Übung 19.1

- Erstellen Sie in der „Default Domain Policy“ eine Ordnerumleitung, in der der Ordner „Dokumente“ auf eine Freigabe auf Server1 mit Namen „Profile“ umgeleitet wird
- Erstellen Sie die benötigte Freigabe und vergeben Sie die Berechtigung „Jeder – Vollzugriff“
- Melden Sie sich danach als Karl Klammer an W11 an, und beobachten Sie, was in der Freigabe auf Server1 passiert

Lösung 19.1

Erstellen der Freigabe auf „Server1“

- Wechseln Sie auf die virtuelle Maschine „Server1“
- Öffnen Sie den Windows Explorer und erstellen Sie im Laufwerk C:\ einen Ordner mit Namen „Profile“
- Klicken Sie mit der rechten Maustaste auf den Ordner mit Namen „Profile“
- Wählen Sie „Eigenschaften“ – „Registerkarte Freigabe“ – „Erweiterte Freigabe“
- Setzen Sie den Haken vor „Diesen Ordner freigeben“
- Klicken Sie im unteren Teil auf „Berechtigungen“
- Geben Sie der Gruppe „Jeder“ die Berechtigung „Vollzugriff“
- Bestätigen Sie alle offenen Fenster mit „OK“

Bearbeiten der „Default Domain Policy“

- Öffnen Sie den Server-Manager der virtuellen Maschine „DC“
- Wählen Sie „Tools“ – „Gruppenrichtlinienverwaltung“
- Öffnen Sie auf der linken Seite die Domänen und wählen Sie die Domäne „Meistertrainer.info“ „Default Domain Policy“ aus
- Klicken Sie mit der rechten Maustaste und wählen Sie „Bearbeiten“
- Navigieren Sie zu
    - Benutzerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Ordnerumleitungen
    - Dokumente
- Klicken Sie mit der rechten Maustaste und wählen Sie „Eigenschaften“
- Wählen Sie auf der Registerkarte „Ziel“ – „Standard-Leitet alle Ordner auf den gleichen Pfad um“
- Geben Sie bei Stammverzeichnis ein \\Server1\Profile
- Bestätigen Sie die Warnmeldung

Anwenden der Gruppenrichtlinie

- Wechseln Sie auf die virtuelle Maschine „W11“
- Melden Sie sich ab und wieder an als als „KK“ mit dem Kennwort „Kennw0rt!“
- Wechseln Sie zur virtuellen Maschine „Server1“
- Beobachten Sie, dass unterhalb des Ordners „Profile“ ein Ordner mit dem Namen „KK“ erstellt wird
- Ein weiterer Unterordner „Documents“ wird ebenfalls unterhalb von „KK“ erstellt, auf den Sie keinen Zugriff haben, da es sich um private Daten handelt

ACHTUNG! Manchmal wird die Gruppenrichtlinie nicht sofort angewendet!

- Sollte das nicht der Fall sein, geben Sie „GPUpdate /Force“ ein
- Sie erhalten den Hinweis, dass der Benutzer sich erneut anmelden muss, bestätigen Sie mit „J“ und führen Sie die Neuanmeldung durch

Übung 19.2

- Erstellen Sie ein VBS-Skript mit Namen „Guten_Morgen.vbs, das eine Textbox mit den Worten „Guten Morgen!“ ausgibt
- Bearbeiten Sie die „Default Domain Policy“ und binden Sie dort dieses Skript als Anmelde-Skript ein
- Melden Sie sich als Karl Klammer an W11 an, und überprüfen Sie, ob das Skript ausgeführt wird

Lösung 19.2

Erstellen des VBS-Skripts

- Wechseln Sie zur virtuellen Maschine „DC“
- Öffnen Sie die App „Editor“
- Schreiben Sie dort folgenden Text:
    - MsgBox "Guten Morgen!"
- Speichern Sie diese Datei als „Guten_Morgen.txt“ im Ordner „Dokumente“
- Öffnen Sie den Windows-Explorer
- Wechseln Sie in den Ordner „Dokumente“
- Um die Dateiextensionen zu sehen, wählen Sie
    - Ansicht

    - Optionen
    - Ordner und Suchoptionen ändern
    - Registerkarte „Ansicht“
    - Haken entfernen vor „Erweiterungen bei bekannten Dateitypen ausblenden“
    - OK
- Klicken Sie mit der rechten Maustaste auf die Datei „Guten_Morgen.txt“
    - Wählen Sie „Umbenennen“
    - Geben Sie ihr den Namen „Guten_Morgen.vbs“
- Bestätigen Sie den Warnhinweis
- Probieren Sie aus, ob das Skript funktioniert, indem Sie darauf einen Doppelklick setzen
- Bestätigen Sie die Funktion mit „OK“
- Kopieren Sie diese Datei in die Zwischenablage (rechte Maustaste auf Datei – Kopieren)

Bearbeiten der „Default Domain Policy“

- Öffnen Sie den Server-Manager der virtuellen Maschine „DC“
- Wählen Sie „Tools“ – „Gruppenrichtlinienverwaltung“
- Öffnen Sie auf der linken Seite die Domänen und wählen Sie die Domäne „Meistertrainer.info“ „Default Domain Policy“ aus
- Klicken Sie mit der rechten Maustaste und wählen Sie „Bearbeiten“
- Navigieren Sie zu
    - Benutzerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Skripts (Anmelden/Abmelden)
- Klicken Sie mit der rechten Maustaste auf „Anmelden“ auf der rechten Seite und wählen Sie „Eigenschaften“
- Klicken Sie auf der Registerkarte „Skripts“ auf „Dateien anzeigen“
- Der richtige Ordner wird angezeigt. Klicken Sie auf der rechten Seite des Fensters mit der rechten Maustaste ins Leere und wählen Sie „Einfügen“
- Schließen Sie dieses Fenster
- Das Fenster „Eigenschaften von Anmelden“ – „Skripts“ erscheint wieder
- Wählen Sie „Hinzufügen“
- Fenster „Hinzufügen eines Skripts“: Durchsuchen und Auswahl des Skripts „Guten_Morgen.vbs“
- Bestätigen mit OK
- Schließen der „Eigenschaften von Anmelden“ mit OK
- Schließen der Gruppenrichtlinie

Anwenden der Gruppenrichtlinie

- Wechseln Sie auf die virtuelle Maschine „W11“
- Melden Sie sich ab und wieder an als als „KK“ mit dem Kennwort „Kennw0rt!“
- Das Skript sollte ausgeführt werden

ACHTUNG! Manchmal wird die Gruppenrichtlinie nicht sofort angewendet und das Skript wird nicht direkt nach der Anmeldung des Benutzers ausgeführt!

- Sollte das nicht der Fall sein, geben Sie „GPUpdate /Force“ ein
- Sie erhalten den Hinweis, dass der Benutzer sich erneut anmelden muss, bestätigen Sie mit „J“ und führen Sie die Neuanmeldung durch

Übung 19.3.1

- Erstellen Sie auf der virtuellen Maschine „DC“ eine MMC mit den Snap-ins
    - Sicherheitsvorlagen
    - Sicherheitskonfiguration und –analyse
- Fügen Sie den lokalen Pfad zu den Sicherheitsvorlagen hinzu
- Kopieren Sie die Sicherheitsvorlage „DC security“ und speichern Sie sie unter dem Namen „Meine Vorlage“
- Erstellen Sie eine neue leere Vorlage mit dem Namen „Neue Vorlage“
- Erstellen Sie eine neue Sicherheitsdatenbank mit dem Namen „Test“
- Importieren Sie die Vorlage „Neue Vorlage“
- Starten Sie eine Analyse und betrachten Sie die Ergebnisse

Lösung 19.3.1

MMC erstellen

- Wechseln Sie zur virtuellen Maschine „DC“
- Geben Sie unten in der Taskleiste in das Feld mit der Lupe ein „mmc.exe“
- Es öffnet sich eine leere Management-Konsole
- Wählen Sie
    - Datei
    - Snap-In hinzufügen/entfernen
    - Verfügbare Snap-Ins:
    - Sicherheitsvorlagen - hinzufügen

  - Sicherheitskonfiguration und –analyse - hinzufügen
  - OK
- Klicken Sie mit der rechten Maustaste in der linken Seite der MMC auf „Sicherheitsvorlagen“
- Wählen Sie „Neuer Vorlagensuchpfad“
- Geben Sie als Pfad an: „C:\Windows\security\templates“
- Erweitern Sie die Vorlagen, Sie sehen die Vorlage „DC security“

Kopieren der Vorlage

- Klicken Sie mit der rechten Maustaste auf „DC security“
- Wählen Sie „Speichern unter“
- Nennen Sie die neue Vorlage „Meine Vorlage“

Erstellen einer neuen Vorlage

- Klicken Sie mit der rechten Maustaste auf „C:\Windows \Security Templates“
- Wählen Sie „Neue Vorlage“
- Nennen Sie die neue Vorlage „Neue Vorlage“

Sicherheitsdatenbank erstellen

- Klicken Sie mit der rechten Maustaste auf „Sicherheitskonfiguration und –analyse“
- Wählen Sie „Datenbank öffnen“
- Geben Sie bei „Dateiname“ ein „Test“ und klicken Sie auf „Öffnen“
- Navigieren Sie im Fenster „Vorlage importieren“ zu :
  „C:\Windows\security\templates\Neue Vorlage.inf“

Analyse

- Klicken Sie mit der rechten Maustaste auf „Sicherheitskonfiguration und –analyse“
- Wählen Sie „Computer jetzt analysieren“
- Bestätigen Sie den Speicherpfad des Fehlerprotokolls
- Nach Erstellung der Analyse betrachten Sie diese

Übung 19.3.3

- Öffnen Sie die „Default Domain Policy“ und betrachten Sie die Kontorichtlinien

- Beurteilen Sie die Einstellungen
- Wechseln Sie zu den Überwachungsrichtlinien
- Aktivieren Sie die „Objektzugriffsversuche“ mit „Erfolgreich“ und „Fehler“
- Erstellen Sie auf der virtuellen Maschine „DC“ einen Ordner mit Namen „Daten“
- Aktivieren Sie die Überwachung auf diesem Ordner, für alle Domänenbenutzer mit der Aktion „Löschen“
- Erstellen Sie eine Textdatei im Ordner „Daten“ und löschen Sie diese wieder
- Kontrollieren Sie die Sicherheitseinträge im Ereignisprotokoll

Lösung 19.3.3

Betrachten der Einstellungen der Kontorichtlinien

- Öffnen Sie den Server-Manager der virtuellen Maschine „DC“
- Wählen Sie „Tools“ – „Gruppenrichtlinienverwaltung“
- Öffnen Sie auf der linken Seite die Domänen und wählen Sie die Domäne „Meistertrainer.info“ aus
- Wechseln Sie zu „Default Domain Policy“, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Bearbeiten“
- Navigieren Sie zu
    - Computerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Sicherheitseinstellungen
    - Kontorichtlinien
- Beurteilung: diese Einstellungen gelten für alle Computerkonten in der Domäne und bieten dadurch eine gute Kontensicherheit

Bearbeiten der Überwachungsrichtlinien

- Navigieren Sie zu
    - Computerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Sicherheitseinstellungen
    - Lokale Richtlinien
    - Überwachungsrichtlinie

- Klicken Sie auf der rechten Seite des Fensters auf „Objektzugriffsversuche überwachen“, aktivieren Sie diese Richtlinie und wählen Sie „Erfolgreich“ und „Fehler“
- Schließen Sie die Gruppenrichtlinie

Erstellen der Freigabe und Erzeugen von Vorfällen

- Öffnen Sie den Windows Explorer auf der virtuellen Maschine „DC“ und erstellen Sie auf C:\ den Ordner „Daten“
- Klicken Sie mit der rechten Maustaste auf diesen Ordner und wählen Sie
    - Eigenschaften
    - Registerkarte „Sicherheit“
    - Im unteren Teil des Fensters „Erweitert“
    - Registerkarte „Überwachung“
    - Im unteren Teil des Fensters „Hinzufügen“
- Klicken Sie oben auf „Prinzipal auswählen“
- Geben Sie im unteren Fenster ein „Domänen-Benutzer“ und klicken Sie auf „OK“
- Klicken Sie im mittleren Teil des Fensters auf „Erweiterte Berechtigungen anzeigen“
- Setzen Sie im mittleren Teil des Fensters den Haken bei „Löschen“ und entfernen Sie alle anderen Haken
- Klicken Sie auf „OK“
- Öffnen Sie den Ordner „Daten“
- Klicken Sie mit der rechten Maustaste in das rechte Fenster und wählen Sie „Neu“-„Textdokument“
- Löschen Sie das eben erstellte Textdokument wieder

Kontrolle im Ereignisprotokoll

- Klicken Sie auf der virtuellen Maschine „DC“ mit der rechten Maustaste auf den Start-Button und wählen Sie „Ereignisanzeige“
- Wechseln Sie zu „Windows-Protokolle“ – „Sicherheit“ und betrachten Sie die Daten

Übung 19.3.4

- Betrachten Sie die Einstellungen der Benutzerkontensteuerung genau
- Beachten Sie auch die Erklärungen zu den einzelnen Einstellungen
- Führen Sie keine Änderungen durch

Lösung 19.3.4

- Öffnen Sie den Server-Manager der virtuellen Maschine „DC“
- Wählen Sie „Tools“ – „Gruppenrichtlinienverwaltung“
- Öffnen Sie auf der linken Seite die Domänen und wählen Sie die Domäne „Meistertrainer.info“ aus
- Wechseln Sie zu „Default Domain Policy“, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Bearbeiten“
- Navigieren Sie zu
    - Computerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Sicherheitseinstellungen
    - Lokale Richtlinien
    - Sicherheitsoptionen
- Setzen Sie im rechten Fenster auf die jeweilige Einstellung einen Doppelklick
- Wechseln Sie zur Registerkarte „Erklärung“

Übung 19.4

- Erstellen Sie eine Anwendungssteuerungsrichtlinie in er „Default Domain Policy“, in der Sie den Zugriff auf alle Apps erlauben, die von Microsoft erstellt worden sind
- Setzen Sie alle virtuellen Maschinen auf den Prüfpunkt „Basis“ zurück

Lösung 19.4

- Öffnen Sie den Server-Manager der virtuellen Maschine „DC“
- Wählen Sie „Tools“ – „Gruppenrichtlinienverwaltung“
- Öffnen Sie auf der linken Seite die Domänen und wählen Sie die Domäne „Meistertrainer.info“ aus
- Wechseln Sie zu „Default Domain Policy“, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Bearbeiten“
- Navigieren Sie zu
    - Computerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Sicherheitseinstellungen
    - Anwendungssteuerungsrichtlinien

    - App-Locker
    - Ausführbare Regeln
- Klicken Sie mit der rechten Maustaste und wählen Sie „Neue Regel erstellen“
- Vorbereitung: Weiter
- Berechtigungen: „Zulassen“, Gruppe „Jeder“
- Bedingungen: Herausgeber
- Herausgeber: Referenzdatei-Durchsuchen
- Wählen Sie eine beliebige Datei von Microsoft, beispielsweise Windows Mail – wab.exe
- Klicken Sie auf „Weiter“
- Ausnahmen: Weiter ohne Änderungen
- Name und Beschreibung: Einstellungen lassen oder ändern, nach Belieben
- Erstellen

Zurücksetzen der virtuellen Maschinen

- Wechseln Sie auf Ihre Hostmaschine
- Öffnen Sie den Hyper-V-Manager
- Klicken Sie im mittleren Fenster mit der rechten Maustaste auf die virtuelle Maschine „DC“
- Wechseln Sie auf das Fenster „Prüfpunkte“
- Wählen Sie den Prüfpunkt „Basis“ aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie „Anwenden“
- In der Abfrage wählen Sie „Anwenden“
- Warten Sie, bis der Prüfpunkt angewendet ist, dann können Sie die virtuelle Maschine neu starten
- Verfahren Sie für alle anderen virtuellen Maschinen genauso