Konfigurieren von Cisco DCM - Support für Remote-Authentifizierung

Inhalt

Einführung

Dieses Dokument beschreibt die Cisco Digital Content Manager (DCM)-SoftwareRemote-Authentifizierung mithilfe von RADIUS.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der Cisco DCM-Software, Version 16 und höher, zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco DCM-Software v16.10 und höher
- RADIUS-Server mit freierRadius Open-Source-Software.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In V16.10 des DCM wurde eine neue Funktion eingeführt, mit der auf einem RADIUS-Server

konfigurierte Benutzerkonten für den Zugriff auf die DCM-GUI verwendet werden können. Dieses Dokument beschreibt die für den DCM und den RADIUS-Server erforderliche Konfiguration, um diese Funktion nutzen zu können.

GUI-Konten auf DCM

In Version 16.0 und niedriger waren die Benutzerkonten, die für den Zugriff auf die GUI erforderlich waren, lokal für den DCM, d. h., sie wurden auf dem DCM erstellt, geändert, verwendet und gelöscht.

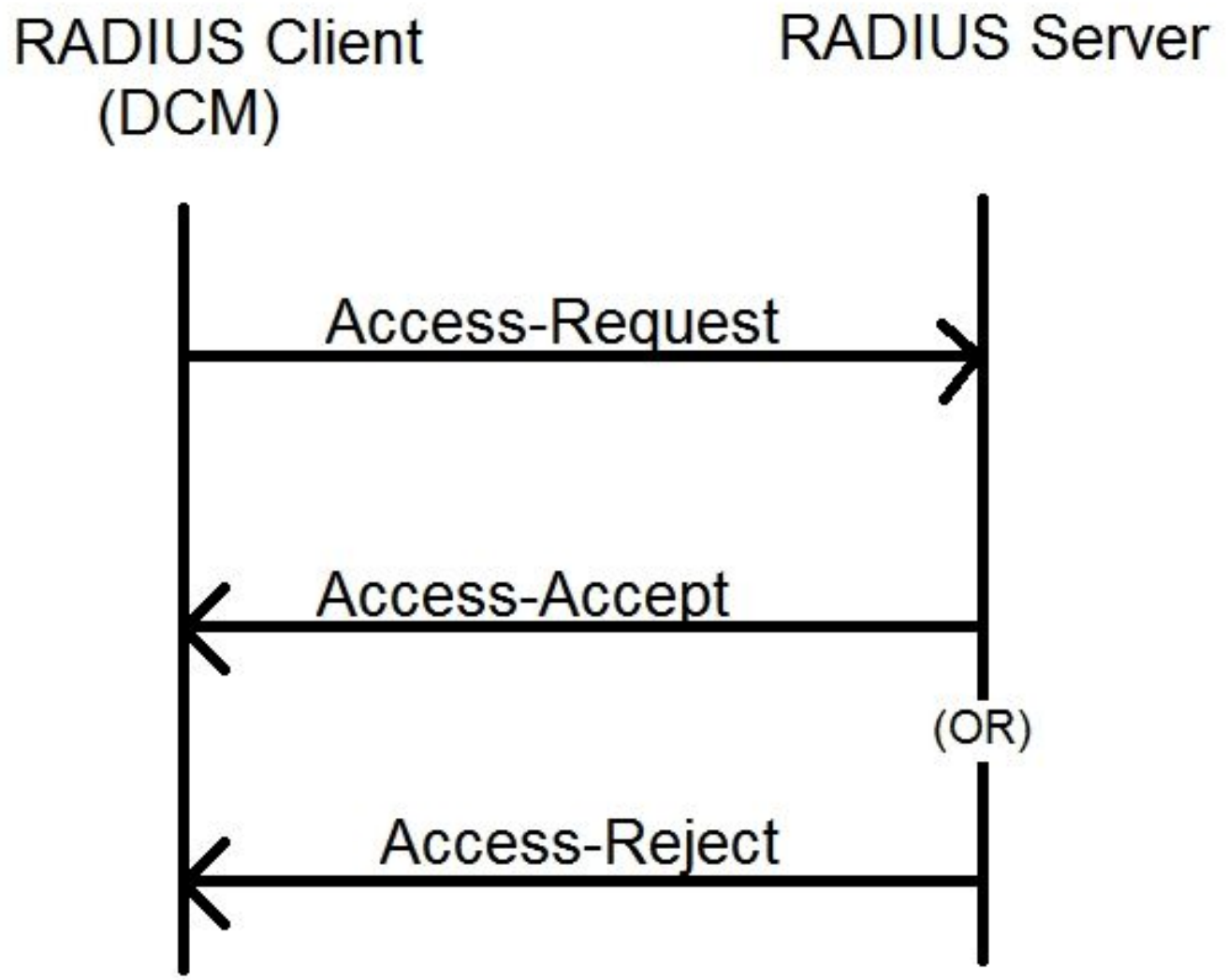
Ein GUI-Benutzerkonto kann einer der folgenden Gruppen angehören:

- Administratoren (Vollzugriff)
- Benutzer (Lese- und Schreibzugriff)
- Gäste (schreibgeschützt)
- Automatisierungsauslöser (externe Trigger)
- DTF-Administratoren (DTF-Schlüsselkonfiguration)

Remote-Authentifizierung

Die Idee der Remote-Authentifizierung besteht in einer zentralisierten Sammlung von Benutzerkonten, die für den Zugriff auf ein Gerät, eine Anwendung, einen Dienst usw. verwendet werden können.

In den Schritten, die im Bild gezeigt werden, wird erläutert, was bei der Verwendung der Remoteauthentifizierung geschieht:



Schritt 1: Der Benutzer gibt auf der Anmeldeseite der DCM-GUI den Anmeldenamen und das Kennwort (auf dem RADIUS-Server konfiguriertes Benutzerkonto) ein.

Schritt 2: Der DCM sendet eine Zugriffsanfrage mit den Anmeldeinformationen an den RADIUS-Server.

Schritt 3: Der RADIUS-Server überprüft, ob die Anforderung von einem der konfigurierten Clients stammt, und ob das Benutzerkonto in seiner DB/Datei vorhanden ist, und überprüft, ob das Kennwort korrekt ist oder nicht. Danach wird eine der folgenden Meldungen an den DCM zurückgegeben

- Access-Accept - Das bedeutet, dass die Anmeldeinformationen gültig sind. Die konfigurierten RADIUS-Attribute werden zurückgegeben.
- Access-Reject (Access-Reject): Dies bedeutet, dass die Anmeldeinformationen ungültig sind und der RADIUS-Server möglicherweise so konfiguriert ist, dass er einige RADIUS-Attribute sendet, um den Fehler zu melden.
- Access-Challenge - Das bedeutet, dass der RADIUS-Server einige zusätzliche Informationen benötigt, um die Authentizität des Benutzers zu überprüfen. Nicht im DCM verarbeitet.

Falls der RADIUS-Server eine Access-Reject sendet, prüft der DCM, ob das Benutzerkonto beim DCM selbst lokal ist, und es werden die Authentifizierungsverfahren befolgt.
Der Benutzer wird in einem Intervall von 15 Minuten (intern) erneut authentifiziert, um sicherzustellen, dass der Benutzername/das Kennwort noch gültig ist und der Benutzer zu einer der GUI-Kontengruppen gehört. Wenn die Authentifizierung fehlschlägt, gilt die aktuelle Benutzersitzung als ungültig und alle Berechtigungen werden für den Benutzer widerrufen.

Konfigurieren des RADIUS-Servers

Um die auf dem RADIUS-Server vorhandenen Benutzerkonten für den Zugriff auf die GUI zu verwenden, müssen die folgenden Schritte ausgeführt werden:

DCM sollte als Client für den RADIUS-Server konfiguriert werden.

1. Fügen Sie die IP-Adresse des DCM als Client für den RADIUS-Server hinzu.

2. Fügen Sie der Client-Konfiguration den gemeinsamen geheimen Schlüssel hinzu (dieser geheime Schlüssel muss mit dem auf dem DCM konfigurierten geheim sein, siehe Abschnitt Konfigurieren des DCM).

3. Es wird empfohlen, für jeden DCM einen anderen gemeinsamen geheimen Schlüssel zu verwenden.

4. Die Länge des gemeinsam genutzten Geheimhaltungsgrades muss mindestens 22 Zeichen lang sein.

5. Das gemeinsame Geheimnis sollte so zufällig wie möglich sein.

   Beispiel für einen guten gemeinsamen geheimen Schlüssel:
   "89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345"

Für ein Benutzerkonto sollte die Access-Accept-Nachricht vom RADIUS-Server über ein RADIUS-Attribut verfügen, das die GUI-Kontengruppe identifiziert, der der Benutzer angehört. Der Attributname kann ausgewählt werden und muss in der Einstellungsdatei des DCM konfiguriert werden.

Dies ist das Format der Zeichenfolge, die als Wert für ein Attribut vom RADIUS-Server gesendet werden muss:

OU=<group_name_string> group_name_string kann eine der folgenden sein:

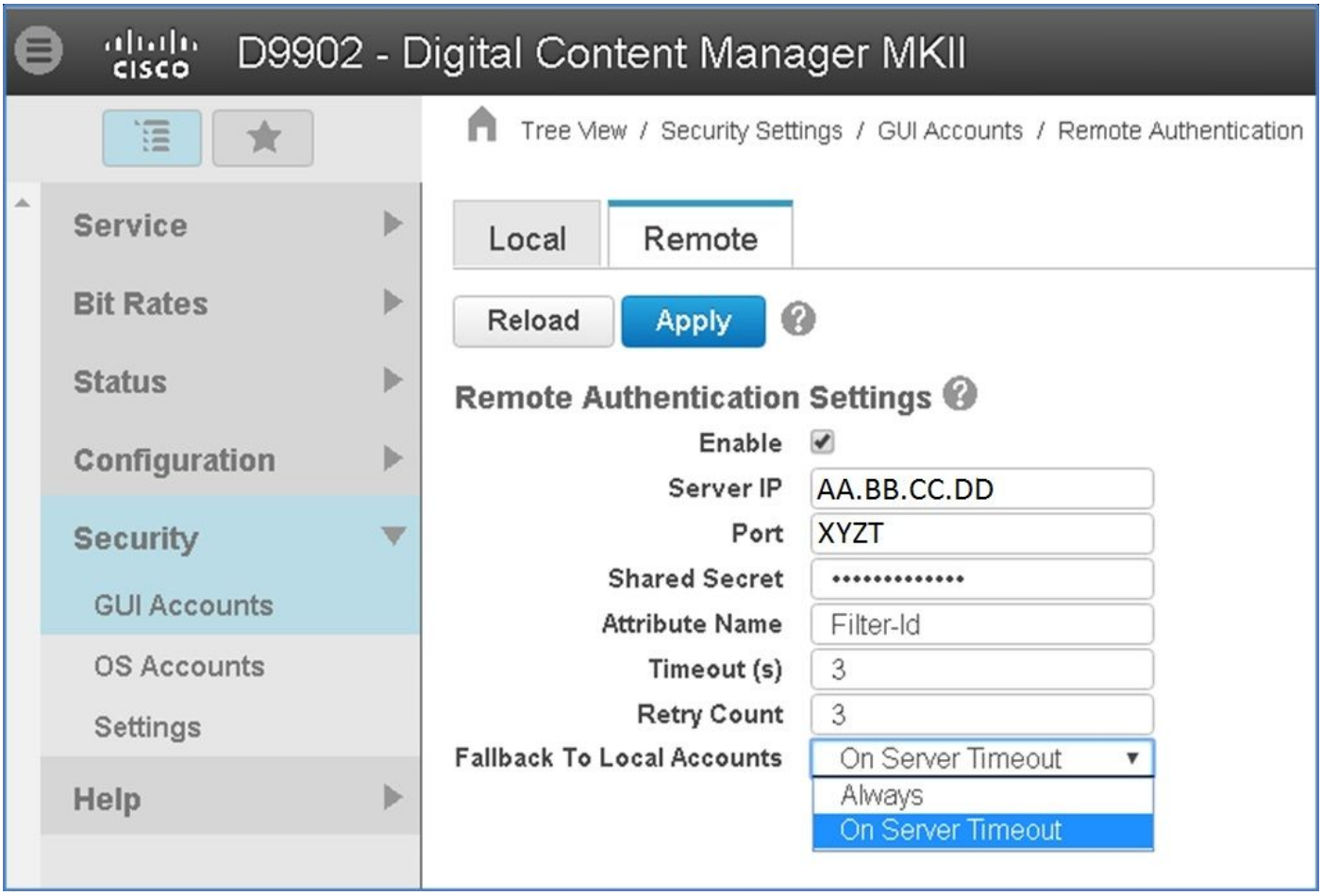
Gruppe	Gruppenname
Administratoren (Vollzugriff)	Administratoren
Benutzer (Lese- und Schreibzugriff)	Benutzer
Gäste (schreibgeschützt)	Gäste
Automatisierungsauslöser (extern) Trigger)	Automatisierung
DTF-Administratoren (DTF-Schlüssel) Konfiguration)	Dtfadmins

Konfigurieren von Cisco DCM

Zum Aktivieren/Konfigurieren der Remote-Authentifizierungsfunktion des DCM ist ein GUI-Administratorkonto erforderlich.
In diesen Schritten wird die Konfiguration der Remote-Authentifizierung beschrieben:

Schritt 1: Melden Sie sich mit dem Administratorkonto beim DCM an.

Schritt 2: Navigieren Sie zu **Security > GUI Accounts (Sicherheit > GUI Accounts),** und wählen Sie die **Remote** Registerkarte aus, wie im Bild gezeigt:



Schritt 3: Konfigurieren Sie die für die RADIUS-Kommunikation erforderlichen Parameter:

- Aktivieren - Diese Einstellung bestimmt, ob die Unterstützung für Remote-Authentifizierung aktiviert werden soll. Bei Überprüfung sind die übrigen Parameterfelder aktiviert.
- Server-IP - IP-Adresse des RADIUS-Servers.
- Port - Port, an dem der RADIUS-Server Authentifizierungspakete überwacht (im Allgemeinen 1812, aber für andere Werte konfiguriert werden kann).
- Secret (Geheim) - Dies ist der geheime Schlüssel, der zum Verschlüsseln des Kennworts verwendet wird, bevor das RADIUS-Paket an den Server gesendet wird. Dieser geheime Schlüssel muss mit dem auf dem RADIUS-Server konfigurierten geheim sein, auf dem das

Kennwort entschlüsselt wird.

- Attributname: Der Name des Attributs, in dem die Autorisierungsdaten vom RADIUS-Server empfangen werden.

- Timeout (in Sekunden) - Diese Einstellung wird für die Kommunikation zwischen dem RADIUS-Server und dem DCM verwendet. Dies ist die Zeit, in der der DCM auf eine Antwort des RADIUS-Servers auf eine bestimmte Anforderung warten muss, bevor die Anforderung beendet wird.

- Wiederholungsanzahl - Die Anzahl der Male, die die RADIUS-Anforderung gesendet werden muss, wenn vorherige Anforderungen das Zeitlimit überschreiten.

- Fallback an lokale Konten: Diese Einstellung ist ab DCM Version 19.0 verfügbar. Der DCM ermöglicht die Anmeldung über ein GUI-Konto (lokal), das über die GUI erstellt wird. Option: **Bei Server-Timeout** können Sie auf die lokalen Konten zurückgreifen, falls der Radius-Server nicht erreicht werden kann, und nicht, wenn die Authentifizierung fehlschlägt. Option, **Always** ermöglicht das Fallback immer - auch wenn die Authentifizierung fehlschlägt.

Schritt 4: Während der Änderungen wird die im Bild angezeigte Warnung angezeigt. Klicken Sie auf **OK**, und die Benutzeroberfläche wird neu gestartet.

Schritt 5: Jetzt ist DCM für die Remote-Authentifizierung bereit.

Konfigurieren von IPSec auf DCM:

1. Melden Sie sich mit einem GUI-Konto, das der Sicherheitsgruppe Administratoren angehört, beim DCM an.

2. Navigieren Sie zu **Konfiguration > System**. Die Seite Systemeinstellungen wird angezeigt.

3. Weitere Informationen finden Sie im Bereich **Add New IPsec** (Neue IPsec hinzufügen), wie im Bild gezeigt.

4. Geben Sie im Feld IP Address (IP-Adresse) die IP-Adresse des neuen IPsec-Peers (RADIUS-Server) ein.

5. Geben Sie in den Feldern **Vorinstallierter** Schlüssel und *Vorinstallierter Schlüssel* erneut den *Vorinstallierten Schlüssel* für den neuen IPsec-Peer ein.

6. Klicken Sie auf **Hinzufügen**. Der neue IPsec-Peer wird der Tabelle mit den IPsec-Einstellungen hinzugefügt.

> **Hinweis**: Informationen zur Konfiguration von IPSec auf dem System, auf dem der RADIUS-Server ausgeführt wird, finden Sie in der Dokumentation/Veröffentlichung des Produkts.

Sicherheitsüberlegungen

- Der gemeinsam genutzte geheime Schlüssel wird im Klartext im Dateisystem des DCM gespeichert.
- Das verschlüsselte Kennwort wird im Speicher des DCM gespeichert und kann während der Sitzung zur erneuten Authentifizierung verwendet werden.
- Angesichts der beiden obigen Punkte wird empfohlen, die Zugriffsrechte der Fehlerbehebung auf den DCM zu beschränken.
- Es wird dringend empfohlen, IPSec zum Sichern des Kommunikationskanals zwischen DCM und RADIUS zu verwenden.
  Server.

Einschränkungen und Einschränkungen

- Die Unterstützung für die Remote-Authentifizierung ist nur für GUI-Konten verfügbar, nicht für die Betriebssystemkonten.
- Eine erneute Authentifizierung erfolgt in einem Intervall von 15 Minuten. Beispiel: Wenn die Benutzergruppe geändert wurde, dauert die Zeit bis zur Änderung im schlimmsten Fall 15 Minuten.

- Wenn die Remote-Authentifizierung aktiviert ist, prüft der DCM zunächst mit dem RADIUS-Server, ob das Benutzerkonto gültig ist oder nicht, und prüft dann die lokale Datenbank. Bei Verwendung von lokalen Konten, die nicht auf dem RADIUS-Server vorhanden sind, wird auf dem RADIUS-Server eine Fehlermeldung bezüglich der Authentifizierung angezeigt.

Einrichten von freeRadius

In diesem Abschnitt wird beispielhaft veranschaulicht, wie Sie freeRadius als Remote-Authentifizierungsserver für den DCM einrichten. Dies dient nur zu Informationszwecken.

FreeRadius wird von Cisco weder bereitgestellt noch unterstützt. Es wird davon ausgegangen, dass die Konfigurationsdateien für freeRadius unter **/etc/freeRadius/** (Distribution überprüfen) gefunden werden.

Nach der Installation des freeRadius-Pakets können Sie diese Dateien ändern.

- Ändern Sie die **/etc/freeradius/clients.conf**
  Schritt 1: Fügen Sie der Liste der Clients einen Eintrag für die IP-Adresse des DCM hinzu.
  Schritt 2: Fügen Sie den freigegebenen Schlüssel in die Clientkonfiguration ein, und belassen Sie die anderen Parameter standardmäßig.

  Es wird empfohlen, für jeden DCM einen eindeutigen gemeinsamen geheimen Schlüssel zu verwenden.
  Die Länge des gemeinsam genutzten Geheimhaltungsgrades muss mindestens 22 Zeichen lang sein. Das gemeinsame Geheimnis sollte so zufällig wie möglich sein.

  Beispiel für einen guten gemeinsamen geheimen Schlüssel:
  "89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345"

- Ändern Sie den Befehl **/etc/freeradius/radiusd.conf**, um den Port zu ändern, an dem der Radius-Server lauschen soll (im Allgemeinen 1812).

- Ändern Sie das **/etc/fretilus/users**, um neue Benutzer hinzuzufügen.

- Stellen Sie sicher, dass das RADIUS-Attribut hinzugefügt wird, in dem die Autorisierungsinformationen in diesem Format an den DCM gesendet werden:
  <Attributname> = '**OU=<group_name>'**

  Attributname: Dabei handelt es sich um den Namen des RADIUS-Standardattributs, über das die Autorisierungsdaten an die DCM-Gruppe_Name gesendet werden. Dabei kann es sich um Folgendes handeln:
  Administratoren - Ein Benutzer, der zu dieser Gruppe gehört, verfügt über Administratorrechte, d. h. volle Kontrolle.
  Benutzer - Ein Benutzer, der zu dieser Gruppe gehört, verfügt über Lese- und Schreibrechte.

Gäste - Ein Benutzer, der dieser Gruppe angehört, hat nur Leseberechtigung.
Automatisierung - wird für Automatisierung (externe Trigger) verwendet.
dtfadmins - DTF-Administrator (DTF-Schlüsselkonfiguration)

Beispiel:
Steve Cleartext-Password := "testing"
Filter-ID = "OU=Administratoren"

- (Re)starten Sie den Radius-Server, damit die Änderungen wirksam werden.

- Stellen Sie sicher, dass die Firewall-Konfiguration des Radius-Servers den externen Zugriff auf die ausgewählte Firewall ermöglicht.
Port.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Für Debugzwecke wurden einige zusätzliche Protokolle in das Sicherheitsprotokoll aufgenommen. Um dieses Protokoll anzuzeigen, navigieren Sie in der DCM-GUI zu **Help > Traces page**.

Dieser Abschnitt beschreibt, was in den Protokollen gesucht werden sollte, welche Probleme auftreten könnten und welche Lösungen möglich sind.

Protokollzeile	Fehler beim Remote-Anmeldeversuch: Die Anfrage an den RADIUS-Server wurde zeitlich abgelaufen.
Problem	DCM kann nicht mit dem RADIUS-Server kommunizieren.
Mögliche Lösung	• Überprüfen Sie, ob die IP-Adresse des RADIUS-Servers, die in der Remote-Authentifizierungskonfiguration des DCM angegeben ist, korrekt ist. • Stellen Sie sicher, dass der Zugriff auf den RADIUS-Server vom DCM aus möglich ist. • Stellen Sie sicher, dass der DCM als gültiger Client auf dem RADIUS-Server konfigurie (der RADIUS-Server verwirft unbemerkt Access-Request-Pakete von unbekannten Clients). • Stellen Sie sicher, dass der auf dem DCM konfigurierte geheime Schlüssel dem auf de RADIUS-Server für diesen DCM konfigurierten gemeinsamen geheimen Schlüssel entspricht. (Wenn der Server keinen gemeinsamen geheimen Schlüssel für den Client besitzt, wird die Anforderung unbemerkt verworfen.)
Protokollzeile	Remote-Anmeldeversuch fehlgeschlagen: [Errno 10054] Eine bestehende Verbindung wurd vom Remote-Host zwangsweise geschlossen.
Problem	Der DCM hat eine RADIUS-Anforderung an die angegebene Server-IP gesendet. Die RADI Serveranwendung überwacht jedoch nicht den Port, der in den Remote-Authentifizierungseinstellungen angegeben ist.
Mögliche Lösung	• Stellen Sie sicher, dass der RADIUS-Server ausgeführt wird.

	• Überprüfen Sie, ob die in der RADIUS-Konfiguration des Servers angegebene Portnummer mit der auf dem DCM konfigurierten Nummer übereinstimmt.
Protokollzeile	Fehler beim Remote-Anmeldeversuch: Ungültiger Attributname angegeben oder Antwort vo fehlenden Autorisierungsdaten des RADIUS-Servers.
Problem	Es liegt ein Problem mit der Antwort des RADIUS-Servers vor.
Mögliche Lösung	• Stellen Sie sicher, dass der RADIUS-Server das Attribut (auf dem DCM konfiguriert) in Antwort "Access-Accept" sendet.
Mögliche Lösung	• Stellen Sie sicher, dass der Parameter **Attributname**, der auf den DCM-Remote-Authentifizierungseinstellungen konfiguriert wurde, dem in der Benutzerkonfiguration au dem RADIUS-Server angegebenen Namen entspricht.
Protokollzeile	Ungültige Autorisierungsdaten, die vom RADIUS-Server empfangen wurden.
Problem	Die Authentifizierung war erfolgreich, aber die vom RADIUS-Server erhaltene Antwort enthä ungültige Autorisierungsdaten, d. h. den Namen der Sicherheitsgruppe.
Mögliche Lösung	• Stellen Sie sicher, dass der auf dem RADIUS-Server für diesen Benutzer konfigurierte Gruppenname einer der im Abschnitt Konfigurieren von RADIUS Server angegebenen Sicherheitsgruppennamen ist.
Mögliche Lösung	• Stellen Sie sicher, dass das Format der auf dem RADIUS-Server konfigurierten Zeichenfolge dem im Abschnitt Konfigurieren des RADIUS-Servers angegebenen Form entspricht.