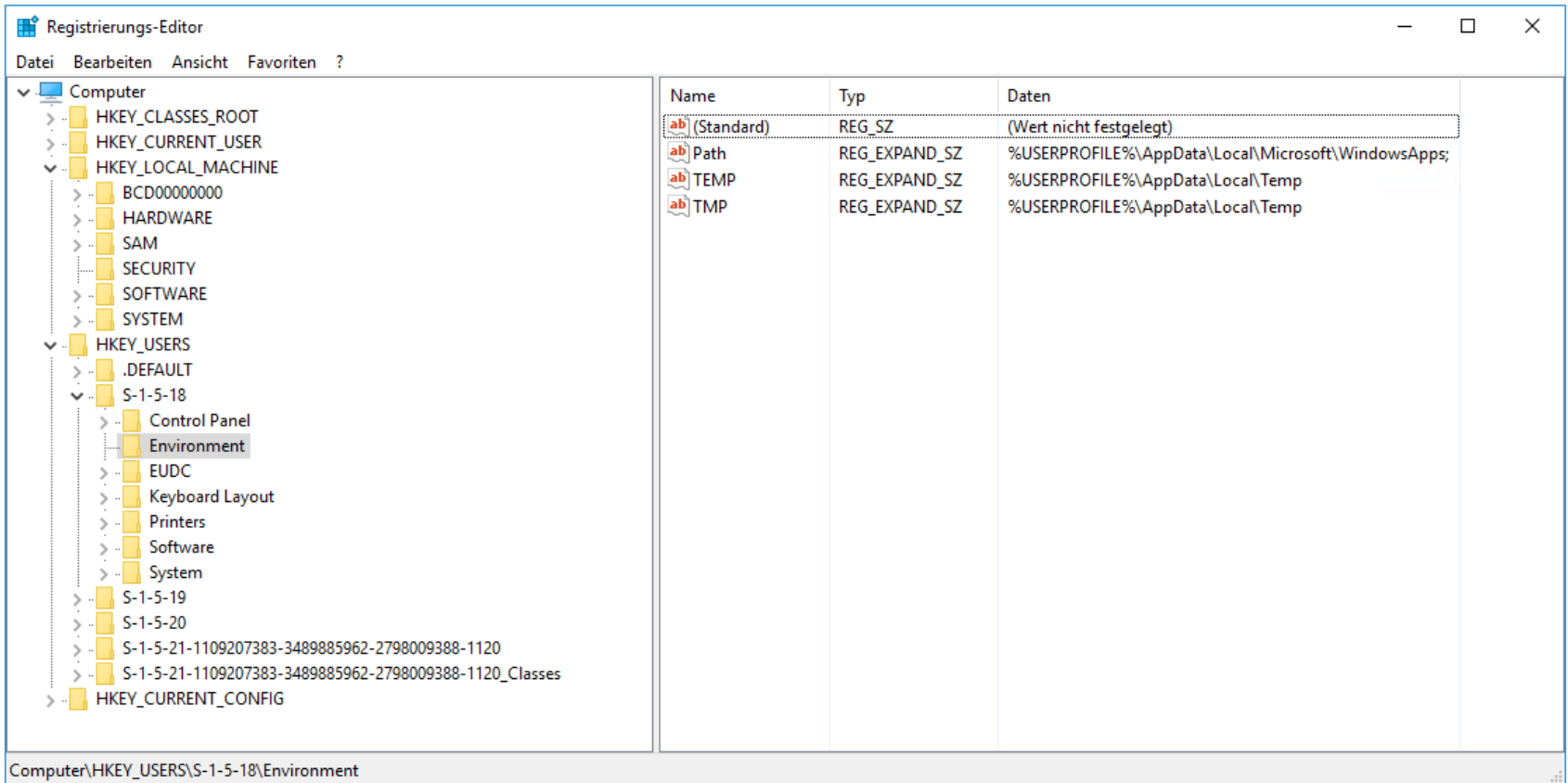
Die Gliederung der Registry (3)

- HKEY_CURRENT_CONFIG
 - Einstellungen des aktuellen Hardwareprofils
 - Zeigt auf 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

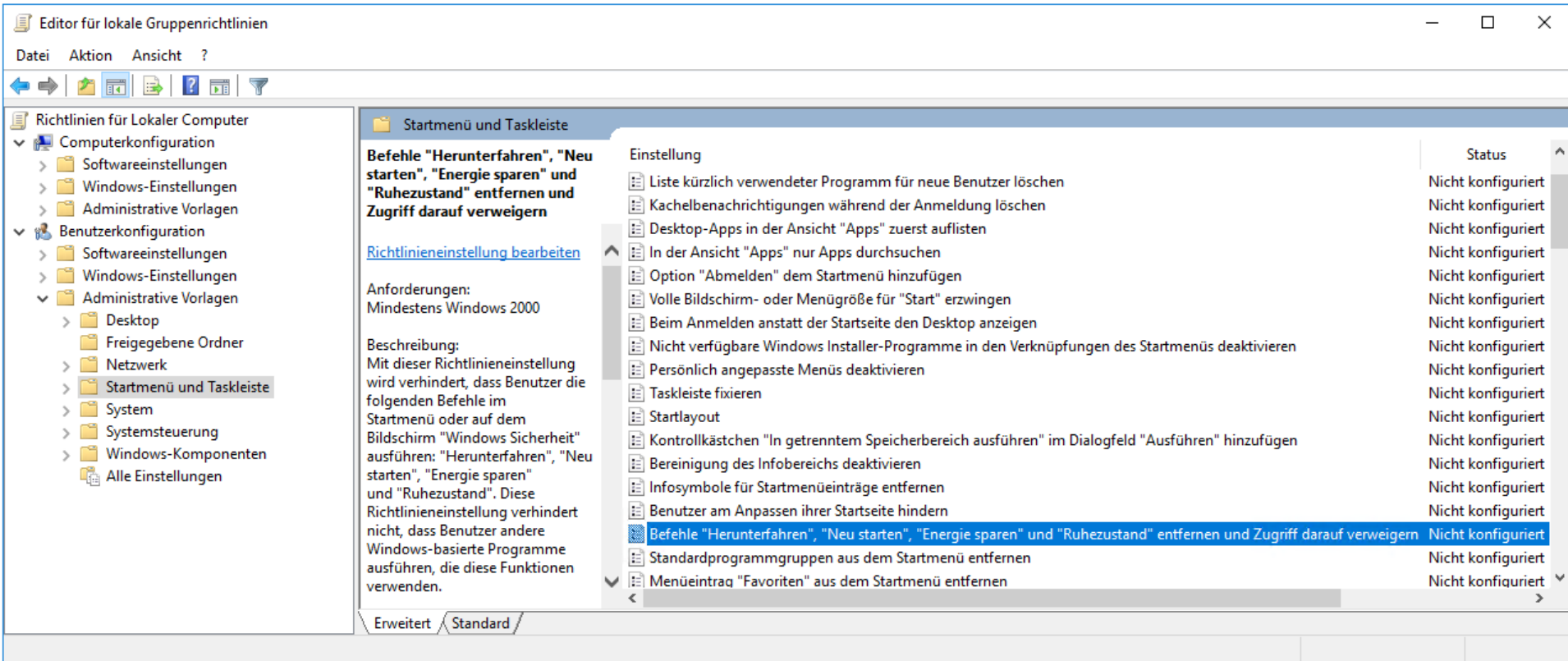
Gruppenrichtlinien (1)

- Vorkonfiguration von Anwendungen / Betriebssystem
- Lokal auf PC und/oder über das AD verwaltete GPOs
- Einträge in die Registry, Skripte, Software, vordefinierte Einstellungen
- gpupdate.exe /force
- gpresult.exe /h <Pfad>\<Name>.html

Gruppenrichtlinien (2)

- Computerkonfiguration
 - Einstellungen die den Rechner betreffen
- Benutzerkonfiguration
 - Einstellungen die den Benutzer betreffen
- Administrative Vorlagen (admx-File)
 - Vorlagen für bestimmte Regeln
 - Erweiterbar
 - Nicht nur von Microsoft

Editor für lokale Gruppenrichtlinien (1)



Editor für lokale Gruppenrichtlinien

Datei Aktion Ansicht ?

Richtlinien für Lokaler Computer

- Computerkonfiguration
 - Softwareeinstellungen
 - Windows-Einstellungen
 - Administrative Vorlagen
- Benutzerkonfiguration
 - Softwareeinstellungen
 - Windows-Einstellungen
 - Administrative Vorlagen
 - Desktop
 - Freigegebene Ordner
 - Netzwerk
 - Startmenü und Taskleiste**
 - System
 - Systemsteuerung
 - Windows-Komponenten
 - Alle Einstellungen

Startmenü und Taskleiste

Befehle "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand" entfernen und Zugriff darauf verweigern

[Richtlinieneinstellung bearbeiten](#)

Anforderungen:
Mindestens Windows 2000

Beschreibung:
Mit dieser Richtlinieneinstellung wird verhindert, dass Benutzer die folgenden Befehle im Startmenü oder auf dem Bildschirm "Windows Sicherheit" ausführen: "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand". Diese Richtlinieneinstellung verhindert nicht, dass Benutzer andere Windows-basierte Programme ausführen, die diese Funktionen verwenden.

Einstellung

Liste kürzlich verwendeter Programme für neue Benutzer löschen	Nicht konfiguriert
Kachelbenachrichtigungen während der Anmeldung löschen	Nicht konfiguriert
Desktop-Apps in der Ansicht "Apps" zuerst auflisten	Nicht konfiguriert
In der Ansicht "Apps" nur Apps durchsuchen	Nicht konfiguriert
Option "Abmelden" dem Startmenü hinzufügen	Nicht konfiguriert
Volle Bildschirm- oder Menügröße für "Start" erzwingen	Nicht konfiguriert
Beim Anmelden anstatt der Startseite den Desktop anzeigen	Nicht konfiguriert
Nicht verfügbare Windows Installer-Programme in den Verknüpfungen des Startmenüs deaktivieren	Nicht konfiguriert
Persönlich angepasste Menüs deaktivieren	Nicht konfiguriert
Taskleiste fixieren	Nicht konfiguriert
Startlayout	Nicht konfiguriert
Kontrollkästchen "In getrenntem Speicherbereich ausführen" im Dialogfeld "Ausführen" hinzufügen	Nicht konfiguriert
Bereinigung des Infobereichs deaktivieren	Nicht konfiguriert
Infosymbole für Startmenüeinträge entfernen	Nicht konfiguriert
Benutzer am Anpassen ihrer Startseite hindern	Nicht konfiguriert
Befehle "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand" entfernen und Zugriff darauf verweigern	Nicht konfiguriert
Standardprogrammgruppen aus dem Startmenü entfernen	Nicht konfiguriert
Menüeintrag "Favoriten" aus dem Startmenü entfernen	Nicht konfiguriert

Erweitert Standard

Editor für lokale Gruppenrichtlinien (2)

Befehle "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand" entfernen und Zugriff darauf verwei...

Befehle "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand" entfernen und Zugriff darauf verweigern

Vorherige Einstellung Nächste Einstellung

☐ Nicht konfiguriert ☒ Aktiviert ☐ Deaktiviert

Kommentar:

Unterstützt auf: Mindestens Windows 2000

Optionen:

Hilfe:

Mit dieser Richtlinieneinstellung wird verhindert, dass Benutzer die folgenden Befehle im Startmenü oder auf dem Bildschirm "Windows Sicherheit" ausführen: "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand". Diese Richtlinieneinstellung verhindert nicht, dass Benutzer andere Windows-basierte Programme ausführen, die diese Funktionen verwenden.

Wenn Sie diese Richtlinieneinstellung aktivieren, werden der Netzschalter und die Befehle "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand" aus dem Startmenü entfernt. Der Netzschalter wird auch vom Bildschirm "Windows-Sicherheit" entfernt, der angezeigt wird, wenn Sie STRG+ALT-ENTF drücken.

Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, sind der Netzschalter und die Befehle "Herunterfahren", "Neu starten", "Energie sparen" und "Ruhezustand" im Startmenü verfügbar. Der Netzschalter ist auch auf dem Bildschirm "Windows-Sicherheit" verfügbar.

Hinweis: Drittanbieterprogramme, die als Microsoft Windows Vista-

OK Abbrechen Übernehmen

		Status
Programm für neue Benutzer löschen		Nicht konfiguriert
Während der Anmeldung löschen		Nicht konfiguriert
Apps zuerst auflisten		Nicht konfiguriert
Suche durchsuchen		Nicht konfiguriert
Startmenü hinzufügen		Nicht konfiguriert
Verbot für "Start" erzwingen		Nicht konfiguriert
Startseite den Desktop anzeigen		Nicht konfiguriert
Alle Programme in den Verknüpfungen des Startmenüs deaktivieren		Nicht konfiguriert
Deaktivieren		Nicht konfiguriert
Im Speicherbereich ausführen" im Dialogfeld "Ausführen" hinzufügen		Nicht konfiguriert
Deaktivieren		Nicht konfiguriert
Verbot entfernen		Nicht konfiguriert
Startseite hindern		Nicht konfiguriert
Befehle "Herunterfahren", "Energie sparen" und "Ruhezustand" entfernen und Zugriff darauf verweigern		Aktiviert
Verbot aus dem Startmenü entfernen		Nicht konfiguriert

Editor für lokale Gruppenrichtlinien (3)

Group Policy Management Editor

File Action View Help

COURSE Link Feedback (U) [+]

- Computer Configuration
 - Policies
 - Preferences
- User Configuration
 - Policies
 - Preferences
 - Windows Settings
 - Applications
 - Drive Maps
 - Environment
 - Files
 - Folders
 - Ini Files
 - Registry
 - Shortcuts
 - Control Panel Set
 - Data Sources
 - Devices
 - Folder Option
 - Internet Setting
 - Local Users and Groups
 - Network Options
 - Power Options

Shortcuts

Name	Order	Action	Shortcut
Feedback	1	Replace	%DesktopDir%\Feedb...

Processing

- Stop processing items in extension on error: No
- Run in user's context: Yes
- Remove if not applied: No
- Apply once: No
- Filtered directly: No
- Filtered by ancestor: No
- Disabled directly: No
- Disabled by ancestor: No

Description

No description provided.

Preferences Extended Standard

Last changed: 27.02.2019 12:00:29

Feedback Properties

General Common

Action: Replace

Name: Feedback

Target type: URL

Location: Desktop

Target URL: <https://www.kurse.rrze.fau.de/tca/fb>

Arguments:

Start in:

Shortcut key: None

Run: Normal Window

Comment:

Icon file path: %SystemRoot%\system32\SHELL32.dll

Icon index: 23

OK Cancel Apply Help



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

- Updates
 - FAU-Test/Next/Current 0, 1, 2 um 0/1/2 Wochen verzögert
- Upgrades
 - FAU-Test 0, 1, 2 sofort (alle Builds)
 - FAU-Next 0, 1, 2 um 12 Monate verzögert (xx09)
 - FAU-Current 0, 1, 2 um 24 Monate verzögert (xx09)
- Weitere Infos <https://www.rrze.fau.de/hard-software/betriebssysteme/windows/sicherheitspatches/>
- Mailingliste „FAUSUS-Nutzer“ in IdM abonnieren

WINDOWS-FIREWALL



FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Windows-Firewall (1)

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

Windows-Firewall (2)

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

Windows-Firewall – Regeltyp

Assistent für neue eingehende Regel

Regeltyp

Wählen Sie den Typ der zu erstellenden Firewallregel aus.

Schritte:

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

Welchen Regeltyp möchten Sie erstellen?

☐ **Programm**
Regel, die die Verbindungen für ein Programm steuert.

☐ **Port**
Regel, die die Verbindungen für einen TCP- oder UDP-Port steuert.

☐ **Vordefiniert:**
Remotedesktop
Regel, die die Verbindungen für einen Windows-Vorgang steuert.

☒ **Benutzerdefiniert**
Benutzerdefinierte Regel

< Zurück Weiter > Abbrechen

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.

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: Anpassen...

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

Assistent für neue eingehende Regel

Aktion

Legen Sie die Aktion fest, die ausgeführt werden soll, wenn eine Verbindung die in der Regel angegebenen Bedingungen erfüllt.

Schritte:

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

Welche Aktion soll durchgeführt werden, wenn eine Verbindung die angegebenen Bedingungen erfüllt?

☒ **Verbindung zulassen**
Dies umfasst sowohl mit IPsec geschützte als auch nicht mit IPsec geschützte Verbindungen.

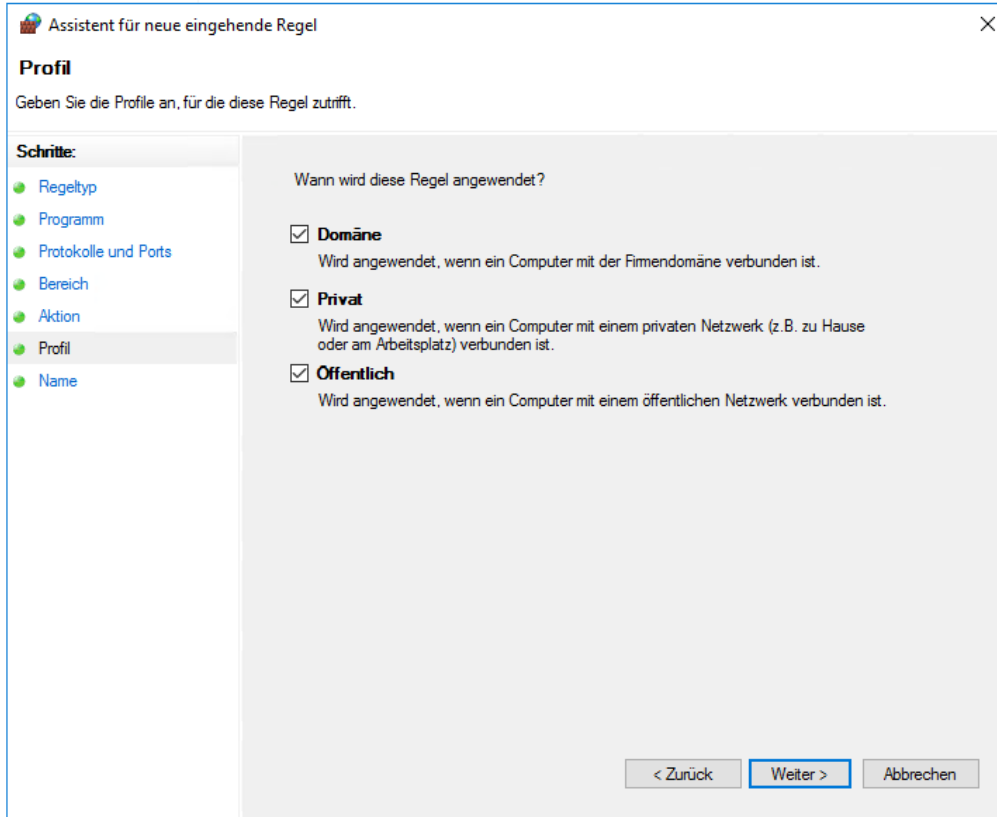
☐ **Verbindung zulassen, wenn sie sicher ist**
Dies umfasst nur mithilfe von IPsec authentifizierte Verbindungen. Die Verbindungen werden mit den Einstellungen in den IPsec-Eigenschaften und -regeln im Knoten "Verbindungssicherheitsregel" gesichert.

Anpassen...

☐ **Verbindung blockieren**

< Zurück Weiter > Abbrechen

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-Firewall mit erweiterter Sicherheit

Datei Aktion Ansicht ?

Windows-Firewall mit erweiterter Sicherheit - Lokaler Computer

- Eingehende Regeln
- Ausgehende Regeln
- Verbindungssicherheitsregeln
- Überwachung

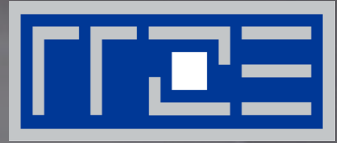
Eingehende Regeln						
Name	Gruppe	Profil	Aktiviert	Aktion	Auswirkung	
Freigabe von Port 80		Alle	Ja	Zulassen	Nein	
Verwaltung virtueller TPM-Smartcards (T...	Verwaltung virtueller TPM-S...	Privat, Öffentlich	Nein	Zulassen	Nein	
Verwaltung virtueller TPM-Smartcards (D...	Verwaltung virtueller TPM-S...	Privat, Öffentlich	Nein	Zulassen	Nein	
SNMP-Ablaufverfolgungsdienst (UDP ein...	SNMP-Trap	Privat, Öffentlich	Nein	Zulassen	Nein	
Leistungsprotokolle und -warnungen (TC...	Leistungsprotokolle und -w...	Privat, Öffentlich	Nein	Zulassen	Nein	
Leistungsprotokolle und -warnungen (D...	Leistungsprotokolle und -w...	Privat, Öffentlich	Nein	Zulassen	Nein	
"Wiedergabe auf Gerät"-Funktionalität (q...	"Wiedergabe auf Gerät"-Fun...	Privat, Öffentlich	Ja	Zulassen	Nein	
"Wiedergabe auf Gerät"-Funktionalität (q...	"Wiedergabe auf Gerät"-Fun...	Privat, Öffentlich	Ja	Zulassen	Nein	
Netzwerkerkennung (WSD-Ereignisse ein...	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (WSD EventsSecure ...	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (WSD eingehend)	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (UPnP eingehend)	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (SSDP eingehend)	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (Pub-WSD eingehen...	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (NB-Name eingehen...	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (NB-Datagramm ein...	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
Netzwerkerkennung (LLMNR-UDP einge...	Netzwerkerkennung	Privat	Ja	Zulassen	Nein	
DIAL-Protokollserver (HTTP-In)	DIAL-Protokollserver	Privat	Ja	Zulassen	Nein	
"Wiedergabe auf Gerät"-Streamingserver ...	"Wiedergabe auf Gerät"-Fun...	Privat	Ja	Zulassen	Nein	
"Wiedergabe auf Gerät"-Streamingserver ...	"Wiedergabe auf Gerät"-Fun...	Privat	Ja	Zulassen	Nein	
"Wiedergabe auf Gerät"-Streamingserver ...	"Wiedergabe auf Gerät"-Fun...	Privat	Ja	Zulassen	Nein	

Aktionen

- Eingehende Regeln
- Neue Regel...
- Nach Profil filtern
- Nach Status filtern
- Nach Gruppe filtern
- Ansicht
- Aktualisieren
- Liste exportieren...
- Hilfe



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

Task Scheduler

File Action View Help

Task Scheduler (Local)

- Task Scheduler Library
 - Microsoft
 - Configuration Manager
 - Office
 - Windows
 - .NET Framework
 - Active Directory Rights I
 - AppID
 - Application Experience
 - ApplicationData
 - AppxDeploymentClient
 - Autochk
 - BitLocker
 - Bluetooth
 - BrokerInfrastructure
 - CertificateServicesClient
 - Chkdsk
 - Clip

Name	Status	Triggers
MicrosoftEdgeUpdateTa...	Ready	Multiple triggers defined
MicrosoftEdgeUpdateTa...	Ready	At 12:03 every day - After triggered, repeat every 1 hour for a duration

General Triggers Actions Conditions Settings History

Name: MicrosoftEdgeUpdateTaskMachineCore

Location: \

Author:

Description: Hält ihre Microsoft-Software auf dem neuesten Stand. Wenn Sie diese Aufgabe deaktivieren, kann die Microsoft-Software nicht auf dem neuesten Stand gehalten werden, was zu Sicherheitsrisiken führt, die nicht zu beheben sind, und bestimmte Funktionen möglicherweise nicht funktionieren. Diese Aufgabe installiert sich selbst, wenn sie von

Actions

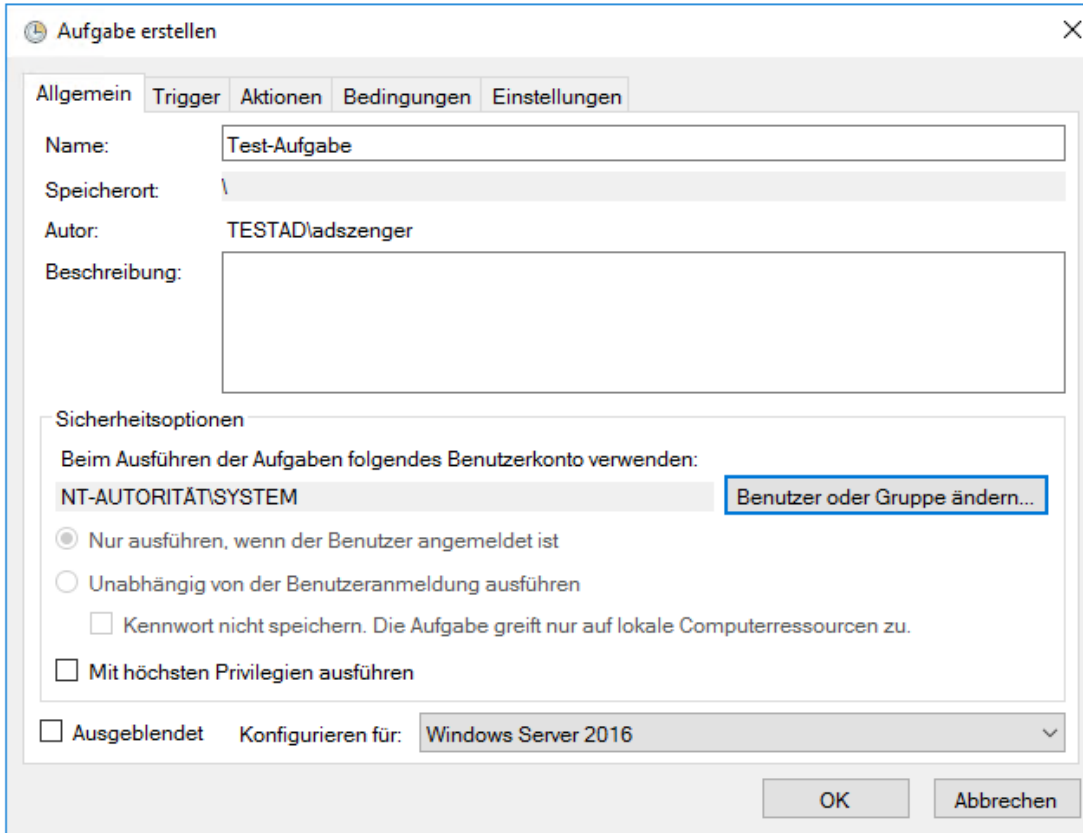
Task Scheduler Library

- Create Basic Task...
- Create Task...
- Import Task...
- Display All Running Tasks
- Disable All Tasks
- New Folder...
- View
- Refresh
- Help

Selected Item

- Run
- End

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. The 'Sicherheitsoptionen' (Security options) section shows 'Beim Ausführen der Aufgaben folgendes Benutzerkonto verwenden:' (When running the task, use the following user account:). The user account is '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.). The first radio button is selected. There are also two checkboxes: 'Mit höchsten Privilegien ausführen' (Run with highest privileges) and 'Ausgeblendet' (Hidden). The 'Konfigurieren für:' (Configure for:) dropdown menu is 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 ☐ Zeitzonenübergreifende 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 ☐ Zeitzonenübergreifende 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 Durchsuchen...

Argumente hinzufügen (optional): <Pfad zum PS-Skript>

Starten in (optional):

OK Abbrechen

Aufgabe erstellt

Aufgabenplanung

Datei Aktion Ansicht ?

Aufgabenplanung (Lokal)

Aufgabenplanungsbibliothek

Name	Status	Trigger	Nächste Lauf...	Ergebnis der letzten Ausführung
Test-Aufgabe	Bereit	Wird am Letzter Dienst...	30.05.2017 14:27:01	Die Aufgabe wurde noch nicht ausgeführt. (0x4...

Allein Trigger Aktionen Bedingungen Einstellungen Verlauf

Anzahl von Ereignissen: 1

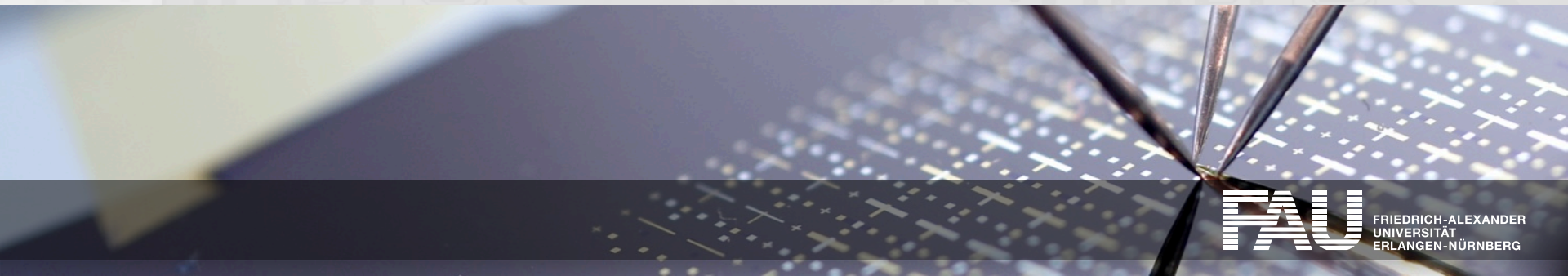
Ebene	Datum und Uhrz...	Ereig...	Aufgabenkatego...	Vorgangscode	Korrelations...
Informationen	25.04.2017 14:27:53	106	Aufgabe registriert	Info	

Aktionen

- Aufgabenplanungsbibliothek
- Einfache Aufgabe erstellen...
- Aufgabe erstellen...
- Aufgabe importieren...
- Alle aktiven Aufgaben anzeigen
- Verlauf für alle Aufgaben deaktivieren
- Neuer Ordner...
- Ansicht
- Aktualisieren
- Hilfe
- Ausgewähltes Element
- Ausführen
- Beenden
- Deaktivieren
- Exportieren...
- Eigenschaften
- Löschen






EREIGNISANZEIGE



FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Ereignisanzeige (Event Viewer)

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

eventvwr.msc

Ereignisanzeige

Datei Aktion Ansicht ?

Ereignisanzeige (Lokal)

- Benutzerdefinierte Ansichten
- Windows-Protokolle
 - Anwendung
 - Sicherheit
 - Installation**
 - System
 - Weitergeleitete Ereignisse
- Anwendungs- und Dienstprotokolle
 - Hardware-Ereignisse
 - Internet Explorer
- Microsoft
 - AppV
 - Client
 - User Experience Virtualization
 - Windows
 - Schlüsselverwaltungsdienst
 - Windows PowerShell
 - Abonnements

Installation Anzahl von Ereignissen: 58

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 Protokolliert: 11.05.2017 14:37:34

Ereignis-ID: 4 Aufgabenkategorie: Keine

Ebene: Warnung Schlüsselwörter:

Benutzer: ... Computer: ...

Vorgangscode: Info

Weitere Informationen: [Onlinehilfe](#)

Aktionen

- Installation
 - Gespeicherte Protokolldatei öffnen...
 - Benutzerdefinierte Ansicht erstellen...
 - Benutzerdefinierte Ansicht importiere...
 - Protokoll löschen...
 - Aktuelles Protokoll filtern...
 - Eigenschaften
 - Suchen...
 - Alle Ereignisse speichern unter...
 - Aufgabe an dieses Protokoll anfügen...
- Ansicht
 - Aktualisieren
 - Hilfe
- Ereignis 4, WUSA
 - Ereigniseigenschaften
 - Aufgabe an dieses Ereignis anfügen...
 - Kopieren
 - Ausgewählte Ereignisse speichern...
 - Aktualisieren
 - Hilfe



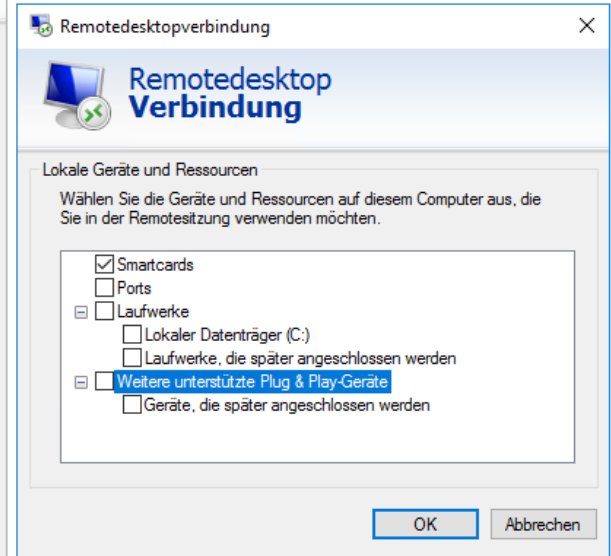
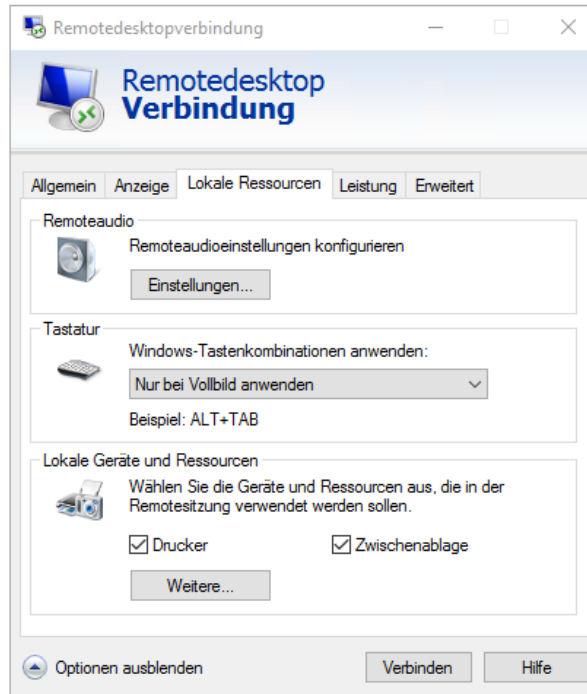
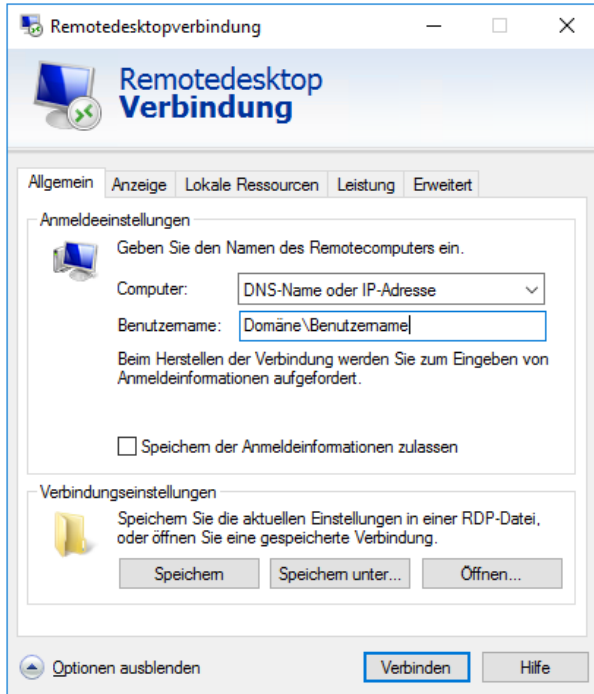
TERMINALSERVER (REMOTE DESKTOP SERVICES)



Terminalserver (Remote Desktop Services)

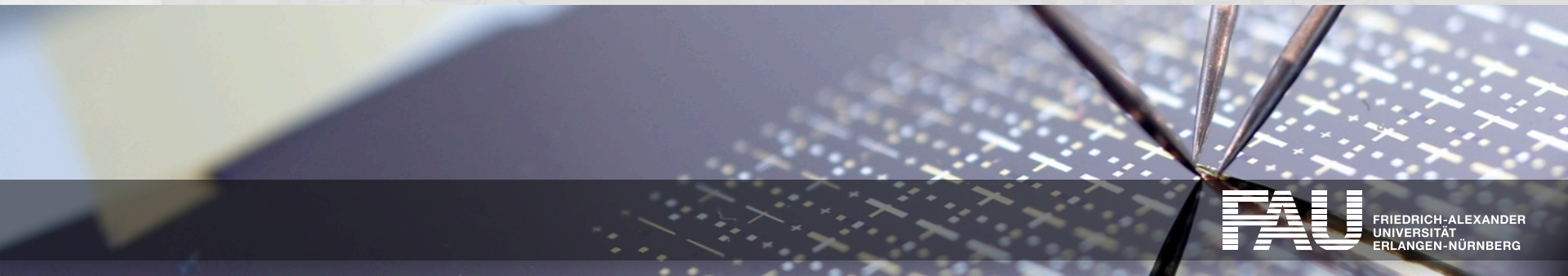
- Zentralbetriebener Windows-Server mit installierten RDS
 - Zentrale Bereitstellung und Administration
 - Keine Begrenzung von zeitgleichen Benutzersitzungen
- Dimensionierung je nach Benutzeranzahl
- Sitzungsbasiert (RDP), RemoteApps und VDI
- Lizenzierung
 - RDS User CALs
 - RDS Device CALs

RDP-Client





ZUM ENDE



FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

Windows 10 - besser als gedacht?!

- Windows 10 „Datensammelwut“ einschränken
 - GPOS in FAUAD (Muster OU)
- Tastenkürzel gehen immer noch
<https://support.microsoft.com/de-de/help/12445/windows-keyboard-shortcuts>
- Leichter managebar mittels Domäne
- Windows 10 Builds aktuell halten



ORGANISATORISCHES



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

Weitere Vorträge zur „Systemausbildung“

13.05.2020 – Windows-Betriebssysteme

20.05.2020 – Systemüberwachung / Monitoring

27.05.2020 – Storage & Filesysteme

17.06.2020 – Virtualisierung

24.06.2020 – Backup / Archiv

01.07.2020 – IT-Sicherheit

08.07.2020 – High Performance Computing

15.07.2020 – Benutzerverwaltung: MS Active Directory

22.07.2020 – LDAP und Kerberos

Immer mittwochs
(ab 14:15 Uhr)
- online -

Details: www.rrze.fau.de/veranstaltungen/veranstaltungskalender/

Weitere Vortragsreihen des RRZE im SoSe 2020

Campustreffen „IT-Dienste des RRZE und der FAU“

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

Nächste Campustreffen

14.05.2020 (9:00-14:30 Uhr) – Microsoft Surface Day

28.05.2020 – Webmaster-Campustreffen

Details: www.rrze.fau.de/veranstaltungen/veranstaltungskalender/

Vortragsfolien und Vortragsaufzeichnung

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

www.rrze.fau.de/ausbildung-schulung/veranstaltungsreihen/systemausbildung/

Die meisten Vorträge des RRZE werden aufgezeichnet und können nach der Veranstaltung vom Videoportal der FAU heruntergeladen werden:

www.fau.tv

RRZE-Veranstaltungskalender und Mailinglisten

- Kalender abonnieren oder bookmarken
 - www.rrze.fau.de/veranstaltungen/veranstaltungskalender/
- Mailingliste abonnieren
 - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste [RRZE-Aktuelles](http://www.rrze.fau.de/aktuelles/) gesendet.
 - Auch diese Liste kann man abonnieren:
<https://lists.fau.de/mailman/listinfo/rrze-aktuelles>

Themenvorschläge und 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>