Produktinformation

netADIT V6.1.0

netADIT

Ein Software-Produkt von

TR-Tec®

Inhalt

Was ist netADIT?

netADIT ist eine modular aufgebaute PHP8-Anwendung zum Einsatz auf Linux um Benutzer für eine freeRadius- und openLDAP-Authentifizierung zu verwalten. Je nach installierten Modulen bietet es die Möglichkeit verschiedenste Linux-Programme einfach zu verwalten und/oder zu benutzen. Somit wird ein einfaches und effizientes Verwalten von reinem Gästemanagement bis hin zu einer fein justierbaren NAC-Lösung möglich.

Konzept

In netADIT wird zwischen „administrativen Benutzern" und „Gästebenutzern" unterschieden. Administrative Benutzer werden beim Erstellen sofort aktiv und können sich an der Administrationsoberfläche von netADIT anmelden um Gästebenutzer zu administrieren. Gästebenutzer bieten nur die Möglichkeit einer freeRadius- oder LDAP-Anmeldung, jedoch keine Anmeldung am netADIT AdminGUI und werden nur für einen definierten Zeitraum als gültige Benutzer im System geführt. Durch die Möglichkeit der Installation zusätzlicher Module ergibt sich ein breit gefächertes Einsatzgebiet beginnend bei der einfachen Radius-Authentifizierung durch Switches, APs, ... bis hin zur kompletten HotSpot-Implementierung.

Technologie

netADIT ist eine auf Linux basierte PHP8 Applikation, welche im täglichen Betrieb zur Gänze über ein webbasiertes GUI die einfache Administration von openLDAP- und MariaDB-Benutzerdaten ermöglicht. Zusätzlich sind noch CLI-Programme zur Administration von Basisfunktionen vorhanden.

Software

Der Einsatz von netADIT setzt zumindest ein minimal installiertes Linux-Betriebssystem inklusive der Software openLDAP, MariaDB, freeRadius, Apache2, PHP8.2 inklusive CLI-Version und den IonCube-Loader voraus. Zugesichert unterstützte Distributionen sind:

- AlmaLinux 9.x
- Red Hat Enterprise Linux (RHEL) 9.x

INFO

Die Systemvoraussetzungen beziehen sich auf eine Basisinstallation. Im Falle einer Implementierung inklusive aller Module müssten noch weitere Module nachinstalliert werden.

Hardware

Für den Einsatz von netADIT gibt es keine speziellen Hardwareanforderungen, es sollte jedoch berücksichtigt werden, dass mit steigender gleichzeitig aktiver Useranzahl des WebGUI dementsprechende Ressourcen braucht. Ebenfalls ein entscheidender Aspekt sind die gleichzeitigen Zugriffe der Gästebenutzer, welche gegen openLDAP und freeRadius authentifiziert werden. Ab einer gewissen

Größenordnung ist zumindest die Auslagerung der openLDAP- und MySQL-Datenbank auf ein sehr performantes Plattensubsystem empfehlenswert.

Benutzerrollen

Wie bereits zuvor erwähnt unterscheidet netADIT zwischen den Benutzerarten „administrative Benutzer" und „Gästebenutzer". Um die Berechtigungen von administrativen Benutzern abzugrenzen nutzt netADIT ein Rollenkonzept mit folgenden drei Benutzerrollen:

- **netADIT SuperUser:** Benutzer dieser Rolle haben alle Rechte im System, können Logdateien uneingeschränkt ansehen und alle Arten von Benutzern administrieren.
- **netADIT Administrator:** Benutzer dieser Rolle haben das Recht, administrative Benutzer der Rolle „netADIT Operatoren" so wie Gästebenutzer zu administrieren.
- **netADIT Operator:** Benutzer dieser Rolle haben das Recht Gästebenutzer zu administrieren.

Aufbau des netADIT AdminGUI

netADIT bietet je nach installierten Modulen verschiedenste Menüpunkte, wobei diese im Grunde auf zwei Bereiche zu reduzieren sind:

- Benutzerbereich
- Administrationsbereich

Um diese Bereiche nutzen und somit netADIT administrieren zu können muss ein erfolgreicher Login mit gültigem, administrativem Benutzer stattfinden. Je nach Rolle, die dem Benutzer zugewiesen ist, sind Menüpunkte sichtbar oder nicht und stehen Funktionen zur Administration zur Verfügung.

Administrationsbereich

Der Administrationsbereich beinhaltet alle administrativen Module inklusive der Systemkonfiguration, Benutzerverwaltung und Logansicht für administrative Benutzer. Dieser Bereich ist nur verfügbar für Benutzer der Rollen „netADIT SuperUser" oder „netADIT Administratoren".

INFO

In diesem Bereich angelegte Benutzer sind so genannte „administrative Benutzer" und können sich nicht im Gästenetz anmelden.

Benutzerbereich

Der Benutzerbereich beinhaltet die für (Gäste-)Benutzer und Geräte relevanten Module die je nach Lizenzierung die folgenden sind:

- **Zeitraum Gastbenutzer**: Dem Gast wird Startdatum/Startzeit und Enddatum/Endzeit zugewiesen. Dieser kann sich nur in dem definierten Zeitraum am Gästesystem anmelden und wird nach Ablauf automatisch aus dem System gelöscht. (Modul naTimeframe)
- **Persistente Gastbenutzer**: Der Gast hat keine zeitliche Limitierung, kann aber die Stati aktiv oder inaktiv besitzen. Nur aktive Gäste können sich am System anmelden. (Modul naPersist)
- **Zeitlimit Gastbenutzer**: Dem Gast wird eine Netto-Zeit in Minuten zugewiesen. Nach Verbrauch der Zeit wird der Gast automatisch abgemeldet und deaktiviert. (Modul naTimelimit)
- **MacAuth Benutzer**: Der Benutzer hat keine zeitliche Limitierung, kann aber die Stati aktiv oder inaktiv besitzen. Diese Benutzerart dient zur Verwaltung von MAC-Adressen/Geräten zur Netzwerkauthentifizierung (NAC). (Modul naMacAuth)
- **Gäste Zutrittsgruppen**: Verwaltung von selbst erstellten Gruppen mit frei definierbaren Zutrittsregeln

Da jede der vier Arten von Benutzern ein eigenes netADIT-Modul ist können diese unabhängig voneinander betrieben und über eigene Bereiche je Benutzer-Art administriert werden. Je nach Einsatzszenario kann dies bedeuten, dass nur eine Art, zwei, drei oder alle Arten von Benutzern verfügbar ist/sind und danach auch die angezeigten Bereiche der Benutzer im netADIT-GUI variieren.

INFO

Gästauthentifizierungen können zusätzlich noch über einen externen Verzeichnisdienst (Modul naDirectory) oder nur mittels Akzeptierens der AGBs (Modul naAGBauth) erfolgen. Hierfür sind zwar in der Systemkonfiguration von netADIT spezielle Konfigurationen möglich, die Gästeverwaltung selbst erfolgt aber bei keinem dieser Module innerhalb von netADIT!

Gästezutritt

Der Zutritt der Gäste und die damit verbundene Authentifizierung können auf verschiedene Arten und Mechanismen erfolgen:

- **naFirewall**: Hierbei handelt es sich um ein Modul von netADIT welches den Server, auf dem netADIT installiert ist, zu einem Router, DHCP-Server und zu einer Firewall umfunktioniert. Verbindet sich der Gast mit dem definierten WLAN oder LAN wird dieser beim Aufruf einer Website automatisch auf die Loginseite von netADIT umgeleitet. Erst nach erfolgreichem Login kann der Gast das Gästenetzwerk nutzen.

- **AccessPoints oder WLAN Systeme** wie etwa von HP Aruba oder Cisco: Hier übernimmt der Accesspoint oder des WLAN-Systems die Authentifizierung, fragt aber über Radius netADIT nach den Korrekten Benutzerdaten ab.

- **Switches**, **Firewalls**, **VPN-Server**, ... : Hier wird ebenfalls netADIT als Radius-Server benutzt um die User zu authentifizieren und/oder autorisieren.

Die Module

1. naBasic

bietet die Basis des gesamten Systems wie die netADIT-Administrationsoberfläche und Hintergrundprogramme.

Voraussetzungen:	AlmaLinux 9.x oder RHEL 9.x, openLDAP, MariaDB, freeRadius, Apache2, PHP8.2 inklusive CLI-Version, IonCube Loader
Funktionen:	WebGUI, Systemkonfiguration über Konfigurationsdatei, anlegen, bearbeiten und löschen von administrativen Benutzern, Ansicht der Logdateien, wechseln zwischen den Sprachen Deutsch und Englisch, Protokollierung von Änderungen (wer was wann gemacht hat), anpassen des Login-Logos durch ein eigenes.
REST-API:	login, known-routes, userinfo

2. naTimeframe

bietet die Verwaltung von zeitgesteuerten Gäste-Benutzern. Beim Anlegen des Gastes wird zu den Benutzerdaten auch Startdatum/Startzeit und Enddatum/Endzeit angegeben. Dem Gast ist es nur möglich sich zum angegebenen Zeitraum anzumelden.

Voraussetzungen:	naBasic
Funktionen:	anlegen von einzelnen Gästen, anlegen von mehreren Gästen mittels Steuerdatei, PDF-Druck des Gästedatenblattes inkl. Logindaten und eigenem Logo, ansehen, bearbeiten und löschen von inaktiven Gästen, ansehen und bearbeiten von aktiven Gästen und ansehen von gelöschten Gästen.
REST-API:	users-list, user-show, user-add, user-del, user-mod

3. naPersist

bietet die Verwaltung von Gäste-Benutzern ohne automatisches Enddatum. Beim Anlegen des Gastes wird zu den Benutzerdaten der Status aktiv oder inaktiv definiert. Nur aktiven Gästen ist es möglich sich anzumelden.

Voraussetzungen:	naBasic
Funktionen:	anlegen von einzelnen Gästen, anlegen von mehreren Gästen mittels Steuerdatei, PDF-Druck des Gästedatenblattes inkl. Logindaten und eigenem Logo, ansehen, bearbeiten und löschen von inaktiven Gästen so wie ansehen und bearbeiten von aktiven Gästen.
REST-API:	users-list, user-show, user-add, user-del, user-mod

4. naTimelimit

bietet die Verwaltung von zeit-limitierten Gäste-Benutzern. Beim Anlegen des Gastes wird zu den Benutzerdaten auch ein Zeitlimit in Minuten angegeben. Der Gast ist sofort aktiv und wird nach tatsächlichem Verbrauch seiner gebuchten Zeit automatisch deaktiviert. Nur aktiven Gästen ist es möglich sich anzumelden.

Voraussetzungen: naBasic, naFirewall

Funktionen: anlegen von einzelnen Gästen, anlegen von mehreren Gästen mittels Steuerdatei, PDF-Druck des Gästedatenblattes inkl. Logindaten und eigenem Logo, ansehen, bearbeiten und löschen von aktiven Gästen.

REST-API: users-list, user-show, user-add, user-del, user-mod

5. naMacAuth

bietet die Verwaltung von Benutzern/Geräten speziell für die Netzwerkauthentifizierung (NAC – NetworkAccessControl) mittels MAC-Adresse ohne automatisches Enddatum. Beim Anlegen des Benutzers/Gerätes wird zu den Geräteinformationen der Status aktiv oder inaktiv definiert. Nur aktiven Benutzern/Geräten ist es möglich sich anzumelden.

Voraussetzungen: naBasic

Funktionen: anlegen von einzelnen Benutzern/Geräten, anlegen von mehreren Bentuzern/Geräten mittels Steuerdatei, ansehen, bearbeiten und löschen von inaktiven Bentuzern/Geräten sowie ansehen und bearbeiten von aktiven Bentuzern/Geräten.

REST-API: users-list, user-show, user-add, user-del, user-mod

6. naABGauth

bietet die einfache Möglichkeit Gäste nur mittels Akzeptieren der AGBs für das Gästenetzwerk frei zu schalten.

Voraussetzungen: naBasic, naFirewall

Funktionen: aktivieren/deaktivieren des Moduls mittels GUI, verwalten/bearbeiten der AGBs für alle Sprachen mittels GUI.

7. naDirectory

bietet die Anbindung an einen externen Verzeichnisdienst zur Authentifizierung von Gästen und somit für die Verwaltung von Gäste-Benutzern in einem externen ActiveDirectory, openLDAP oder eDirectory.

Voraussetzungen: naBasic, naFirewall

Funktionen: Anbindung an Directory zur Authentifizierung.

8. naSysinfo

bietet Informationen über netADIT wie zum Beispiel Festplattenverbrauch, angemeldete Benutzer, eingesetzte Versionen und Lizenzen, ...

Voraussetzungen: naBasic

Funktionen: auflisten und abmelden aktuell angemeldeter administrativer Benutzer, auflisten aktuell angemeldeter Gäste (nur bei Verwendung von naFirewall), auflisten und zum Teil löschen von netADIT Log- und Backup-Dateien, anzeigen des verbrauchten Speicherplatzes, anzeigen der lizenzierten Module und verbrauchten Lizenzen.

9. naFirewall

bietet die Möglichkeit den Server, auf dem netADIT installiert ist, als Router und Firewall einzusetzen und die Authentifizierung der Gäste durchzuführen. Die Zutrittsberechtigungen des Gastes werden bei dessen Login auf Basis der Einstellung in der Konfiguration zugewiesen. Die in Folge beschriebenen Funktionen können über die Konfiguration aktiviert oder deaktiviert werden.

Voraussetzungen: naBasic so wie die Linux-Programme Squid, dhcpd, bind9, syslog-ng und arpwatch

Funktionen: DHCP- und DNS-Server, redirect auf Loginseite von netADIT beim Aufruf einer Website (auch wenn Gast eine fixe IP-Adresse oder einen Proxy konfiguriert hat), transparenter Proxy (lokal oder externer Server), Protokollierung der Anmeldungen, Landingpage nach Anmeldung, anpassen des Login-Logos durch ein eigenes.

10. naAuth

bietet die Möglichkeit zusätzlich zur lokalen Verwaltung der administrativen User einen externen Verzeichnisdienst wie ActiveDirectory, openLDAP oder eDirectory anzubinden. Somit kann die Benutzerverwaltung für administrative User im gewohnten System erfolgen.

Voraussetzungen: naBasic

Funktionen: Lizenz "limit": alle Benutzer des externen Verzeichnisdienstes dürfen sich anmelden und sind Operatoren, Lizenz "full": das gesamte Rollenkonzept wird auf Basis von Gruppenzuweisungen im externen Verzeichnisdienst abgebildet.

11. naFreelog

bietet die Möglichkeit frei definierte Logdateien anzugeben und diese im GUI zu betrachten.

Voraussetzungen: naBasic sowie optional das Linux-Programm Syslog-NG

Funktionen: Angabe und Auswahl unbegrenzter Logdateien, Volltextsuche inklusive logischer Operatoren und Sortierung in der jeweils ausgewählten Logdatei.

12. naGroups

bietet die Möglichkeit Zutrittsgruppen für Gäste zu verwalten. Pro Gruppe können individuelle Firewallregeln erstellt werden und beim Anlegen eines Gastes kann diesem eine der Gruppen zugewiesen werden. Meldet sich der Gast am System an werden nicht die in der Konfigurationsdatei sondern in der ihm zugewiesenen Gruppe angegebenen Dienste freigeschaltet. Somit können Gästen verschiedene Zutrittsberechtigungen vergeben werden.

Voraussetzungen: naBasic, naFirewall

Funktionen: Gruppenzuweisung in der Verwaltung von Gästen, erstellen von Gruppen inklusive Zutrittsregeln. auflisten von Gruppen so wie anzeigen, bearbeiten und löschen dieser oder deren Zutrittsregeln, überprüfen, auf welche Gruppen und Benutzer eine Regel zutrifft.

13. naAGB

bietet die Möglichkeit beim ersten Login des Gastes eigens definierte Benutzungsrichtlinien anzuzeigen welche der Gast für ein erfolgreiches Login akzeptieren muss.

Voraussetzungen: naBasic, naFirewall

Funktionen: Definition der Benutzungsrichtlinien Deutsch und Englisch in der Konfigurationsdatei.

14. naDynVLAN

bietet die Möglichkeit dem Gast eine VLAN-ID zuzuweisen und diese bei einer Radius-Authentifizierung dem Netzwerkdevice mitzuliefern!

Voraussetzungen: naBasic

Funktionen: Dynamische VLAN-Zuweisung beim Einsatz von netADIT als NAC

REST-API: vlans-list, vlan-show, vlan-add, vlan-del

15. naNACconf

bietet per netADIT-GUI die Möglichkeit zur zentralen Verwaltung von NAC-Boxen (freeRadius-Server basierend auf AlmaLinux/RHEL in Version 9.x für den Einsatz von NetworkAccessControl) und deren Diensten, zur Basis-Konfiguration für NAC, MAC und/oder 802.1x Authentifizierung so wie die Konfiguration einer komplexen VLAN-Zuweisung mittels Regelwerke von Benutzer-Geräte- oder sogar Benutzer-Geräte-SSID-Kombinationen. Ebenso möglich ist das Verwalten von erlaubten NAC-Clients (Geräte wie AccessPoints, Switches, Router, ... welche die Endgeräte/Benutzer authentifizieren) und das Ansehen der Authentifizierungsprotokolle.

Voraussetzungen: naBasic, naDynVLAN

Funktionen: Basis- und 802.1x-Konfiguration sowie Verwaltung von VLAN-Zuweisungs-Regeln für die generelle Konfiguration von NAC, verwalten der NAC-Clients, verwalten von NAC-Boxen und deren Dienste sowie deren Synchronisationsstatus, zentrales Log der Netzwerkauthentifizierungen im netADIT-GUI

16. naHSGconf

bietet per netADIT-GUI die Möglichkeit zum Betrieb und zentraler Verwaltung von dezentralen naFirewall-Instanzen (**H**ot**S**pot**G**ateways basierend auf AlmaLinux/RHEL in Version 9.x)

Voraussetzungen: naBasic, naFirewall

Funktionen: Anlegen und verwalten von HSG-Boxen inklusive deren Diensten und Zertifikaten. Konfiguration aller für die HSGs relevanten Module, zentrales Logging und Verwaltung von Gästeanmeldungen.

17. naURLfilter

bietet die Möglichkeit auf Grund von selbst definierten Black- und White-Listen aufgerufene Webseiten zu sperren. Im Fall einer gesperrten Webseite wird eine Fehlerseite im Design von netADIT und (wenn bei naFirewall konfiguriert) dem eigenen Logo angezeigt.

Voraussetzungen: naBasic, naFirewall sowie das Linux-Programm Squid

Funktionen: anzeigen, erstellen und löschen von geblockten Wörtern (Blacklist), anzeigen, erstellen und löschen von freigegebenen Wörtern (Whitelist).

18. naBandwidth

bietet die Möglichkeit Bandbreiten zu verwalten und diesen Gästebenutzern zuzuweisen. Bei der Authentifizierung über freeRadius durch Switches, PPoE-Server oder ähnliches können diese Attribute (vorausgesetzt der Drittanbieter stellt dies zur Verfügung) verarbeitet werden.

Voraussetzungen: naBasic

Funktionen: anzeigen, erstellen und löschen von Bandbreiten, Bandbreitenzuweisung in der Verwaltung von Gästen.

19. naSMSreg

bietet dem Gast die Möglichkeit sich über das Anmeldeportal von netADIT selbst per SMS zu registrieren und sich somit einen Gästebenutzer automatisiert anlegen zu lassen!

Voraussetzungen: naBasic, naTimeframe und/oder naTimelimit, naFirewall sowie das Linux-Programm smstools3 und ein kompatibles Gerät zum SMS-Versand.

Funktionen: Benutzererstellung und Registrierung durch den Gast selbst für den Einsatz von netADIT als HotSpot-Lösung.

20. naSMSregXtend

bietet die Möglichkeit das Modul naSMSreg im Admi-GUI von netADIT so zu erweitern, dass zusätzliche Felder wie eai Adresse, Land, PLZ, Stadt und Straße bei der SMS-Registrierung des Gastes abgefragt werden. Ebenso kann definiert werden, ob es sich hierbei um ein optionales oder verpflichtendes Feld handelt. Sobald dieses Modul aktiv ist muss der Gast eine Datenschutzklausel, dessen Text ebenfalls im Admin-GUI definiert werden kann, akzeptieren. Die Auswertung der Daten erfolgt in Tabellenform und bietet eine Volltextsuche mit frei wählbarer Sortierung so wie den Download des Ergebnisses per CSV-Daten!

Voraussetzungen: naSMSreg

Funktionen: Ein-/Ausschalten des Moduls, Definition zusätzlicher Abfragefelder bei der SMS-Registrierung und Auswertung inkl. CSV-Download der gespeicherten Daten.

TR-Tec GmbH
Strudenzeile 3
A–3270 Scheibbs

M: +43 664 2120576
T: +43 7482 43131
F: +43 7482 43131

FN 368113c
LG St. Pölten
UID: ATU66673646
Firmensitz: Scheibbs

E: office@tr-tec.at
www.tr-tec.at