IEEE 802.1X-Authentifizierung

Kurzanleitung

Stand: 2022-05-27

05-31 04:44

1. IEEE 802.1X-Authentifizierung für eLux

Zertifikatbasierte Anmeldung mit 802.1X

IEEE 802.1X ist ein Standard zur Authentifizierung und Autorisierung in IEEE-802-Rechnernetzen. Die Authentifizierung eines Client-Gerätes (Supplicant) erfolgt am Netzwerkzugang eines LAN oder WLAN durch einen Authenticator. Der Authenticator kann ein IEEE 802.1X-fähiger Router oder WLAN-Access-Point sein. Der Authenticator überprüft die Authentifizierungsinformationen mit Hilfe eines Authentifizierungsservers (RADIUS).

Als RADIUS-Server können Sie beispielsweise den Microsoft Netzwerkrichtlinienserver (Network Policy Server, NPS) oder die freie Software freeRADIUS einsetzen.

Der Supplicant wird in Form einer Software-Implementierung umgesetzt. Wir unterstützen die freie Sofware **wpa_supplicant**.

Der Standard empfiehlt das Extensible Authentication Protocol (EAP) oder das PPP-EAP-TLS Authentication Protocol zur Authentifizierung.

Hinweis
Für die Zertifikatsverwaltung können Sie SCEP einsetzen. Eine entsprechende Implementierung für eLux ist verfügbar.

Zertifikatbasierte Anmeldung mit 802.1X und TPM 2.0

In Kombination mit SCEP können auf TPM 2.0-Geräten private Schlüssel im TPM 2.0-Modul gespeichert werden.[1] Um die Sicherheit der Authentifizierung noch weiter zu erhöhen, werden die kryptographischen Schlüssel ab eLux RP 6 2101 - bei Vewendung der entsprechenden Funktion -- im TPM 2.0-Modul eines Gerätes erzeugt und können weder angezeigt noch exportiert werden.

Für weitere Informationen siehe Zertifikate für SCEP in der **SCEP** Kurzanleitung.

[1] ab eLux RP 6.7

2. 802.1X für eLux konfigurieren

Hinweis
802.1X können Sie für LAN oder WLAN konfigurieren. Die Vorgehensweise unterscheidet sich in der Ablage der Konfigurationsdatei und einigen Parametern. Für weitere Informationen siehe WPA-Supplicant konfigurieren.

1. Stellen Sie sicher, dass das eLux-Paket **WLAN drivers** und das hierin enthaltene Feature-Paket **WPA supplicant** auf den Clients installiert ist. Dies kann eine Anpassung der Image-definitions-Datei am Webserver mit Hilfe von ELIAS erfordern.
2. Übertragen Sie die benötigten Zertifikate mit der Scout-Funktion Dateien auf die Clients nach `/setup/cacerts`.

   Hinweis
   Die Zertifikate Ihrer RADIUS-Umgebung benötigen als Common Name (CN) den FQDN.

3. Konfigurieren Sie die Datei `wpa.conf` und übertragen Sie die Datei anschließend mit der Scout-Funktion Dateien auf die Clients. Für weitere Informationen siehe WPA-Supplicant konfigurieren.
4. Wenn Sie SCEP verwenden, können Sie die Datei `wpa.conf` alternativ über die Vorlage `wpa.conf.scep` generieren lassen. Für weitere Informationen siehe WPA-Konfiguration über Vorlage.
5. Nur für LAN: Aktivieren Sie in der Scout Console, für die relevante OU, in der Geräte-Konfiguration unter **Netzwerk > LAN > Erweitert > IEEE 802.1X-Authentifizierung** die Option **Aktivieren**.

Wenn die Konfiguration korrekt ist und die benötigten Zertifikate ausgerollt sind, können Sie Geräte am 802.1X-Port verwenden.

2.1. WPA-Supplicant konfigurieren

Hinweis
Für die Konfigurationsdatei des WPA-Supplicant finden Sie Beispieldateien auf den Clients: `/setup/scep/wpa.conf.*`

1. Erstellen Sie eine individuelle Konfigurationsdatei `wpa.conf`.

   Standardmäßig enthält die Datei folgende Angaben:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=0
network={
    key_mgmt=IEEE8021X
    eapol_flags=0
    eap=TLS
    identity="<Common Name wie im Zertifikat angegeben>"
    priority=6
    ca_cert="/setup/cacerts/scep/serverca.pem"
    client_cert="/setup/cacerts/scep/client.pem"
    private_key="/setup/cacerts/scep/client.key"
        }
```

   Fügen Sie weitere Einträge entsprechend Ihrer CA-Implementierung hinzu.

   Die Zertifikatsdatei mit Pfad können Sie wie im Beispiel unten angeben, beispielsweise wenn Sie auf eine externe Stammzertifizierungsstelle zugreifen. Beachten Sie, dass nur eine Datei über `ca_cert` referenziert werden darf. Diese Datei darf jedoch mehrere Zertifikat-Einträge enthalten.

```
ca_cert="/setup/cacerts/<root_extern>.pem"
ca_cert="/setup/cacerts/<subordinate_int>.pem"
ca_cert="/setup/cacerts/<radius>.ssl"
```

   Wenn das RADIUS-Zertifikat statt FQDN den NetBIOS-Namen enthält, verwenden Sie beispielsweise folgenden Eintrag:

```
ca_cert="/setup/cacerts/<root>.pem"
```

   Achtung Die Groß-/Kleinschreibung der Zertifikat-Dateinamen muss mit der Schreibweise der übertragenen Zertifikat-Dateien übereinstimmen.

2. Wenn Sie TPM 2.0 über WLAN nutzen möchten, geben Sie für das Netzwerk zusätzlich folgende **engine**-Parameter an:[1]

```
...
network={
    ssid="WLAN-ABC"
    scan_ssid=1
    key_mgmt=WPA-EAP
    proto=WPA2
    eap=TLS
    engine=1        # Wert muss immer 1 sein
    engine_id="tpm2tss"    # Private Key wird aus TPM 2.0-Modul genommen
    dentity="__IDENTITY__"
    priority=6
    ca_cert="/setup/cacerts/scep/serverca.pem"
    client_cert="/setup/cacerts/scep/client.pem"
    private_key="/setup/cacerts/scep/client.key"    # Öffentlicher Teil
}
```

3. Übertragen Sie die Konfigurationsdatei `wpa.conf` mit Hilfe der Scout- Funktion **Konfigurierte Dateiübertragung** auf die Clients in folgendes Verzeichnis:

LAN	`setup/scep/`
WLAN	`setup/wlan/`

Für weitere Informationen siehe Erweiterte Geräte-Konfiguration > Dateien im **Scout**-Handbuch.

Verwendung mehrerer WLAN-Netze

- Um mehrere SSIDs nutzen zu können, setzten Sie den **network**-Eintrag mehrfach.

Beispiel:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=1
network=
{ ssid="" scan_ssid=1 key_mgmt=WPA-EAP eap=TLS identity="" priority=5 ca_cert="" ca_cert=""
client_cert="" private_key="" }
network=
{ ssid="" scan_ssid=1 key_mgmt=WPA-EAP eap=TLS identity="" priority=6 ca_cert="" ca_cert=""
client_cert="" private_key="" }
```

[1] ab eLux RP 6 2103

Einsatz von Variablen

Für `identity` und `hostname` können Sie alternativ Variablen setzen:[1]

Schreibweise	Beschreibung	Bemerkung
`%IDENTITY%`	Common name aus dem Zertifikat	Die alte Schreibweise vor eLux RP 6.9.100 (Variablenname in Großbuchstaben und 2 x 2 Unterstriche) wird aus Kompatibilitätsgründen weiter unterstützt. Beispiel: `__IDENTITY__`
`%HOSTNAME%`	Hostname aus `terminal.ini`	

Variablen dürfen auch für einen Teil eines Wertes verwendet werden.[2] Präfixe und Suffixe einer Variable sind reine Zeichenfolgen, die durchgereicht werden.
Beispiel: `identity="host/%HOSTNAME%"`

Für weitere Informationen zur 802.1X-Konfiguration für WLAN siehe WPA-Unterstützung im **Scout**-Handbuch.

[1] ab eLux RP 6.9
[2] ab wlandrivers 10.2, enthalten ab eLux RP 6.9.100 und eLux RP 6.10

2.2. WPA-Konfiguration über Vorlage (SCEP)

- nur bei Verwendung von SCEP -

Hinweis
Die folgenden Informationen beziehen sich nur auf die Konfiguration von 802.1X für LAN.

Wenn Sie SCEP einsetzen, können Sie die auf den Clients bereitgestellte Vorlage `/setup/scep/wpa.conf.scep` verwenden:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=0
network={
    key_mgmt=IEEE8021X
    eapol_flags=0
    eap=TLS
    identity="%IDENTITY%"
    ca_cert="/setup/cacerts/scep/serverca.pem"
    client_cert="/setup/cacerts/scep/client.pem"
    private_key="/setup/cacerts/scep/client.key"
        }
```

Hinweis
Die Variable `%IDENTITY%`[1] wird durch den CN des Client-Zertifikats ersetzt.

Der Client wertet diese Vorlage aus und erstellt die Datei `wpa.conf`, wenn folgende Bedingungen erfüllt sind:

- SCEP ist für den Client in der `terminal.ini` konfiguriert. Für weitere Informationen siehe SCEP für eLux-Clients konfigurieren in der SCEP-Anleitung.
- Es ist keine individuelle `/setup/scep/wpa.conf` vorhanden.

Wenn erforderlich passen Sie die Vorlage an und übertragen sie mit Hilfe der Scout-Funktion **Konfigurierte Dateiübertragung** auf die Clients nach `/setup/scep/wpa.conf.scep`. Beachten Sie, dass eine eventuell vorhandene individuelle `/setup/scep/wpa.conf`[2] Vorrang hat.

Hinweis
Die aus der Vorlage generierte `wpa.conf` wird in einem temporären Verzeichnis erstellt und ist nur über die Diagnosedateien zu sehen.

[1] Alte Schreibweise: `__IDENTITY__`
[2] siehe WPA-Supplicant konfigurieren

3. Diagnose für 802.1X

Client-Zertifikat in einer Shell angezeigen

- Verwenden Sie folgendes Kommando:
  `openssl x509 -in /setup/cacerts/scep/client.pem -noout -text`

Alle Informationen des Zertifikats werden angezeigt.

Protokolldateien anzeigen

1. Schalten Sie die erweitere Protokollierung ein.
2. Fordern Sie die Diagnosedateien an. Für weitere Informationen siehe Diagnosedateien anfordern im Scout-Handbuch.

`/tmp/systemd-journal.log`	Protokolldatei für Netzwerk-Aktivitäten[1]

[1] ab eLux RP 6.4