HOLGER REIBOLD

INKLUSIVE E-BOOK

AdminMission

Das NetBird-Handbuch

Zero-Trust-Netzwerke mit WireGuard aufbauen, betreiben und prüfsicher dokumentieren

40 interaktive Missionen
mit dem Online-Lernspiel AdminMission



BRAIN-MEDIA.DE

Holger Reibold

Das NetBird-Handbuch

Zero-Trust-Netzwerke mit WireGuard aufbauen, betreiben und prüfsicher dokumentieren

BRAIN-MEDIA.DE

24 Anhang – A Befehlsreferenz netbird CLI

Die folgende Übersicht fasst die im Buch verwendeten Befehle und Schalter zusammen. Sie ist eine Auswahl. Die vollständige, zur installierten Version passende Liste zeigt netbird --help beziehungsweise netbird <Befehl> --help.

24.1 Verbinden und trennen

Befehl	Wirkung
netbird up	verbindet mit der Steuerungsebene, startet bei Bedarf die Anmeldung im Browser
netbird up --setup-key <KEY>	registriert das Gerät mit einem Setup-Key
netbird up --management-url <URL>	verwendet eine selbst betriebene Instanz
netbird up --hostname <NAME>	legt den Gerätenamen im Overlay fest
netbird down	trennt die Verbindung
netbird login	meldet das Gerät an, ohne sofort zu verbinden
netbird version	zeigt die Version des Clients

Tabelle A.1: Verbinden und trennen.

24.2 Optionen für netbird up

Schalter	Wirkung	Kapitel
--allow-server-ssh	aktiviert den NetBird-SSH-Server	15
--disable-ssh-auth	schaltet die Identitätsprüfung für SSH ab	15
--ssh-jwt-cache-ttl <DAUER>	Zwischenspeicher für SSH-Tokens	15
--enable-ssh-sftp	erlaubt SFTP über NetBird SSH	15
--enable-ssh-local-port-forwarding	erlaubt lokale Portweiterleitung	15
--enable-rosenpass	aktiviert den Post-Quanten-Schutz	3
--rosenpass-permissive	Verbindung auch zu Peers ohne Rosenpass	3
--preshared-key <KEY>	zusätzlicher Preshared Key	2, 3
--disable-dns	NetBird verwaltet das DNS des Geräts nicht	12
--disable-ipv6	keine IPv6-Adresse im Overlay	13
--allow-remote-jobs	erlaubt Debug-Bundles auf Anforderung aus dem Dashboard (ab 0.78)	18

Tabelle A.2: Wichtige Optionen für netbird up.

24.3 Status und Diagnose

Befehl	Wirkung
netbird status	Kurzstatus: Verbindung zu Management, Signal, Relays, Peers
netbird status -d	Details je Peer: Verbindungsart, Kandidaten, Handshake, Datenmenge
netbird status --json	maschinenlesbare Ausgabe
netbird status -d --filter-by-status connected	nur verbundene Peers
netbird debug bundle -A -S	anonymisiertes Debug-Bundle mit Systeminformationen
netbird debug bundle -U	Bundle verschlüsselt an NetBird übertragen
netbird debug log level trace	Protokollstufe bis zum Neustart erhöhen
netbird debug for 5m	Protokolle über fünf Minuten sammeln und Bundle erzeugen

Tabelle A.3: Status und Diagnose.

24.4 Profile, SSH, Kubernetes, Dienst

Befehl	Wirkung
netbird profile add <NAME>	legt ein Profil an
netbird profile list	listet die Profile
netbird profile select <NAME>	wechselt das aktive Profil
netbird profile rename <ALT>	benennt ein Profil um

<NEU>	
netbird profile remove <NAME>	entfernt ein inaktives Profil
netbird ssh <benutzer>@<peer>	SSH-Verbindung über NetBird SSH
netbird kubernetes list	erreichbare Kubernetes-Cluster anzeigen und einrichten
netbird service install, start, stop, uninstall	Systemdienst verwalten

Tabelle A.4: Profile, SSH, Kubernetes und Dienst.

24.5 Umgebungsvariablen

Variable	Wirkung
NB_SETUP_KEY	Setup-Key, etwa im Container
NB_MANAGEMENT_URL	Adresse der Steuerungsebene
NB_HOSTNAME	Gerätename
NB_LOG_LEVEL	Protokollstufe
NB_LAZY_CONN_INACTIVITY_-THRESHOLD	Leerlaufzeit für Lazy Connections
NB_DISABLE_CUSTOM_ROUTING, NB_USE_LEGACY_ROUTING	Routing-Modus, etwa für MikroTik
NB_DISABLE_GEOLOCATION	Geolokalisierung im Management abschalten (Server)

Tabelle A.5: Umgebungsvariablen (Auswahl).

25 Anhang B – Portübersicht und Firewall-Regeln

25.1 Clients zum Managed Service (ausgehend)

Dienst	Ziel	Protokoll und Port
Management	api.netbird.io	TCP 443
Signal	signal.netbird.io	TCP 443
STUN	stun.netbird.io	UDP 80, 443, 3478, 5555
Relay	*.relay.netbird.io	TCP und UDP 443

Tabelle B.1: Ausgehende Verbindungen zum Managed Service laut Herstellerdokumentation.

25.2 Selbst betriebene Instanz (eingehend)

Port	Protokoll	Zweck
80	TCP	Zertifikatsausstellung, Weiterleitung auf HTTPS
443	TCP	Dashboard, API, gRPC für Management und Signal, Relay über WebSocket
3478	UDP	STUN, immer direkt, nie über einen HTTP-Proxy
weiterer UDP-Port	UDP	Relay über QUIC, sofern konfiguriert
9090, 9000	TCP	Kennzahlen und Zustandsabfrage, nur intern

Tabelle B.2: Ports der selbst betriebenen Instanz.

25.3 Zwischen Peers

WireGuard verwendet UDP, auf Clients standardmäßig Port 51820, bei Bedarf dynamisch. Eingehende Freigaben sind nicht nötig, weil Verbindungen per Hole Punching aufgebaut werden. Ausgehendes UDP muss erlaubt sein.

25.4 Empfehlungen für Firmen-Firewalls

- Ausgehendes UDP für Geräte mit NetBird-Client erlauben, mindestens zu beliebigen Zielen auf dem WireGuard-Port und zu den STUN-Ports der Steuerungsebene.
- Für Routing Peers und wichtige Server eine NAT-Regel mit statischem Quellport anlegen.
- Die Domains der Steuerungsebene von der TLS-Inspektion ausnehmen.
- Keine eingehenden Freigaben für NetBird auf Clients.

AUSZUG AUS DEM BUCH

Das NetBird-Handbuch

Zero-Trust-Netzwerke mit WireGuard aufbauen,
betreiben und prüfsicher dokumentieren

- 22 Kapitel, 500 Seiten, Hardcover
- Fallbeispiel Saarmetall GmbH durch alle Kapitel
- In jedem Kapitel: Kasten „Evidenz“ mit den Nachweisen für ISO 27001, NIS-2 und IT-Grundschutz
- E-Book als PDF inklusive
- NetBird-Missionen im Praxislabor AdminMission

39,00 EUR · ISBN 978-3-95444-379-6

Bestellen bei Amazon:
amazon.de/dp/3954443791

Mehr zum Buch, Leseprobe und Begleitmaterial:
brain-media.de/Buecher/buch-netbird.html

© 2026 Brain-Media.de · Dr. Holger Reibold · Alle Rechte vorbehalten.