
nm-settings

Paramètres et propriétés des profils de connexion NetworkManager

NetworkManager est basé sur un concept de profils de connexion. Les profils de connexions sont gérés par NetworkManager via le services de paramètres et sont exportés sur D-Bus.

802-1x

- altsubject-matches** (tableau de chaînes) Liste de chaînes à matcher avec le altSubjectName du certificat présenté par le serveur d'authentification. vide, aucune vérification n'est effectuée. Défaut : vide
- anonymous-identity** (chaîne) identité anonyme pour les méthodes d'authentification EAP. Utilisé comme identité non-chiffrée avec les type EAP qui supportent différentes identités tunnelisées come EAP-TTLS
- ca-cert** (chaîne d'octets) Contient le certificat CA utilisé par la méthode EAP spécifié dans la propriété eap.
- ca-path** (chaîne) chemin d'un répertoire contenant les certificats à ajouter à la chaîne de vérification
- client-cert** (chaîne d'octets) Contient le certificat client utilisé par la méthode EAP spécifiée dans la propriété eap
- domain-suffix-match** (chaîne) Contrainte pour le nom de domaine. Si définis, ce FQDN est utilisé comme suffixe requis pour les éléments dNSName du certificat présenté par le serveur d'authentification.
- eap** (tableau de chaînes) La méthode EAP permise pour l'authentification avec 802.1x. (leap, md5, tls, peap, ttls, pwd fast).
- identity** (chaîne) Identité pour les méthodes d'authentification. Généralement le login
- name** (chaîne) Nom du paramètre qui identifie le paramètre dans la connexion. Chaque type de paramètre a un nom unique pour ce type, par exemple ppp, wireless, wired. Défaut : 802-1x
- pac-file** (chaîne) Chemin du fichier contenant PAC pour EAP-FAST
- password** (chaîne) mot de passe pour les méthodes l'authentification EAP. A précédence sur 'password-raw'
- password-flags** (NMSettingSecretFlags) Flags indiquant comment manipuler la propriété password
- password-raw** (tableau d'octets) Mot de passe utilisé par les méthodes d'authentification EAP.
- password-raw-flags** (NMSettingSecretFlags) Flags indiquant comment manipuler la propriété password-raw
- phase1-fast-provisionning** (chaîne) active/désactive le provisionning in-line des accreditifs EAP-FAST quand FAST est spécifié comme méthode EAP. (0-désactivé, 1-provisionning non-authentifié, 2-provisionning authentifié, 3-provisionning authentifié et non authentifié)
- phase1-peaplabel** (chaîne) Force l'utilisation du nouveau label PEAP durant la dérivation de clé. Certains serveurs RADIUS peuvent l'exiger pour interopérer avec PEAPv1.
- phase1-peapver** Version PEAP à utiliser. Non définis, la version donné par le serveur est utilisé. (0 ou 1)
- phase2-altsubject-matches** (tableau de chaînes) Liste de chaîne à matche avec le altSubjectName du certificat présenté par le serveur d'authentification durant la phase 2. vide, aucune vérification n'est effectuée
- phase2-auth** (chaîne) Spécifie les méthodes d'authentification non-EAP de la phase 3 quand EAP utilise un tunnel TLS (pap, chap, mschap, mschapv2, gtc, otp, md5, tls).
- phase2-autheap** (chaîne) Spécifie les méthodes d'authentification EAP de la phase 2 quand la méthode EAP utiliser un tunnel TLS. (md5, mschapv2, otp, gtc, tls).
- phase2-ca-cert** (tableau d'octets) Contient le certificat CA de la phase 2.
- phase2-ca-path** (chaîne) répertoire contenant les certificats additionnels
- phase2-client-cert** (tableau d'octets) Contient le certificat client de la phase 2.
- phase2-domain-suffix-match** (chaîne) Contraint le nom de domaine du serveur. ce FQDN est un suffixe à matcher dans dNSName du certificat présenté par le serveur d'authentification.

phase2-private-key (tableau d'octets) Contient la clé privée de la phase 2 quand phase2-auth ou phase2-authheap est à 'tls'.

phase2-private-key-password [chaîne) mot de passe utilisé pour déchiffrer la clé privée

phase2-private-key-password-flags (NMSettingSecretFlags) Flags indiquant comment gérer la propriété phase2-private-key-password.

phase2-subject-match (chaîne) sous-chaîne à matcher avec le sujet du certificat présenté par le serveur d'authentification durant la phase2.

pin (chaîne) PIN utilisé pour les méthodes d'authentification EAP

pin-flags (NMSettingSecretFlags) Flags indiquant comme gérer la propriété pin.

private-key (tableau d'octets) Contient la clé privée quand la propriété eap est à 'tls'.

private-key-password (chaîne) mot de passe pour déchiffrer la clé privée

private-key-password-flags (NMSettingSecretFlags) flags indiquant comme gérer la propriété private-key-password.

subject-match (chaîne) sous-chaîne à matcher avec le sujet du certificat présenté par le serveur d'authentification. déprécié en faveur de NMSetting8021x :domain-suffix-match

system-ca-certs (bool) à TRUE, écrase ca-path et phase2-ca-path en utilisant le répertoire CA système spécifié à la configuration avec `-system-ca-path`.

adsl

encapsulation (chaîne) Encapsulation de la connexion ADSL. (vcmux ou llc)

name (chaîne) nom du paramètre, qui identifie de manière unique le paramètre dans la connexion. défaut : adsl

password (chaîne) mot de passe utilisé pour authentifier le service ADSL

password-flags (NMSettingSecretFlags) flags indiquant comme gérer la propriété password

protocol (chaîne) protocole de connexion ADSL (pppoa, pppoe, ou ipoatm)

username (chaîne) username pour l'authentification

vci (uint32) VIC de la connexion ADSL

vpi (uint32) VPI de la connexion ADSL

bluetooth

bdaddr (tableau d'octets) l'adresse bluetooth du périphérique

name (chaîne) nom du paramétrage : bluetooth

type (chaîne) soit 'dun' pour Dial-Up Networking ou 'panu' pour Personal Area Networking

bond

interface-name (chaîne) déprécié en faveur de connection.interface-name.

name (chaîne) nom du paramétrage (bond)

options (dictionnaire) dictionnaire de paires clé/valeurs d'option bonding. défaut : { 'mode' : 'balance-rr' }

bridge

ageing-time (uint32) temps en seconde de la durée de l'adresse MAC ethernet. défaut : 300

forward-delay (uint32) forwarding delay STP, en secondes. Défaut : 15
hello-time (uint32) hello time STP, en secondes. défaut : 2
interface-name (chaîne) déprécié en faveur de connection.interface-name
mac-address (tableau d'octets) si spécifié, l'adresse mac du commutateur.
max-age (uint32) amximum message age STP, en secondes. défaut : 20
multicast-snooping (bool) contrôle si IGMP snooping est activé pour ce commutateur.
name (chaîne) nom du paramétrage : bridge
priority (uint32) Priorité STP du bridge. défaut : 32768
stp (bool) Active STP.

bridge-port

hairpin-mode (bool) Active le mode hairpin pour le port, les frames sont renvoyés via le port ou la frame a été reçue
name (chaîne) nom du paramètrage = bridge-port
path-cost (uint32) port cost STP pour les destinations via ce port
priority (uint32) priorité STP de ce port

cdma

name (chaîne) nom du paramètrage : cdma
number (chaîne) numéro à composer pour établir la connexion au réseau mobile CDMA. défaut : #777
password (chaîne) mot de passe pour l'authentification
password-flags (NMSSettingSecretFlags) Flags indiquant comment manipuler la propriété password
username (chaîne) username pour l'authentification

connection

autoconnect (bool) si la connexion est automatiquement connectée par NetworkManager quand les ressources pour la connexion sont disponibles. Défaut : TRUE
autoconnect-priority (int32) Priorité autoconnect. défaut : 0
autoconnect-retries (int32) nombre de tentatives de connexions durant l'autoactivation. 0 signifie indéfiniment, -1 et le défaut global (4 fois si non modifié)
autoconnect-slaves (NMSSettingConnectionAutoconnectSlaves) Si ou non les esclaves de cette connexion devraient être automatiquement activés. 0-non, 1-activer les connexions esclave, -1-défaut.
gateway-ping-timeout (uint32) > à 0, délais du succès de l'adressage IP jusqu'à que le timeout soit atteint, ou une réponse d'une gateway à un ping
id (chaîne) identifiant unique pour la connexion
interface-name (chaîne) nom de l'interface réseau à laquelle la connexion est lié
lldp (int32) Si lldp est activé pour la connexion. Défaut :-1
master (chaîne) Nom de l'interface du périphérique maître ou l'uuid de la connexion maître
metered (NMMetered) Si la connexion est mesurée
name (chaîne) Nom du paramètrage : connection

permissions (tableau de chaînes) Tableau définissant l'accès d'un utilisateur à cette connexion. Vide, tous les utilisateurs sont autorisés à accéder à cette connexion. Chaque entrée est sous la forme "[type] :[id] :[reserved]". Actuellement seul le type "user" est utilisé.

read-only (bool) indique si la connexion peut être modifiée en utilisant D-Bus (FALSE), ou non (TRUE)

secondaries (tableau de chaînes) Liste d'UUID de connexions qui devraient être activés quand la connexion de base elle-même est activée. Actuellement seul les connexions VPN sont supportés

slave-type (chaîne) nom du paramètre du type de périphérique de cette connexion maître (ex : bond0) ou NULL si cette connexion n'est pas un esclave

stable-id (chaîne) Token pour générer des ID stable pour la connexion. Il est utilisé pour générer des IPv6 privées stable avec `ipv6.addr-gen-mode=stable-privacy`. Également utilisé pour émettre l'adresse MAC clonée générée pour `ethernet.cloned-mac-address=stable` et `wifi.cloned-mac-address=stable`. Spécifie un stable-id permet à plusieurs connexions de générer les mêmes adresses. Il est possible de générer des ID via des substitutions : `${CONNECTION}`, `${BOOT}`, `${RANDOM}`.

timestamp (uint64) Temps en seconde depuis l'Epoch, que la connexion a été activée avec succès. NetworkManager met à jours cette valeur périodiquement.

type (chaîne) Type de base de la connexion. Pour les connexions dépendantes du hardware, devrait contenir le nom du paramètre du type de matériel (ex : 802-3-ethernet, 802-11-wireless, bluetooth, etc.), et pour les connexions non hardware, devrait contenir le nom du type de paramètre (vpn, bridge, etc.)

uuid (chaîne) Identifiant unique pour la connexion. Devrait être assigné à la création de la connexion, et ne devrait jamais être changé.

zone (chaîne) Niveau de confiance de la connexion. Texte lisible insensible à la casse (ex : Home, Work, Public). NULL ou non spécifié, la connexion sera placée dans la zone par défaut tel que définis par le firewall.

dcb

app-fcoe-flags (NMSettingDcbFlags) Flags pour l'application FCoE DCB. Peut être une combinaison de `NM_SETTINGS_DCB_FLAG_ENABLE(0x1, NM_SETTING_DCB_FLAG_ADVERTISE (0x2), et NM_SETTING_DCB_FLAG_WILLING (0x4)`

app-fcoe-mode (chaîne) Mode contrôleur FCoE ; soit "fabric" ou "vn2vn"

app-fcoe-priority (int32) Priorité la plus élevée (0-7) à utiliser pour les frames FCoE, ou -1 pour la priorité par défaut

app-fip-flags (NMSettingDcbFlags) Flags pour l'application DCB FIP. peut être une combinaison de `NM_SETTINGS_DCB_FLAG_ENABLE(0x1, NM_SETTING_DCB_FLAG_ADVERTISE (0x2), et NM_SETTING_DCB_FLAG_WILLING (0x4)`

app-fip-priority (int32) Priorité la plus élevée (0-7) à utiliser pour les frames FIP, ou -1 pour la priorité par défaut

app-iscsi-flags (NMSettingDcbFlags) Flags pour l'application DCB iSCSI. peut être une combinaison de `NM_SETTINGS_DCB_FLAG_ENABLE(0x1, NM_SETTING_DCB_FLAG_ADVERTISE (0x2), et NM_SETTING_DCB_FLAG_WILLING (0x4)`

app-iscsi-priority (int32) Priorité la plus élevée (0-7) à utiliser pour les frames iSCSI, ou -1 pour la priorité par défaut

name (chaîne) Nom du paramètre : dcb

priority-bandwidth (tableau de uint32) Tableau de 8 valeurs uint, où l'indexe correspond à la priorité utilisateur (0-7), et la valeur indique le pourcentage de bande passante du groupe assigné à la priorité. La somme de tous les pourcentages doit faire 100%

priority-flow-control (tableau de uint32) Tableau de 8 booléens où l'indexe correspond à la priorité utilisateur (0-7) et la valeur indique si la priorité devrait transmettre une pause de priorité

priority-flow-control-flags (NMSettingDcbFlags) flags pour DCP PFC (Priority Flow Control). peut être une combinaison de `NM_SETTINGS_DCB_FLAG_ENABLE(0x1, NM_SETTING_DCB_FLAG_ADVERTISE (0x2), et NM_SETTING_DCB_FLAG_WILLING (0x4)`

priority-group-bandwidth (tableau de uint32) Tableau de 8 valeurs uint, où l'indexe correspond à la priorité de groupe (0-7), et la valeur indique le pourcentage de bande passante allouée à ce groupe. La somme de tous les pourcentages doit faire 100%

priority-group-flags (NMSettingDcbFlags) Flags pour DCB Priority Groups. peut être une combinaison de `NM_SETTINGS_DCB_FLAG_ENABLE(0x1, NM_SETTING_DCB_FLAG_ADVERTISE (0x2), et NM_SETTING_DCB_FLAG_WILLING (0x4)`

priority-group-id (tableau de uint32) Tableau de 8 valeurs uint, où l'indexe correspond à la priorité utilisateur (0-7), et la valeur indique le Priority Group ID. Les priorités permises sont 0-7, ou 15 pour le groupe non restreint.

priority-strict-bandwidth (tableau de uint32) Tableau de 8 booléens où l'indexe correspond à la priorité utilisateur (0-7) et la valeur indique si la priorité peut utiliser toute la bande passante allouée au groupe assigné

priority-traffic-class (tableau de uint32) Tableau de 8 valeurs uint, où l'indexe correspond à la priorité utilisateur (0-7), et la valeur indique la classe de trafic (0-7) pour laquelle la priorité est mappée

generic

name (chaîne) Nom du paramétrage, qui identifie de manière unique les paramètres dans la connexion.

gsm

apn (chaîne) Nom du point d'accès GPRS spécifiant l'APN utilisé pour établir une session de données avec le réseau GSM.

device-id (chaîne) Identifiant unique de périphérique (tel que donné par le service de gestion WWAN)

home-only (bool) à TRUE, seuls les connexions au réseau personnel est autorisé. Les connexions aux réseaux roaming ne sont pas faites. Défaut : FALSE

name (chaîne) Nom du paramétrage : gsm

network-id [chaîne] ID réseau (format GSM LAI, ex : MCC-MNC) pour forcer un enregistrement spécifique.

number (chaîne) Numéro à composer pour établir une session de données PPP.

password (chaîne) Mot de passe utilisé pour l'authentification avec le réseau.

password-flags (NMSSettingSecretFlags) flags indiquant comment gérer la propriété password

pin (chaîne) Si la SIM est bloquée avec un PIN, elle doit être débloquée avec un PIN

pin-flags (NMSSettingSecretFlags) Flags indiquant comment gérer la propriété pin

sim-id (chaîne) identifiant unique de carte SIM

sim-operator-id (chaîne) chaîne MCC/MNC comme "310260" ou "21601" identifiant l'opérateur mobile.

username (chaîne) username utilisé pour l'authentification sur le réseau.

infiniband

mac-address (tableau d'octets) Si spécifié, cette connexion ne s'applique qu'au périphérique IPoIB dont l'adresse mac correspond. Cette propriété ne change pas l'adresse MAC

mtu (uint32) non 0, ne transmet que les paquets de la taille spécifiée ou inférieur, splittant les paquets plus gros en plusieurs frames.

name (chaîne) Nom du paramétrage : infiniband

p-key (int32) P_Key infiniband à utiliser pour ce périphérique. -1 utilise le P_Key par défaut (à l'index 0)

parent (chaîne) nom de l'interface du périphérique parent de ce périphérique. Normalement NULL, sauf si p_key est définis.

transport-mode (chaîne) Mode IPoIB (datagram ou connected)

ipv4

address-data (tableau d'ipv4) tableau d'IPv4. Chaque dictionnaire d'adresse contient au moins les entrées 'address', et 'prefix'

addresses (tableau de tableau de uint32) déprécié en faveur de address-data et gateway

dad-timeout (int32) Timeout en ms utilisé pour vérifier la présence d'adresse IP dupliquées

dhcp-client-id (chaîne) chaîne envoyée au serveur DHCP pour identifier la machine

dhcp-fqdn (chaîne) Si la propriété `dhcp-send-hostname` est à `TRUE`, le `fqdn` spécifié sera envoyé au serveur DHCP en acquérant le bail. exclusif avec `dhcp-hostname`.

dhcp-hostname (chaîne) si `dhcp-send-hostname` est à `true`, le nom spécifié ici est envoyé au serveur DHCP

dhcp-send-hostname (bool) à `true`, envoie le `hostname` au serveur DHCP

dhcp-timeout (int32) timeout de transaction DHCP, en secondes. Défaut : 0

dns [tableau d'uint32] tableau d'adresses IP des serveurs DNS

dns-options (tableau de chaînes) tableau d'options DNS tel que décrits dans `man resolv.conf`. `NULL` utilise les valeurs par défaut

dns-priority (int32) Priorité DNS intra-connexion. La priorité relative est utilisée pour déterminer l'ordre des serveurs DNS dans `resolv.conf`. Une valeur faible place les serveurs en haut du fichier. Défaut : 0, qui sélectionne la valeur par défaut : 50 pour VPN, et 100 pour les autres connexions.

dns-search (tableau de chaîne) tableau de domaines de recherche DNS

gateway (chaîne) La passerelle associée avec cette configuration

ignore-auto-dns (bool) Quand `method` est à `auto` et cette propriété à `TRUE`, les serveurs de nom et domaines de recherche automatiquement configurés sont ignorés et seuls les serveurs et domaines spécifiés dans les propriétés `dns` et `dns-search` sont utilisés.

ignore-auto-routes (bool) si `method` est à `'auto'` et cette propriété à `TRUE`, les routes automatiquement configurées sont ignorées et seules les routes dans la propriété `routes` sont utilisées

may-fail (bool) à `TRUE`, autorise la configuration réseau même si le fichier de configuration spécifié par cette propriété échoue au timeout. Noter qu'au moins une configuration IP doit réussir pour la configuration réseau générale échoue.

method (chaîne) Méthode de configuration IP `'auto'`, `'manual'`, `'link-local'`, et `'shared'`

name (chaîne) Nom du paramétrage : `ipv4`

never-default (bool) à `TRUE`, cette connexions n'est jamais la connexion par défaut pour ce type IP, ce qui signifie que la route par défaut n'est jamais assignée

route-data (tableau de dictionnaire) Tableau de routes IPv4. Chaque dictionnaire de route contient au moins les entrées `'dest'` et `'prefix'`. La plupart des routes ont également une entrée `'gateway'`

route-metric (int64) Métrique par défaut pour les routes qui n'en spécifient pas une explicite. Défaut : -1 signifiant que la métrique est choisie automatiquement basé sur le type de périphérique.

routes (tableau de tableau d'uint32) Déprécié en faveur de `route-data`

ipv6

addr-gen-mode (int32) Configure la méthode pour créer l'adresse rfc4862 : `eui64` ou `stable-privacy` (rfc7217)

address-data (tableau de dictionnaire) Tableau d'IPv6. chaque entrée contient au moins `address` et `prefix`.

addresses (tableau d'ipv6) déprécié en faveur de `address-data`

dad-timeout (int32) timeout en ms pour vérifier la présence d'adresses IP dupliquées. défaut : -1, utilise la valeur par défaut.

dhcp-hostname (chaîne) si `dhcp-send-hostname` est à `true`, le nom spécifié ici est envoyé au serveur DHCP

dhcp-send-hostname (bool) à `true`, envoie le `hostname` au serveur DHCP

dhcp-timeout (int32) timeout de transaction DHCP, en secondes. Défaut : 0

dns [tableau d'uint32] tableau d'adresses IP des serveurs DNS

dns-options (tableau de chaînes) tableau d'options DNS tel que décrits dans `man resolv.conf`. `NULL` utilise les valeurs par défaut

dns-priority (int32) Priorité DNS intra-connexion. La priorité relative est utilisée pour déterminer l'ordre des serveurs DNS dans `resolv.conf`. Une valeur faible place les serveurs en haut du fichier. Défaut : 0, qui sélectionne la valeur par défaut : 50 pour VPN, et 100 pour les autres connexions.

dns-search (tableau de chaîne) tableau de domaines de recherche DNS

gateway (chaîne) La passerelle associée avec cette configuration

ignore-auto-dns (bool) Quand `method` est à `auto` et cette propriété à `TRUE`, les serveurs de nom et domaines de recherche automatiquement configurés sont ignorés et seuls les serveurs et domaines spécifiés dans les propriétés `dns` et `dns-search` sont utilisés.

ignore-auto-routes (bool) si method est à 'auto' et cette propriété à TRUE, les routes automatiquement configurées sont ignorées et seules les routes dans la propriété routes sont utilisées

ip6-privacy (NMSettingIP6ConfigPrivacy)

may-fail (bool) à TRUE, autorise la configuration réseau même si le fichier de configuration spécifié par cette propriété échoue au timeout. Noter qu'au moins une configuration IP doit réussir ou la configuration réseau générale échoue.

method (chaîne) Méthode de configuration IP 'auto', 'manual' ou 'link-local'

name (chaîne) Nom du paramétrage : ipv6

never-default (bool) à TRUE, cette connexions n'est jamais la connexion par défaut pour ce type IP, ce qui signifie que la route par défaut n'est jamais assignée

route-data (tableau de dictionnaire) Tableau de routes IPv6. Chaque dictionnaire de route contient au moins les entrées 'dest' et 'prefix'. La plupart des routes ont également une entrée 'gateway'

route-metric (int64) Métrique par défaut pour les routes qui n'en spécifient pas une explicite. Défaut : -1 signifiant que la métrique est choisie automatiquement basé sur le type de périphérique.

routes (tableau de tableau d'uint32) Déprécié en faveur de route-data

token (chaîne) configure le token pour les identifiants d'interface IPv6 draft-chown-6man-tokenised-ipv6-identifiers-02. Utile avec eui64.

ip-tunnel

encapsulation-limit (uint32) Nombre de niveaux d'encapsulation additionnels à ajouter aux paquets. Uniquement pour les tunnels IPv6

flow-label (uint32) Label de flux à assigner aux packets.

input-key (chaîne) La clé utilisée pour les paquets entrant.

local (chaîne) endpoint local du tunnel. doit contenir une IPv4 ou IPv6.

mode (uint32) Mode de tunneling, par exemple NM_IP_TUNNEL_MODE_IPIP, ou NM_IP_TUNNEL_MODE_GRE

mtu (uint32) 0

name Nom du paramétrage : ip-tunnel

output-key (chaîne) Clé utilisée pour les paquets sortants

parent (chaîne) nom de l'interface parent ou UUID de la connexion parent

path-mtu-discovery (bool) Si Path MTU Discovery est activé dans ce tunnel (défaut : TRUE)

remote (chaîne) endpoint distant du tunnel. Doit être une IPv4 ou IPv6

tos (uint32) Type de service IPv4 ou classe de trafic IPv6

tll (uint32) TTL à assigner aux paquets tunnelisés. Défaut : 0, les paquets héritent de la valeur TTL

macsec

encrypt (bool) Si le trafic transmis doit être chiffré (défaut : TRUE)

mka-cak (chaîne) CAK pré-partagé pour l'agrément de clé MACsec

mka-cak-flags (NMSettingSecretFlags) Flags indiquant comment gérer la propriété mka-cak.

mka-ckn (chaîne) CKN pré-partagé pour l'agrément de clé MACsec

mode (int32) Spécifie commande la CAK pour MKA est obtenue

name Type de paramétrage : macsec

parent (chaîne) nom de l'interface parent ou UUID de la connexion parent

port (int32) Composant port du SCI, entre 1 et 65534

validation (int32) Mode de validation pour les frames entrantes

macvlan

mode (uint32) mode macvlan qui spécifie le mécanisme de communication entre plusieurs macvlans dans le même périphérique
name (chaîne) nom du paramétrage : macvlan
parent (chaîne) nom de l'interface parent ou UUID de la connexion parent
promiscuous (bool) si l'interface devrait être en mode promiscuous. Défaut : TRUE
tap (bool) Si l'interface devrait être un MACVTAP. Défaut : FALSE

802-11-olpc-mesh

channel (uint32) Canal sur lequel le réseau à joindre est localisé
dhcp-anycast-address (tableau d'octets) adresse MAC DHCP anycast utilisé pour demander une adresse IP via DHCP
name (chaîne) nom du paramétrage : 802-11-olpc-mesh
ssid (tableau d'octets) SSID du réseau à joindre

ppp

baud (uint32) non 0, indique à pppd de définir le port série au baudrate spécifié. à 0, la vitesse est choisie automatiquement
crtscts (bool) à TRUE, pppd doit définir le port série pour utiliser le contrôle de flux hardware avec les signaux RTS et CTS. Défaut : FALSE
lcp-echo-failure (uint32) non 0, pppd assume que la connexion au paire a échoué si le numéro spécifié de LCP echo-requests n'a pas reçu de réponse du paire.
lcp-echo-interval (uint32) non 0, pppd envoie un LCP echo-request au paire toutes les n secondes.
mppe-stateful (bool) à TRUE, MPPE avec état est utilisé.
mru (uint32) non 0, pppd demande au paire d'envoyer des paquets au maximum à la taille spécifiée
mtu (uint32) non 0, pppd n'envoie pas de paquet dont la taille excède cette taille
name (chaîne) nom du paramétrage : ppp
no-vj-comp (bool) À true, ne demande pas la compression d'en-tête TCP Van Jacobsen
noauth (bool) à TRUE, ne demande pas d'authentification
nobsdcomp (bool) à TRUE, ne demande pas de compression BSD
nodeflate (bool) à TRUE ne demande pas de compression 'deflate'
refuse-chap (bool) à TRUE, n'utilise pas la méthode d'authentification CHAP
refuse-eap (bool) à TRUE, n'utilise pas la méthode d'authentification EAP
refuse-mschap (bool) à TRUE, n'utilise pas la méthode d'authentification MSCHAP
refuse-mschapv2 (bool) à TRUE, n'utilise pas la méthode d'authentification MSCHAPv2
refuse-pap (bool) à TRUE, n'utilise pas la méthode d'authentification PAP
require-mppe (bool) à TRUE, mppe est requis pour la session PPP.
require-mppe-128 (bool) à TRUE MPPE 128-bits est requis pour la session PPP.

pppoe

name (chaîne) nom du paramétrage : pppoe
password (chaîne) Mot de passe utilisé pour authentifier le service PPPeE
password-flags (NMSettingSecretFlags) Flags indiquant comment manipuler la propriété password

service (chaîne) si spécifié, instruit PPPoE à seulement initier des session avec des concentrateurs d'accès.

username (chaîne) username pour l'authentification

proxy

browser-only (bool) Si la configuration proxy est pour les navigateurs uniquement

method (int32) Méthode pour la configuration proxy défaut : NM_SETTING_PROXY_METHOD_NONE(0)

name (chaîne) nom du paramétrage : proxy

pac-script (chaîne) script PAC pour la connexion

pac-url (chaîne) URL pour obtenir le fichier PAC

serial

baud (uint32) Vitesse pour la communication. Défaut : 57600

bits (uint32) Largeur d'octet de la communication. Défaut : 8

name (chaîne) nom du paramétrage : serial

parity (octet) Parité de la connexion : 69 (ASCII 'E') pour une parité paire, 111 (ASCII 'o') pour impaire, 110 (ASCII 'n') pour aucune parité

send-delay (uint64) Temps d'attente entre chaque octet envoyé au modem, en microsecondes. Défaut : 0

stopbits (uint32) Nombre de bits stop pour la communication, 1 ou 2. Défaut : 1.

team

config (chaîne) la configuration JSON pour l'interface team. La configuration devrait contenir une configuration acceptable pour teamd.

interface-name (chaîne) déprécié en faveur de connection.interface-name.

name (chaîne) nom du paramétrage : team

team-port

config (chaîne) la configuration JSON pour l'interface team. La configuration devrait contenir une configuration acceptable pour teamd.

name (chaîne) nom du paramétrage : team-port

tun

group (chaîne) Le group ID qui possède le périphérique. à NULL, tout le monde peut utiliser le périphérique

mode (uint32) Mode opératoire du périphérique NM_SETTING_TUN_MODE(1) pour créer un périphérique L3 et NM_SETTING_TUN_MODE_TAP(2) pour créer un périphérique L2

multi-queue (bool) à TRUE, l'interface supporte plusieurs descripteurs de fichier (queues) pour paralléliser l'envoi/réception des paquets, sinon, l'interface ne supporte qu'une seule queue. Défaut : FALSE

name (chaîne) nom du paramétrage : tun

owner (chaîne) Le user ID qui possède le périphérique. NULL, tout le monde peut utiliser le périphérique
pi (bool) à TRUE, l'interface ajoute 4 octets d'en-tête décrivant l'interface physique aux paquets. Défaut : FALSE
vnet-hdr (bool) à TRUE, les paquets IFF_VNET_HDR incluent un en-tête de réseau virtio. Défaut : FALSE

vlan

egress-priority-map (tableau de chaînes) pour les paquets sortants, une liste de mappage de priorités SKB Linux en priorités 802.1p. Le mappage est donné au format "from :to" et sont des entiers non-signés.

flags (NMVlanFlags) Flags qui contrôlent le comportement et les fonctionnalités de l'interface vlan.

NM_VLAN_FLAG_REORDER_HEADERS (0x1) réordonne les en-tête des paquets sortants, NM_VLAN_FLAG_GVRP (0x2) utilise le protocole GVRP, NM_VLAN_FLAG_LOOSE_BINDING (0x4) perd la liaison de l'interface de l'état opérant du périphérique maire. NM_VLAN_FLAG_MVRP (0x8) utilise le protocole MVRP.

id (uint32) Identifiant du vlan, de 0 à 4094. Défaut : 0

ingress-priority-map (tableau de chaînes) Pour les paquets entrants, une liste de mappage de priorité 802.1p en priorité SKB Linux.

interface-name (chaîne) déprécié en faveur de connection.interface-name

name (chaîne) nom du paramétrage : vlan

parent (chaîne) si donné, spécifie le nom de l'interface parent. non spécifié, la connexion doit contenir un paramètre "802-3-ethernet" avec une propriété "mac-address"

vpn

data (dictionnaire de chaîne) dictionnaire de paires clé/valeurs de données spécifique au plugin VPN.

namo (chaîne) nom du paramétrage : vpn

persistent (bool) Si le service VPN supporte la persistance, et cette propriété à TRUE, le VPN tente de rester connecté entre les changements de liens, jusqu'à déconnexion explicite

secrets (dictionnaire de chaîne) Dictionnaire de paires clé/valeur de secrets spécifique au plugin VPN, comme des mots de passe ou des clés privées

service-type (chaîne) Nom du service D-Bus du plugin VPN que ce paramètre utilise pour se connecter au réseau (ex : org.freedesktop.NetworkManager.vpnc pour le plugin vpnc)

timeout (uint32) timeout du service VPN pour établir la connexion. Certains services peuvent prendre du temps pour se connecter. 0 signifie le timeout par défaut : 60 secondes.

user-name (chaîne) Si la connexion VPN nécessite un username pour l'authentification.

vxlan

ageing (uint32) Durée de vie en secondes des entrées FDB apprises par le kernel. défaut : 300

destination-port (uint32) port UDP de destination pour communiquer au endpoint distant

id (uint32) Spécifie l'identifiant réseau VXLAN à utiliser

l2-miss (bool) Spécifie si les notification LL ADDR miss sont générés. défaut : FALSE

l3-miss (bool) Spécifie si les notification IP ADDR miss sont générés. défaut : FALSE

learning (bool) Spécifie si une adresse L2 inconnue et les IP sont entrée dans la learning base VXLAN. Défaut : TRUE

limit (uint32) Spécifie le nombre max d'entrées FDB. Défaut : 0 = illimité

local (chaîne) nom du paramétrage : vxlan

parent (chaîne) nom de l'interface parent

proxy (bool) Spécifie si le proxy ARP est activé. Défaut : FALSE

remote (chaîne) Spécifie l'adresse IP unicast de destination pour les paquets sortants quand l'adresse l2 n'est pas connue dans la forwarding base VXLAN, ou l'IP multicast à joindre

rsc (bool) Spécifie si le route short circuit est activé. Défaut : FALSE

source-port-max (uint32) port UDP source max pour communiquer au endpoint

source-port-min (uint32) port UDP de destination minimum

tos (uint32) Valeur TOS pour les paquets sortants

ttl (uint32) ttl à utiliser pour les paquets sortants

wimax

mac-address (tableau d'octets) Déprécié. Si spécifié, cette connexion s'applique au périphérique WiMAX qui matche cette adresse MAC.

name (chaîne) nom du paramétrage : wimax

network-name (chaîne) Déprécié. Nom du NSP du réseau WiMAX

802-3-ethernet

assigned-mac-address (chaîne) Adresse MAC clonée. Peut être une adresse MAC, ou un des mots clés suivant : preserve, permanent, random, ou stable.

auto-negotiate (bool) à TRUE, force l'auto-négociation de vitesse de port et le mode duplex. Défaut : FALSE

cloned-mac-address (tableau d'octets) déprécié en faveur de assigned-mac-address

duplex (chaîne) uniquement si auto-negotiate vaut 'off'. Configure le périphérique pour utiliser le mode duplex spécifié : half ou full.

generate-mac-address-mask (chaîne) si cloned-mac-address vaut random ou stable, cette propriété spécifie les bits qui sont fixes.

mac-address (tableau d'octets) si spécifié, cette connection ne s'applique qu'au périphérique dont l'adresse MAC permanent correspond

mac-address-blacklist (tableau de chaînes) Cette connection ne s'applique jamais aux périphérique dont l'adresse MAC permanente matche une de ces adresses

mtu (uint32) spécifie le mtu max pour cette connection

name (chaîne) nom du paramétrage : 802-3-ethernet

port (chaîne) Spécifie le type de port à utiliser si le périphérique support plusieurs méthodes d'attachement. tp (twisted Pair), aui (Attachment Unit Interface), bnc (Thin Ethernet) ou mii (Media Independant Interface).

s390-nettype (chaîne) Type de périphérique réseau s390 (qeth, lcs, ou ctc).

s390-options (dictionnaire de chaînes) dictionnaire de paires de clé/valeurs d'options s390. Les clés permises sont portno, layer2, portname et protocol.

speed (uint32) Peut être définis à une valeur supérieur à 0 quand auto-negotiate est à off. Dans ce cas, définis la vitesse en Mbit/s.

wake-on-lan (uint32) Options NMSettingWiredWakeOnLan à activer. peut être une des combinaisons : NM_SETTING_WIRED_WAKE_ON_LAN_PHY (0x2), NM_SETTING_WIRED_WAKE_ON_LAN_UNICAST (0x4), NM_SETTING_WIRED_WAKE_ON_LAN_MULTICAST (0x8), NM_SETTING_WIRED_WAKE_ON_LAN_BROADCAST (0x10), NM_SETTING_WIRED_WAKE_ON_LAN_ARP (0x20), NM_SETTING_WIRED_WAKE_ON_LAN_MAGIC (0x40) ou les valeurs spéciales NM_SETTING_WIRED_WAKE_ON_LAN_DEFAULT (0x1) (pour utiliser les paramètres globaux) et NM_SETTING_WIRED_WAKE_ON_LAN_IGNORE (0x8000) (pour désactiver la gestion de Wake-on-LAN dans NetworkManager).

wake-on-lan-password (chaîne) Mot de passe utilisé avec magic-packet-based Wake-on-LAN, représentée comme une adresse MAC. NULL indique qu'aucun mot de passe n'est requis.

802-11-wireless

assigned-mac-address (chaîne) Le nouveau champ pour l'adresse MAC clonée. Peut être une adresse MAC ou un des mots spécial "preserve", "random" ou "stable".

band (chaîne) bande de fréquence 802.11 : "a" (5GHz 802.11a), ou "bg" (2,4GHz 802.11).

bssid (tableau d'octets) Dirige le périphérique au point d'accès associé.

channel (uint32) Canal wireless à utiliser. Défaut : 0

cloned-mac-address (tableau d'octets) déprécié en faveur de assigned-mac-address

generate-mac-address-mask (chaîne) si cloned-mac-address vaut random ou stable, cette propriété spécifie les bits qui sont fixes.

hidden (bool) à TRUE, indique que ce réseau cache son SSID.

mac-address (tableau d'octets) si spécifié, cette connection ne s'applique qu'au périphérique dont l'adresse MAC permanent correspond

mac-address-blacklist (tableau de chaînes) Cette connection ne s'applique jamais aux périphérique dont l'adresse MAC permanente matche une de ces adresses

mac-address-randomization (uint32) déprécié en faveur de cloned-mac-address.
NM_SETTING_MAC_RANDOMIZATION_DEFAULT (0) (Utilise la valeur globale par défaut),
NM_SETTING_MAC_RANDOMIZATION_NEVER (1) (pas d'aléatoire),
NM_SETTING_MAC_RANDOMIZATION_ALWAYS (2).

mode (chaîne) mode réseau Wi-Fi : "infrastructure", "adhoc" ou "ap".

mtu (uint32) mtu pour les paquets transmis

name (chaîne) nom du paramétrage : 802-11-wireless

powersave (uint32) NM_SETTING_WIRELESS_POWERSAVE_DISABLE (2),
NM_SETTING_WIRELESS_POWERSAVE_ENABLE (3), NM_SETTING_WIRELESS_POWERSAVE_IGNORE (1),
NM_SETTING_WIRELESS_POWERSAVE_DEFAULT (0)

rate (uint32) Dirige de périphérique pour utiliser seulement le bitrate spécifié pour la communication avec le point d'accès, en Kb/s.

security déprécié

seen-bssids (tableau de chaînes) Une liste de BSSID (formaté sous forme d'adresse MAC) qui ont été détectés comme partie de la connection Wi-Fi. Géré par NetworkManager

ssid (tableau d'octets) SSID du réseau Wi-Fi. Doit être spécifié

tx-power (uint32) le périphérique utilise la puissance de transmission spécifiée, en dBm.

802-11-wireless-security

auth-alg (chaîne) avec WEP, indique l'algorithme d'authentification requise "open", "shared" "leap".

group (tableau de chaînes) Liste d'algorithmes de chiffrement qui empêche les connection aux réseaux Wi-Fi qui n'utilisent pas un de ces algorithmes. "wep40", "wep104", "tkip" ou "ccmp"

key-mgmt (chaîne) Gestion de clé utilisé pour la connection "none" (WEP), "ieee8021x" (Dynamic WEP), "wpa-none" (Ad-Hoc WPA-PSK), "wpa-psk" (infrastructure WPA-PSK), ou "wpa-eap" (WPA-Enterprise).

leap-password (chaîne) password de connexion pour les connexions LEAP

leap-password-flags (NMSettingSecretFlags) Flags indiquant comment gérer la propriété leap-password.

leap-username (chaîne) username pour la connexion

name (chaîne) nom du paramétrage : 802-11-wireless-security

pairwise (tableau de chaînes) Liste d'algorithme de chiffrement d'appairement permis pour les connections Wi-Fi

proto (tableau de chaînes) Liste de chaînes spécifiant les versions WPA permises "wpa" ou "rsn" (autorise WPA2/RSN).

psk (chaîne) Clé pré-partagée pour les réseaux WPA.

psk-flags (NMSettingSecretFlags) Flags indiquant comment gérer la propriété psk

wep-key-flags (NMSettingSecretFlags) Flags indiquant comment gérer les propriétés wep-key[0-3].

wep-key-type (NMWepKeyType) Contrôle l'interprétation des clés WEP. NM_WEP_KEY_TYPE_KEY (1) (la clé a 10 ou 26 caractères hexa, ou 5 ou 13 caractères ASCII) ou NM_WEP_KEY_TYPE_PASSPHRASE (2)

wep-key0 (chaîne) Clé WEP d'index 0

wep-key1 (chaîne) Clé WEP d'index 1

wep-key2 (chaîne) Clé WEP d'index 2

wep-key3 (chaîne) Clé WEP d'index 3

wep-tx-keyidx (uint32) Si WEP statique est utilisé et un index de clé WEP non-défaut est utilisé par l'AP, place cet index ici. (0 à 3)

Types de flags secret

0x0 Le système doit fournir et stocker le secret

0x1 Un agent userspace gère le secret

0x2 Le secret n'est pas sauvegardé et est demandé à l'utilisateur à chaque fois.

0x4 Indique que le secret n'est pas requis et ne devrait pas être demandé à l'utilisateur