revobox office

Windows Server 2008 für die RADIUS-Authentisierung einrichten

Version 0.2

Windows Server 2008

Die aktuellste Version dieser Installationsanleitung ist verfügbar unter:
http://www.revosec.ch/files/windows-radius.pdf

Einleitung

Die *revobox* erlaubt das delegieren der Nutzerauthentisierung an einen externen Server über das RADIUS-Protokoll. Dabei können beliebige Authentisierungs-Methoden des EAP-Standards verwendet werden.

Eine typische Anwendung ist die Verwendung eines *Active Directory*® für die Authentisierung über EAP-MSCHAPv2. Somit können die zentralen Nutzerdaten verwendet werden, was die Administration für grössere Nutzergruppen wesentlich vereinfacht.

Diese Anleitung beschreibt die Einrichtung eines Windows Server® 2008 R2 über die Rolle *Network Policy Server* (NPS). Unter Windows Server 2003 heisst der Dienst *Internet Authentication Server* (IAS). Auf das Einrichten von IAS wird nicht im Detail eingegangen, die Installation läuft jedoch analog zu der Einrichtung von NPS ab.

Voraussetzungen

Um anhand dieser Anleitung die Authentisierung einzurichten, müssen folgende Voraussetzungen gegeben sein:

- Windows Server® 2008 R2 ist installiert
- Ein Active Directory® mit allen Diensten ist eingerichtet
- Nutzer sind im Active Directory® erfasst

Diese Anleitung richtet sich an erfahrene Administratoren von Windows Server® 2008. Es werden die Bezeichner einer englischen Installation verwendet.

Network Policy Server installieren

Der *Network Policy Server* erlaubt es dem Windows Server® 2008 als RADIUS-Server zu agieren. Gehen Sie folgendermassen vor, um den entsprechenden Dienst zu installieren:

- Starten Sie den Server Manager
- Fügen Sie eine neue Rolle hinzu
- Wählen Sie *Network Policy and Access Services*
- Lediglich der Dienst *Network Policy Server* wird benötigt

RADIUS-Client erfassen

Nach der Installation steht die Rolle *Network Policy and Access Services* zur Verfügung. Öffnen Sie daruntern den Baum *NPS -> RADIUS Clients and Servers -> RADIUS Clients*.

Hier werden verschiedenen RADIUS-Clients (NAS) erfasst, welchen die Authentisierung über RADIUS abwickeln dürfen. Fügen Sie einen neuen Eintrag hinzu. Definieren Sie einen Namen (*Friendly Name*), tragen Sie als IP-Adresse die Adresse der *revobox* ein und wählen Sie ein sicheres Passwort.

Tragen Sie in der *revobox* dasselbe Passwort zusammen mit der IP-Adresse oder dem DNS-Namen des Servers ein.

Connection Request Policy einrichten

Um Anfragen für die Authentisierung zu verarbeiten, ist eine *Connection Request Policy* erforderlich. Diese entscheidet, ob die Authentisierung überhaupt durchgeführt wird, und ob sie lokal oder an einen weiteren Server geleitet wird.

Öffnen Sie den Baum *NPS -> Policies -> Connection Request Policies*. Erstellen Sie eine neue Policy:

- Geben Sie der Policy einen Namen.
- Belassen Sie den NAS-Typ auf *Unspecified*.
- Nun muss mindestens eine *Condition* definiert werden, damit sich der Server für diese Policy entscheiden kann. Sie können hier den *NAS-Identifier* "revobox" oder alternativ auch den *Client Friendly Name* definieren, welcher Sie für den RADIUS-Client gesetzt haben.
- Wählen Sie eine Authentisierung auf dem lokalen Server und übernehmen Sie die weiteren Einstellungen wie vorgegeben.

Network Policy hinzufügen

Die eigentliche Authentisierung wird in einer *Network Policy* definiert. Anhand der hier definierten Regeln entscheidet der Server, wie die Authentisierung erfolgt.

Öffnen Sie den Baum *NPS -> Policies -> Network Policies*. Erstellen Sie eine neue Policy:

- Geben Sie der Policy einen Namen.
- Belassen Sie den NAS-Typ auf *Unspecified*.
- Nun muss wieder mindestens eine *Condition* definiert werden, damit sich der Server für diese Policy entscheiden kann. Sie können hier wiederum den *NAS-Identifier* "revobox" oder alternativ auch den *Client Friendly Name* definieren, welcher Sie für den RADIUS-Client gesetzt haben.
- Sie können weitere Kriterien definieren, wie etwa bestimmte Nutzergruppen oder zeitliche Einschränkungen.
- Erlauben Sie den Zugriff bei den *Access Permissions*.
- Optional können Sie den Zugriff abhängig von den Einstellungen des Nutzerkontos machen. Damit werden nur Nutzer akzeptiert, welchen in den Dial-In Einstellungen der Zugriff erlaubt wurde (*Network Access Permission*).
- Fügen Sie bei den Authentisierungs-Methoden den EAP-Typ EAP-MSCHAPv2 für die Passwort-Authentisierung hinzu. Entfernen Sie alle weniger sicheren Methoden im unteren Teil, diese sind für die EAP-Authentisierung nicht erforderlich.
- Übernehmen Sie alle weiteren Einstellung wie vorgeschlagen.

Beachten Sie, das zeitliche oder andere Restriktionen sich lediglich auf den Verbindungsaufbau beziehen, aktive Verbindungen sind dadurch nicht beeinflusst.

Nach Abschluss dieser Einstellungen ist die Authentisierung eingerichtet, alle nicht auf der revobox definierten Nutzer werden über das Active Directory® authentisiert.

Fehlersuche

Sollte die Authentisierung fehlschlagen, helfen die Events in der Rolle *Network Policy and Access Services* im *Server Manager* weiter.

revosec AG
Bungerstrasse 5
CH-7323 Wangs

Tel. 081 284 53 82
support@revosec.ch
www.revosec.ch