Übung 32.1

- Richten Sie „Server3“ als RADIUS-Server ein
- Richten Sie „Server2“ als RADIUS-Client ein

Lösung 32.1

Installation der Rolle auf „Server3“

- Wechseln Sie zur virtuellen Maschine „Server3“
- Klicken Sie im „Server-Manager“ – „Dashboard“ auf „Rollen und Features hinzufügen“
    - Vorbemerkungen: Weiter
    - Installationstyp auswählen: Rollenbasierte oder featurebasierte Installation , Weiter
    - Zielserver auswählen: Server3.Meistertrainer.info, Weiter
    - Serverrollen auswählen:
        - Netzwerkrichtlinien- und Zugriffsdienste
        - Bestätigen Sie die benötigten Features
        - Weiter
    - Features auswählen
        - Weiter
    - Netzwerkrichtlinien- und Zugriffsdienste
        - Weiter
    - Bestätigung
        - Installieren
    - Installationsstatus
        - Schließen

Einrichten des Netzwerkrichtlinienservers und Definition des Radius-Clients

- Wechseln Sie zur virtuellen Maschine „Server3“
- Wählen Sie im Server-Manager
    - Tools
    - Netzwerkrichtlinienserver
- Navigieren Sie zu „Radius-Clients“
- Klicken Sie mit der rechten Maustaste
    - Neu
    - Einstellungen
        - Diesen RADIUS-Client aktivieren
        - Anzeigenname

        - Server2
    - Adresse
        - Server2
    - Gemeinsamer geheimer Schlüssel
        - 1234
        - Bestätigen
    - OK

Einrichten von „Server2“ als Radius-Client

- Wechseln Sie zur virtuellen Maschine „Server2“
- Wählen Sie im Server-Manager
    - Tools
    - Routing und RAS
- Rechte Maustaste auf „Server2“
    - Eigenschaften
- Registerkarte Sicherheit
    - Authentifizierungsanbieter
        - RADIUS-Authentifizierung
    - Konfigurieren
        - Hinzufügen
        - Servernamen
            - Server3
        - Gemeinsamer geheimer Schlüssel
            - Ändern
                - Neuer Schlüssel: 1234
                - Schlüssel bestätigen: 1234
                - OK
            - OK
        - OK

Übung 32.2

- Sie möchten Always On VPN einrichten, dafür installieren Sie eine Unternehmens-CA auf „Server1“
- Erstellen Sie drei Sicherheitsgruppen:
    - AlwaysOn Benutzer
        - Mitglied: Karl Klammer

- Always On NPS-Server
  - Mitglied: Server3
- Always On VPN-Server
  - Mitglied: Server2

- Konfigurieren Sie die „Default Domain Policy“ für „Autoenrollment“
- Erstellen Sie (als Beispiel für alle zu erstellenden Vorlagen) eine Vorlage für die VPN-Benutzerauthentifizierung
  - Name: Always On Benutzerauthentifizierung
- Registrieren Sie diese Vorlage

ACHTUNG!

Dies ist keine komplette Konfiguration für Always On VPN, eine komplette Konfiguration würde den Rahmen dieses Kurses sprengen!

- Setzen Sie die virtuellen Maschinen auf den Prüfpunkt „Basis“ zurück

Lösung 32.2

Installieren der CA auf „Server1“

- Wechseln Sie zur virtuellen Maschine „„Server1““
- Klicken Sie im „Server-Manager“ – „Dashboard“ auf „Rollen und Features hinzufügen“
  - Vorbemerkungen: Weiter
  - Installationstyp auswählen: Rollenbasierte oder featurebasierte Installation , Weiter
  - Zielserver auswählen: Server1.Meistertrainer.info, Weiter
  - Serverrollen auswählen: Active Directory Zertifikatdienste
    - Bestätigen Sie die benötigten Features
    - Weiter
  - Features auswählen: Weiter
  - AD-Zertifikatdienste: Weiter
  - Rollendienste auswählen
    - Zertifizierungsstelle
      - Benötigte Features bestätigen
    - Weiter
  - AD-Zertifikatdienste
    - Weiter
  - Rollendienste auswählen:

        - Zertifizierungsstelle
        - Weiter
    - Installationsauswahl bestätigen: installieren
- Klicken Sie nach Ende der Installation auf das gelbe Symbol im oberen Teil des Server-Managers
- Active Directory-Zertifikatdienste auf dem Zielserver einrichten
    - Anmeldeinformationen:
        - Weiter
    - Rollendienste:
        - Zertifizierungsstelle
        - Weiter
    - Installationstyp:
        - Unternehmenszertifizierungsstelle
        - Weiter
    - ZS-Typ:
        - Stammzertifizierungsstelle
        - Weiter
    - Privater Schlüssel:
        - Neuen privaten Schlüssel erstellen
        - Weiter
    - Kryptografie
        - Weiter
    - ZS-Name
        - Weiter
    - Gültigkeitsdauer
        - Weiter
    - Zertifikatdatenbank
        - Weiter
    - Bestätigung: Konfigurieren

Erstellen der Sicherheitsgruppen

- Bleiben Sie auf der virtuellen Maschine „Server1“
- Wählen Sie im Server-Manager
    - Tools
    - Active Directory-Benutzer und –Computer
- Navigieren Sie zu
    - Meistertrainer.info

    - Users
- Klicken Sie mit der rechten Maustaste
    - Neu
    - Gruppe
    - Gruppenname
        - Always On Benutzer
    - Gruppenbereich
        - Global
    - Gruppentyp
        - Sicherheit
    - OK
- Erstellen Sie auf die gleiche Art die Gruppen
    - Always On NPS-Server
    - Always On VPN-Server

Hinzufügen der Mitglieder

- Klicken Sie mit der rechten Maustaste auf die eben erstellte Gruppe „Always On Benutzer“
    - Eigenschaften
    - Registerkarte Mitglieder
        - Hinzufügen
        - Karl Klammer
        - Namen überprüfen
        - OK
    - Ok

- Klicken Sie mit der rechten Maustaste auf die eben erstellte Gruppe „Always On NPS-Server“
- Eigenschaften
- Registerkarte Mitglieder
    - Hinzufügen
    - Objekttypen
        - Haken setzen vor „Computer“
        - OK
    - Server3
    - Namen überprüfen
    - OK

- Fügen Sie auf die gleiche Art „Server2“ der Gruppe „Always On VPN-Server“ hinzu

„Default Domain Policy“ für „Autoenrollment“ konfigurieren

- Bleiben Sie auf der virtuellen Maschine „Server1“
- Wählen Sie im Server-Manager
    - Tools
    - Gruppenrichtlinienverwaltung
- Navigieren Sie zu
    - Domänen
    - Meistertrainer.info
    - Default Domain Policy
- Klicken Sie mit der rechten Maustaste
    - Bearbeiten
- Navigieren Sie zu
    - Computerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Sicherheitseinstellungen
    - Richtlinien für öffentliche Schlüssel
- Wählen Sie auf der rechten Seite des Fensters
    - Zertifikatclient – Automatische Registrierung
        - Konfigurationsmodell
            - Aktiviert
        - Haken vor
            - Abgelaufene Zertifikate erneuern…
        - Haken vor
            - Zertifikate, die Zertifikatvorlagen verwenden…
        - Ok
- Navigieren Sie zu
    - Benutzerkonfiguration
    - Richtlinien
    - Windows-Einstellungen
    - Sicherheitseinstellungen
    - Richtlinien für öffentliche Schlüssel
- Wählen Sie auf der rechten Seite des Fensters

- Zertifikatclient – Automatische Registrierung
  - Konfigurationsmodell
    - Aktiviert
  - Haken vor
    - Abgelaufene Zertifikate erneuern…
  - Haken vor
    - Zertifikate, die Zertifikatvorlagen verwenden…
  - Ok

Erstellen der Vorlage für die VPN-Benutzerauthentifizierung

- Bleiben Sie auf der virtuellen Maschine „Server1“
- Wählen Sie im Server-Manager
  - Tools
  - Zertifizierungsstelle
- Navigieren Sie zu
  - Meistertrainer-Server1-CA
  - Zertifikatvorlagen
- Klicken Sie mit der rechten Maustaste
  - Verwalten
- Klicken Sie auf der rechten Seite des Fensters mit der rechten Maustaste auf „Benutzer“
  - Vorlage duplizieren
- Registerkarte Kompatibilität
  - Zertifizierungsstelle
    - Windows Server 2012 R2
    - Bestätigen Sie die resultierenden Änderungen
  - Zertifikatempfänger
    - Windows 8.1/Windows Server 2012 R2
    - Bestätigen Sie die resultierenden Änderungen
- Registerkarte Allgemein
  - Vorlagenanzeigename
    - Always On Benutzerauthentifizierung
  - Haken entfernen vor
    - Zertifikat in Active Directory veröffentlichen
- Registerkarte Anforderungsverarbeitung
  - Haken entfernen vor
    - Exportieren von privatem Schlüssel zulassen

- Registerkarte Kryptografie
    - Anbieterkategorie
        - Schlüsselspeicheranbieter
    - Für Anforderungen muss einer der folgenden Anbieter verwendet werden
        - Microsoft Platform Crypto Provider
        - Microsoft Software Key Storage Provider
- Registerkarte Antragstellername
    - Haken entfernen vor
        - E-Mail-Name im Antragstellernamen
        - E-Mail-Name
- Registerkarte Sicherheit
    - Gruppen- oder Benutzernamen
        - Hinzufügen
        - AlwaysOn Benutzer
        - Namen überprüfen
        - OK
    - Berechtigungen für „AlwaysOn Benutzer“
        - Lesen
        - Registrieren
        - Automatisch registrieren
    - Gruppen- oder Benutzernamen
        - Domänen-Benutzer
            - Entfernen
    - OK

Registrieren der Vorlage

- Bleiben Sie auf „Server1“
- Wählen Sie im Server-Manager
    - Tools
    - Zertifizierungsstelle
- Navigieren Sie zu
    - Meistertrainer-Server1-CA
    - Zertifikatvorlagen
- Klicken Sie mit der rechten Maustaste
    - Neu
    - Auszustellende Zertifikatvorlage

    - Always On Benutzerauthentifizierung
- OK

Zurücksetzen der virtuellen Maschinen

- Wechseln Sie auf Ihre Hostmaschine
- Öffnen Sie den Hyper-V-Manager
- Klicken Sie im mittleren Fester 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