Guide de démarrage rapide - Configuration et politiques simplifiées du SD-WAN Catalyst

Table des matières

- Introduction
- Résumé
  - Nouveaux déploiements
  - Déploiements existants
- Améliorations de l'expérience utilisateur et simplification opérationnelle
- Définition de la hiérarchie réseau et des composants du système
  - Hiérarchie réseau
  - Constructions système
- Workflows
- Groupes de configuration
  - Exemples de déploiement de groupes de configuration
    - Cas d'utilisation 1 : Client du gouvernement
    - Cas d'utilisation 2 : Client de détail
  - Associer
  - Déploiement
  - Réutilisabilité
  - Profil d'objet de stratégie
  - Minuteur de restauration
- Catalogue d'applications
- Groupes de stratégies
  - Priorité des applications et SLA
    - Mode simple
    - Mode avancé
    - Qualité de service
    - Routage sensible aux applications
    - Politique Du Trafic
  - Sécurité intégrée
  - Passerelle Internet sécurisée/Périphérie de service sécurisé
  - Sécurité DNS
  - Groupes d'intérêt
  - Associer et déployer
  - Stratégies localisées
- Topologie
  - Topologie et VPN
    - Mappage d'un nom VPN sur plusieurs ID VPN
    - Mappage de plusieurs noms VPN sur le même ID VPN
- Intégration
- Marquage

- Ajouter une balise
- Règles de balise dans le groupe de configuration
- Illustration

Déploiements existants

- Groupes de configuration
- Groupes de stratégies
- Topologie

Outil de conversion de configuration

- Portée
- Détails d'accès
- Marche à suivre
  - Flux de travail SD-WAN connecté au gestionnaire
  - Flux De Travail À Air Interdit
  - Post-Conversion
- Considérations
- Communiquer avec le service de soutien à la clientèle

20.12 Considérations

Informations connexes

Introduction

Ce document décrit un guide de démarrage rapide pour une configuration et des politiques simplifiées dans Catalyst SD-WAN.

Résumé

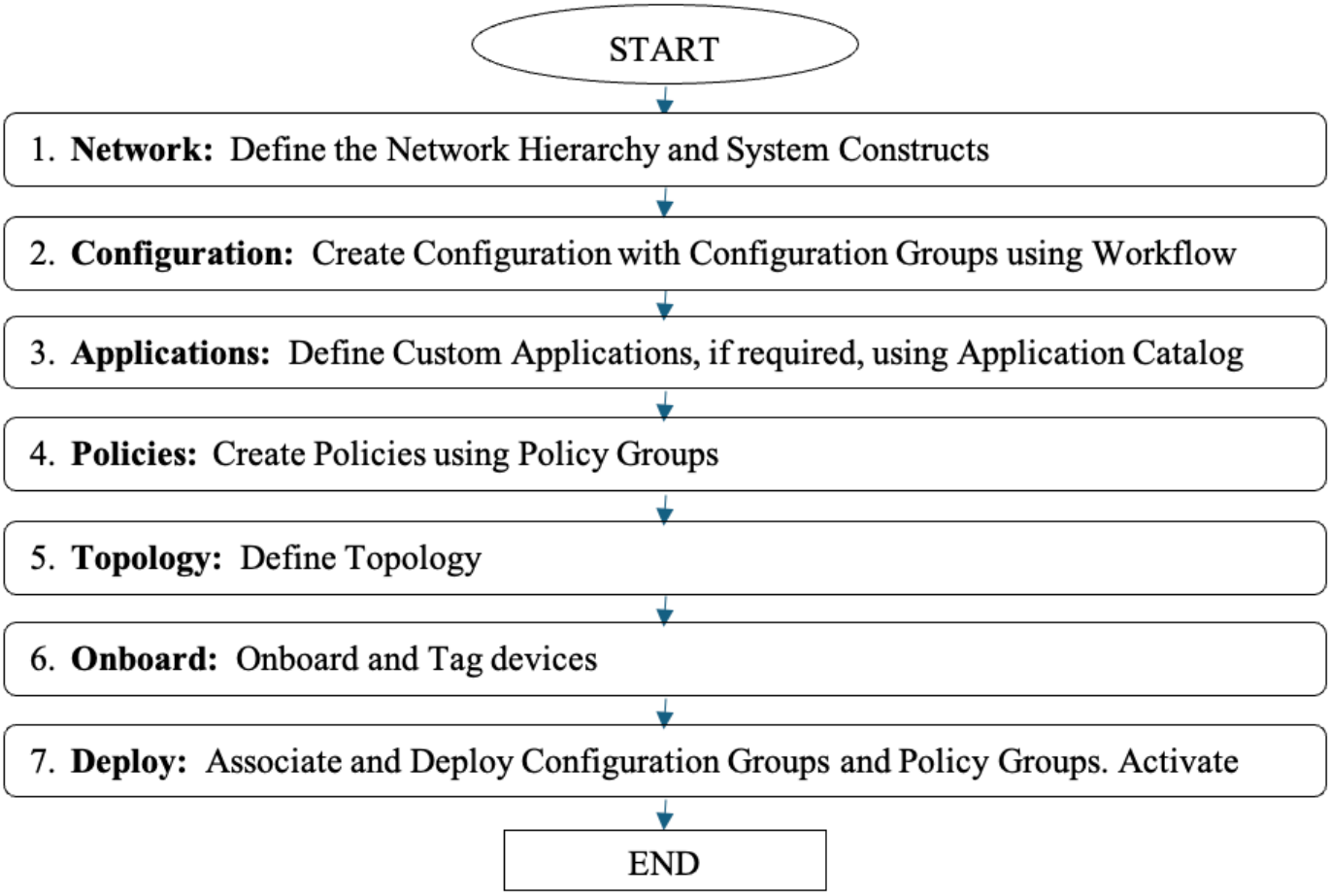
Avec le logiciel Cisco Catalyst SD-WAN version 20.12/17.12, il est recommandé aux utilisateurs de commencer la migration d'une configuration traditionnelle basée sur des modèles de périphériques et de fonctionnalités vers la nouvelle approche de configuration basée sur des groupes de configuration et des groupes de politiques. Dans ce document, des détails importants pour la nouvelle approche de configuration sont décrits.

L'objectif principal de ce document est de servir de guide pour commencer à utiliser de nouvelles constructions pour la configuration, les stratégies et l'intégration, avec la version 20.12. Le document ne couvre pas les explications des fonctionnalités individuelles.

Nouveaux déploiements

Afin d'utiliser avec succès la nouvelle approche de configuration, vous devez exécuter ces étapes :

1. Réseau: Définissez la hiérarchie du réseau et les composants système.
2. Configuration: Créer une configuration avec des groupes de configuration à l'aide du workflow.
3. Applications : Définissez des applications personnalisées, si nécessaire, à l'aide du catalogue d'applications.
4. Politiques : Créez des stratégies à l'aide de groupes de stratégies.
5. Topologie: Définissez la topologie.
6. À bord : périphériques embarqués et Tag.
7. Déployer : associer et déployer des groupes de configuration et des groupes de stratégies. Activez la topologie.



Organigramme des nouveaux déploiements

Déploiements existants

1. Exécutez les étapes mentionnées dans la section Déploiements existants.
2. Utilisez l'outil Conversion afin de convertir la configuration et les stratégies existantes en nouveaux groupes de configuration et groupes de stratégies.

Améliorations de l'expérience utilisateur et simplification

opérationnelle

Cisco Catalyst SD-WAN offre une expérience utilisateur améliorée et simplifie les opérations.

- Interface utilisateur commune : Un nouveau cadre d'expérience utilisateur (UX) a été introduit dans Catalyst SD-WAN Manager et d'autres produits Cisco, afin d'assurer la cohérence dans l'UX et de fournir une apparence commune à tous les produits.
- Configuration: Simplification de la configuration et de la création et du déploiement de politiques grâce à des workflows intuitifs basés sur des intentions et à l'utilisation des valeurs par défaut intelligentes recommandées par Cisco.
- Surveillance : Des informations complètes sur les performances et l'état du réseau et des applications avec de nouveaux widgets et des tableaux de bord personnalisables et améliorés.
- Dépannage : Vues dynamiques de la topologie du site et du réseau, accès aux outils de dépannage contextuels, rapports sur les performances du réseau et des applications planifiés.

Avantages:

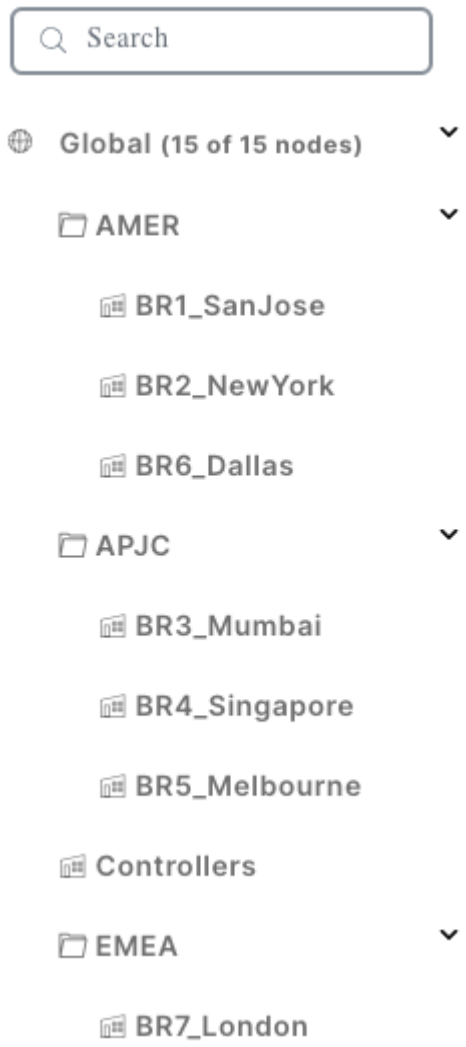
Facilité d'utilisation	Workflows intuitifs et guidés
Prolifération de configuration	Réduction de la prolifération (modèle agnostique, réutilisation, structure)
Création de configuration	Plus rapide et plus facile avec des valeurs par défaut intelligentes
Modification de configuration	Modifier maintenant, déployer sélectivement plus tard
Visibilité	Nouveaux tableaux de bord, contrôle des performances des applications/sites
Conseils de dépannage	Topologie du site, conseils sur les outils de dépannage

Définition de la hiérarchie réseau et des composants du système

Hiérarchie réseau

Fournit une notion de « hiérarchie », c'est-à-dire des sites, des régions et des zones, pour le réseau. Vous pouvez le créer en fonction de votre réseau.

Exemple :



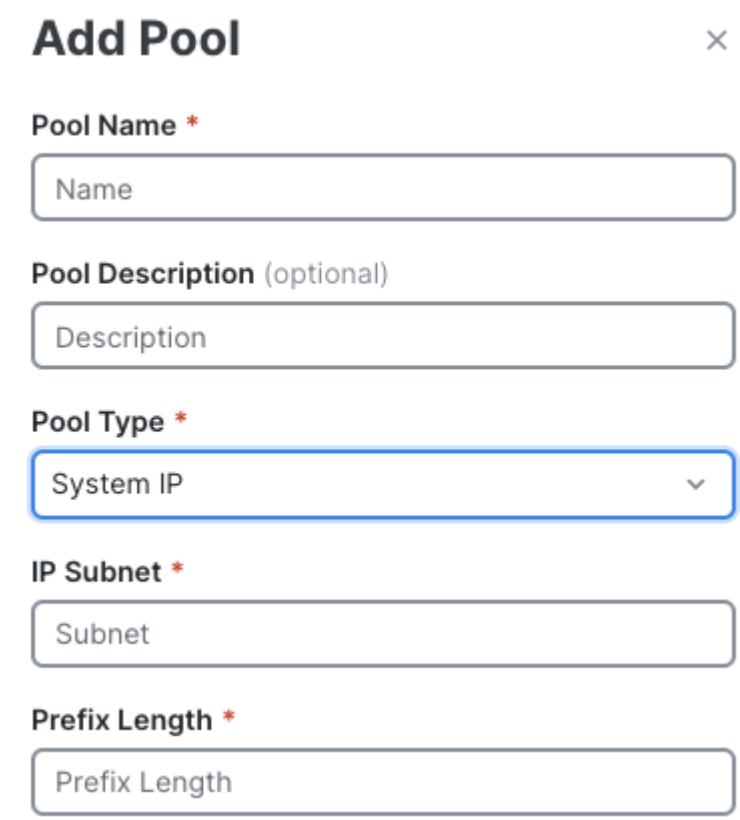
Gestionnaire de hiérarchie réseau (NHM)

Cela permet de définir des noms de sites conviviaux, ce qui contribue à simplifier les opérations.

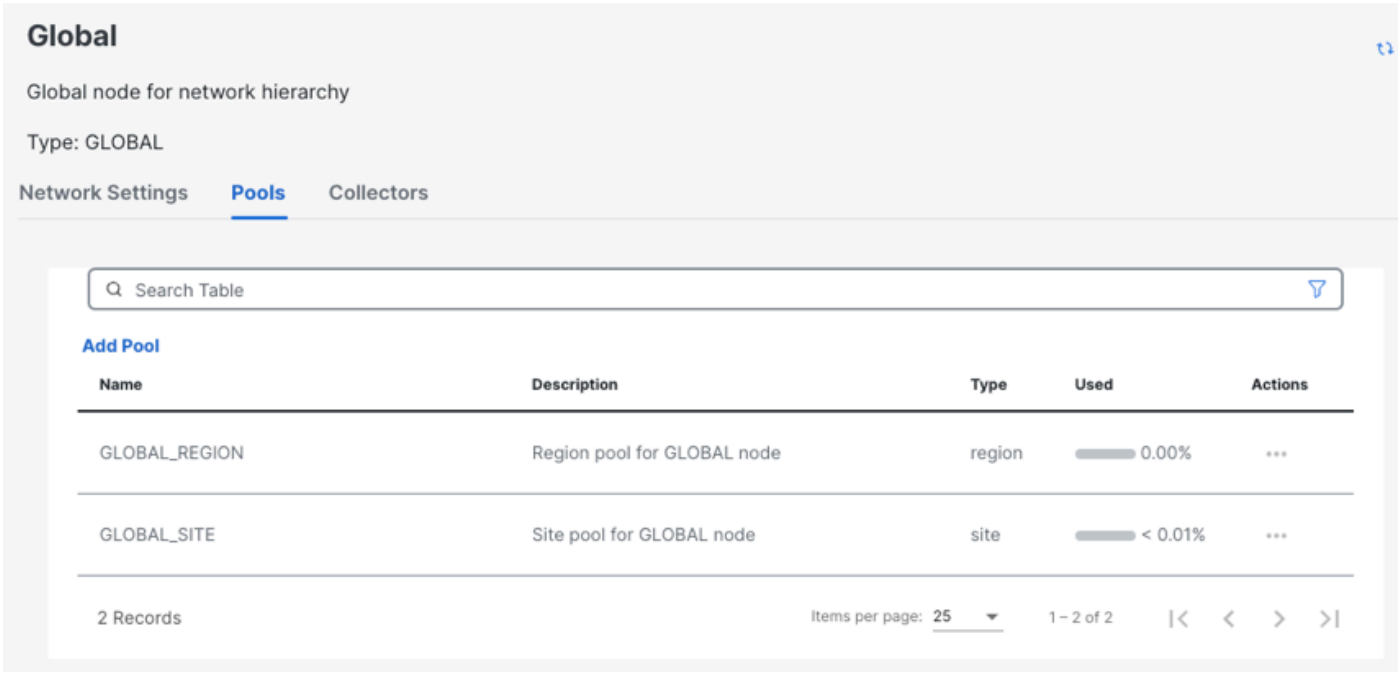
Constructions système

Ces pools automatisent les affectations d'ID de site et d'IP système lors du déploiement de la configuration des périphériques.

Vous pouvez définir le pool d'adresses IP pour les affectations automatiques d'adresses IP système. L'ID de site est affecté à partir du pool Global_Site.



Ajouter des paramètres de pool



Afficher et gérer les pools

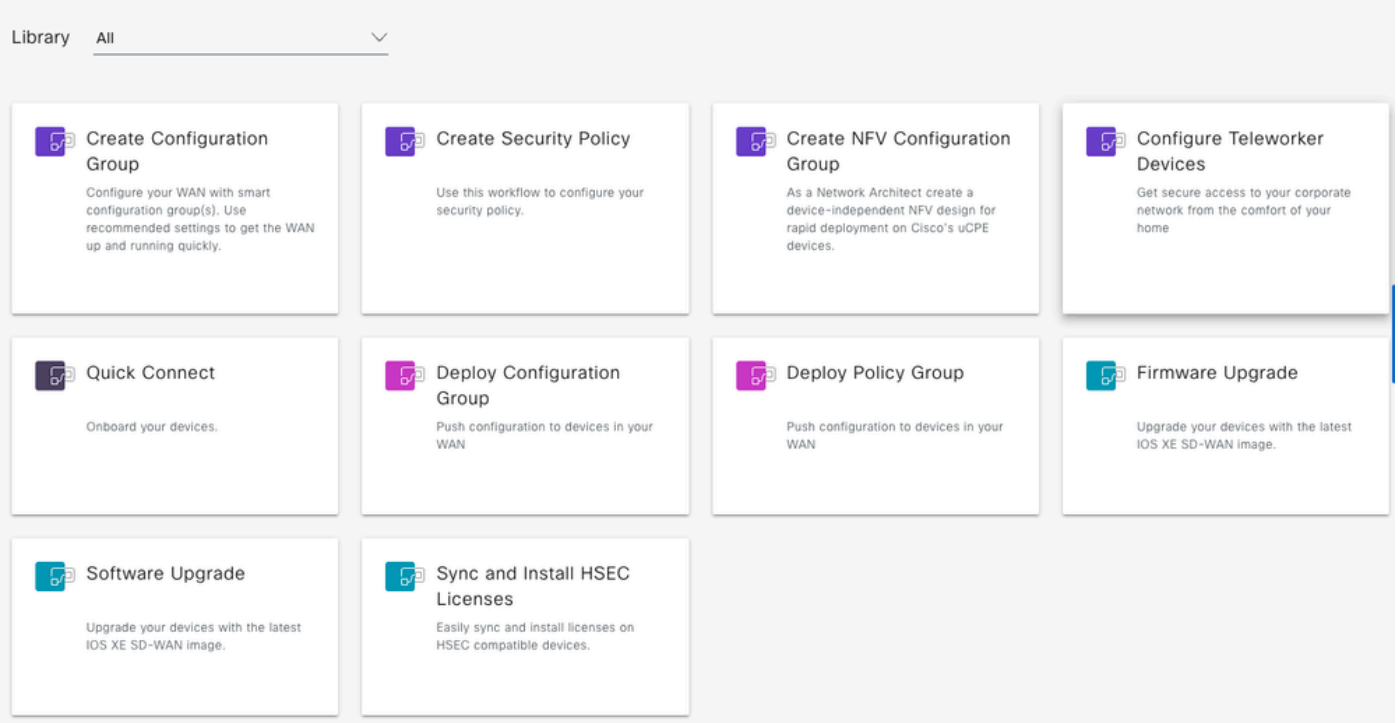
Workflows

Un flux de travail est un ensemble d'étapes guidées qui vous aident à effectuer facilement une

tâche donnée.

- L'objectif d'un workflow est d'aider les utilisateurs débutants à créer facilement des configurations et à les déployer sur le périphérique.
- La plupart des boutons/paramètres de configuration sont définis sur les valeurs par défaut recommandées par Cisco.
- Les utilisateurs ne doivent spécifier que quelques configurations.
- Les boutons de configuration avancée sont disponibles en dehors du workflow, où le groupe de configuration peut être modifié manuellement.

Une bibliothèque de workflows répertorie tous les workflows disponibles.

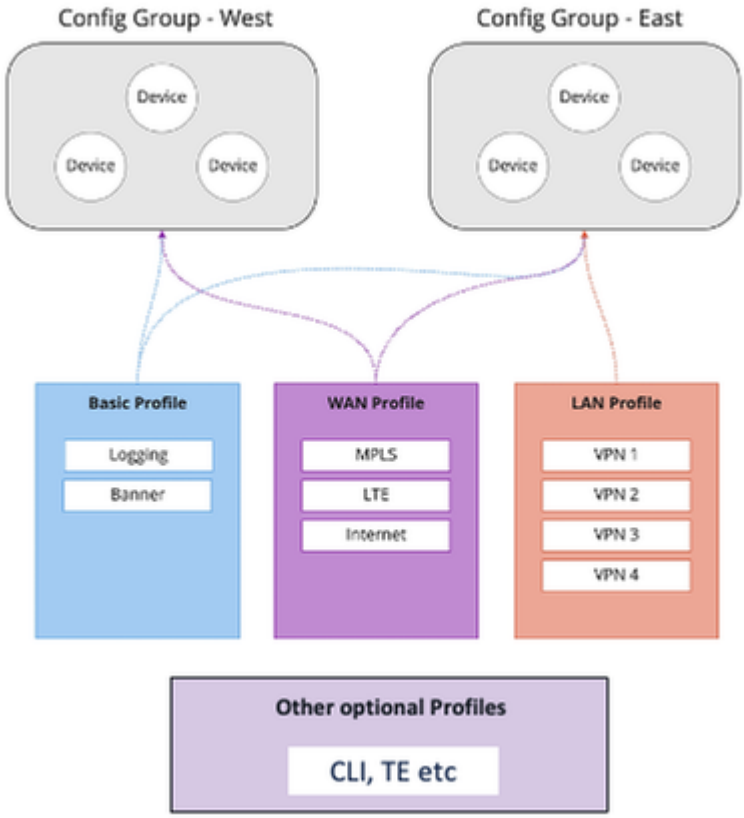


Bibliothèque de workflows

Groupes de configuration

Les groupes de configuration constituent une nouvelle approche de la configuration du fabric basée sur des principes de simplicité, de réutilisation et de structure.

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/config-groups/configuration-group-guide/using-config-groups.html.



Structure des groupes de configuration

Groupes de configuration :

- Regroupement logique de périphériques partageant un objectif commun au sein du WAN.
- L'utilisateur définit et peut personnaliser ce regroupement en fonction de ses besoins professionnels.

Exemple ; Est/Ouest, Amériques/APJC/EMEAR, Retail Store/Distribution Center.

Profils de fonctionnalités :

- « Compartiments » flexibles de configuration pouvant être partagés entre plusieurs groupes de configuration.
- Créez des profils de fonction en fonction des fonctions requises.
- Rassemblez les profils afin de compléter la configuration des périphériques, comme les blocs de construction.
- Créer, enregistrer et réutiliser.

Exemple ; Profil de base, profil WAN, profil LAN.

Exemples de déploiement de groupes de configuration

Remarque :

- Les groupes de configuration sont indépendants du modèle de périphérique.
- Les profils de fonction peuvent être partagés entre plusieurs groupes de configuration.

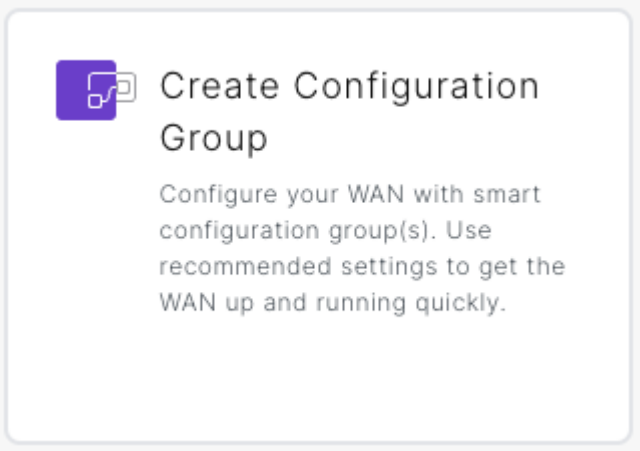
Cas d'utilisation 1 : Client du gouvernement



Exemple d'utilisation 1 - Groupes de configuration

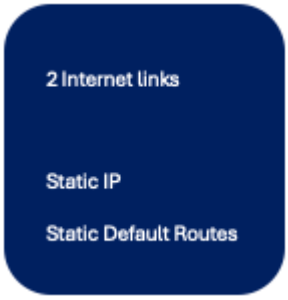
HUB du groupe de configuration :

Exécutez le workflow Créer un groupe de configuration.



Option de workflow Créer un groupe de configuration

Profil WAN



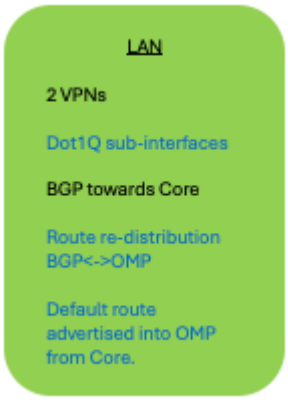
Exemple d'utilisation 1 : profil WAN 1

Le workflow permet de générer la configuration complète du profil WAN pour cet exemple d'utilisation.

Les entités telles que l'adresse IP statique réelle, l'adresse IP/sous-réseau/tronçon suivant de la route statique par défaut, etc., peuvent être spécifiées comme globales ou spécifiques au périphérique.

L'option spécifique au périphérique peut être spécifiée avec des valeurs réelles pendant le déploiement du groupe de configuration sur les périphériques.

Profil LAN



Exemple d'utilisation 1 - LAN Profile 1

À l'aide du workflow, vous pouvez générer la plupart de la configuration du profil de réseau local pour ce cas d'utilisation.

- 2 VPN
- Routage BGP dans chacun des VPN (numéro de système autonome, préfixes réseau, voisins)

Les entités telles que les sous-interfaces Dot1Q réelles et toute autre entité marquée comme spécifique au périphérique peuvent être spécifiées avec des valeurs réelles lors du déploiement du groupe de configuration sur les périphériques.

Remarque : La configuration avancée, telle que la redistribution de route et l'annonce de route par défaut, doit être configurée après le workflow, en modifiant manuellement le groupe Configuration, ainsi que les sous-interfaces si celles-ci doivent être utilisées pendant le déploiement.

Profil système



Exemple d'utilisation 1 : profil système 1

En utilisant le workflow, la plupart de la configuration du profil système pour ce cas d'utilisation

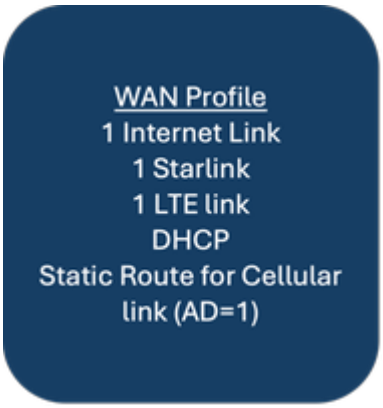
peut être générée : OMP, AAA, NTP, Logging, etc.

Remarque : La configuration avancée, telle que la redistribution OMP-BGP et toute autre modification apportée aux fonctionnalités du système, telles que OMP, AAA, NTP, etc., doit être configurée après le workflow, en modifiant manuellement le groupe Configuration.

Groupe de configuration SiteType1 :

Exécutez le workflow Créer un groupe de configuration.

Profil WAN



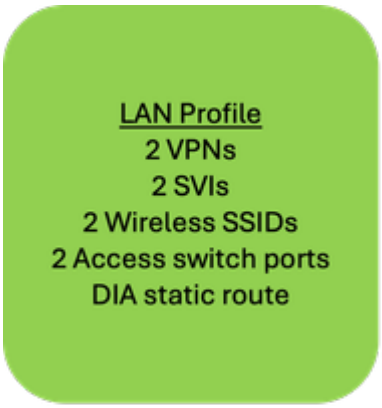
Exemple d'utilisation 1 : profil WAN 2

Le workflow permet de générer la plupart de la configuration du profil WAN de ce cas d'utilisation. Interfaces Ethernet pour Internet et Starlink. DHCP.

Remarque : L'interface cellulaire pour la liaison LTE, y compris la route statique, doit être configurée après le workflow, en modifiant manuellement le groupe de configuration.

---

profil LAN



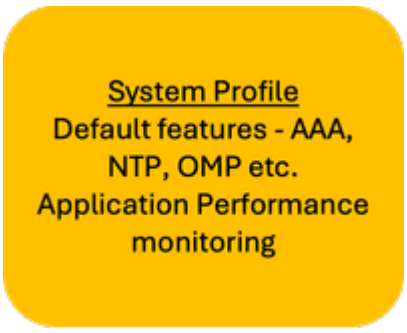
Exemple d'utilisation 1 - LAN Profile 2

À l'aide du workflow, une partie de la configuration du profil LAN de ce cas d'utilisation peut être générée. 2 VPN, route statique DIA.

Les entités telles que les sous-interfaces Dot1Q réelles et toute autre entité marquée comme spécifique au périphérique peuvent être spécifiées avec des valeurs réelles lors du déploiement du groupe de configuration sur les périphériques.

Remarque : Les interfaces SVI, les SSID sans fil, les ports de commutation d'accès, etc., doivent être configurés après le workflow, en modifiant manuellement le groupe Configuration.

Profil système

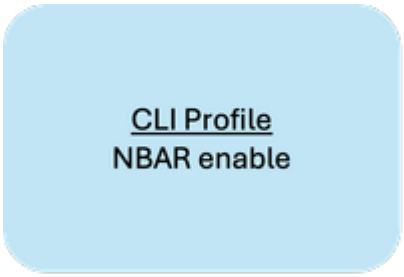


Exemple d'utilisation 1 : profil système 2

En utilisant le workflow, la plupart de la configuration du profil système pour ce cas d'utilisation peut être générée : OMP, AAA, NTP, Logging, etc.

Remarque : La configuration avancée, telle que la surveillance des performances de l'application, doit être configurée après le workflow, en modifiant manuellement le groupe Configuration.

Profil CLI



Exemple d'utilisation 1 - CLI Profile 2

Les fonctionnalités non prises en charge via l'interface utilisateur graphique, telles que l'activation de la visibilité sur les applications et les flux (NBAR), peuvent être configurées à l'aide d'un profil CLI.

Visibilité des applications/flux :

Afin d'activer la visibilité des applications et des flux, utilisez le profil/paquet CLI.

(Dans les versions 20.13 et ultérieures, il est disponible sous Paramètres avancés dans Groupe de stratégies)

Cependant, dans la version 20.12, si une stratégie AAR est configurée, alors la visibilité sur les applications/flux est activée. Il n'est pas nécessaire de configurer ce paramètre à l'aide du profil/colis CLI.

Type de site du groupe de configuration2 :

Exécutez le workflow Créer un groupe de configuration.

Profil WAN



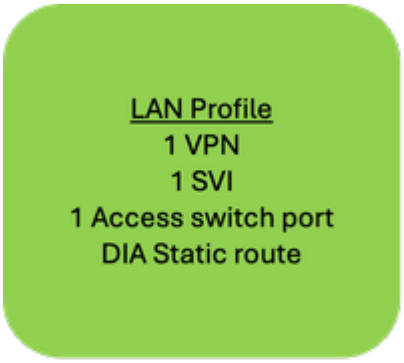
Exemple d'utilisation 1 : profil WAN 3

Le workflow permet de générer la plupart de la configuration du profil WAN de ce cas d'utilisation. Interface Ethernet pour Internet. DHCP.

Remarque : L'interface cellulaire pour la liaison LTE, y compris la route statique, doit être configurée après le workflow, en modifiant manuellement le groupe de configuration.

---

profil LAN



Exemple d'utilisation 1 - LAN Profile 3

À l'aide du workflow, une partie de la configuration du profil LAN de ce cas d'utilisation peut être

générée. 1 VPN, route statique DIA.

Les entités telles que les sous-interfaces Dot1Q réelles et toute autre entité marquée comme spécifique au périphérique peuvent être spécifiées avec des valeurs réelles lors du déploiement du groupe de configuration sur les périphériques.



Remarque : L'interface SVI, le port du commutateur d'accès, etc., doivent être configurés après le workflow, en modifiant manuellement le groupe de configuration.

Profil système :

Identique à Configuration Group SiteType1.

Profil CLI :

Identique à Configuration Group SiteType1.

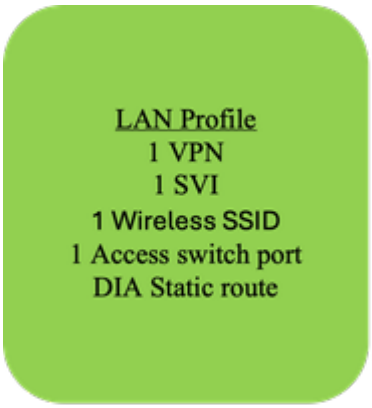
Type de site du groupe de configuration3 :

Exécutez le workflow Créer un groupe de configuration.

Profil WAN :

Identique à Configuration Group SiteType2.

Profil LAN



Exemple d'utilisation 1 - LAN Profile 4

À l'aide du workflow, une partie de la configuration du profil LAN de ce cas d'utilisation peut être générée. 1 VPN, route statique DIA.

Les entités telles que les sous-interfaces Dot1Q réelles et toute autre entité marquée comme spécifique au périphérique peuvent être spécifiées avec des valeurs réelles lors du déploiement du groupe de configuration sur les périphériques.

Remarque : L'interface SVI, le SSID sans fil, le port du commutateur d'accès, etc., doivent être configurés après le workflow, en modifiant manuellement le groupe de configuration.

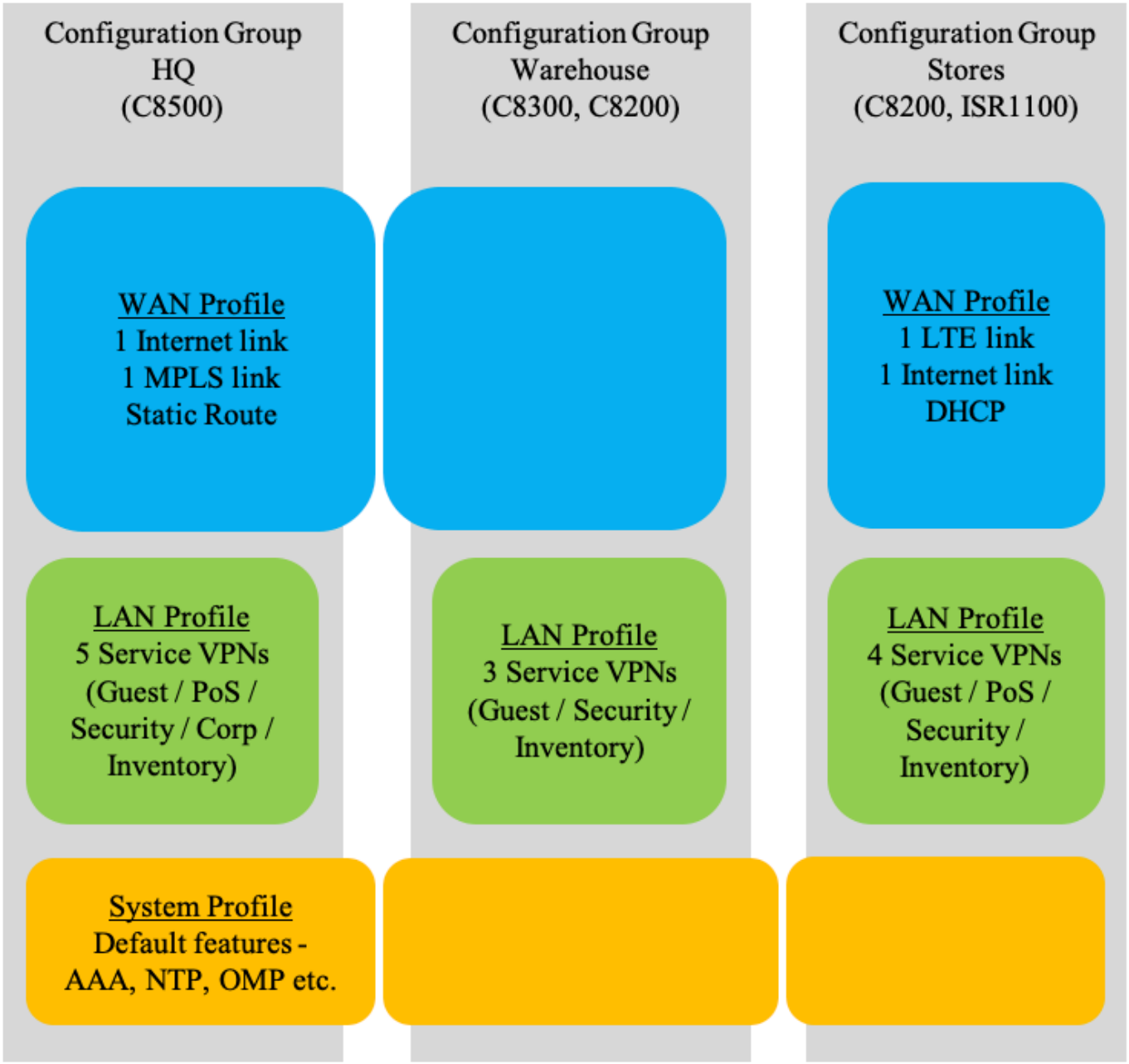
Profil système :

Identique à Configuration Group SiteType1.

Profil CLI :

Identique à Configuration Group SiteType1.

Cas d'utilisation 2 : Client de détail



Exemple d'utilisation 2 - Groupes de configuration

Siège et entrepôt du groupe de configuration

Exécutez le workflow Créer un groupe de configuration.

Profil WAN :

À l'aide du workflow, toute la configuration du profil WAN de ce cas d'utilisation peut être générée.

Profil LAN :

À l'aide du workflow, toute la configuration du profil LAN de ce cas d'utilisation peut être générée.

Les entités telles que les sous-interfaces Dot1Q réelles et toute autre entité marquée comme spécifique au périphérique peuvent être spécifiées avec des valeurs réelles lors du déploiement du groupe de configuration sur les périphériques.

Profil système :

À l'aide du workflow, toute la configuration du profil système de ce cas d'utilisation peut être générée.



Remarque : Si des modifications sont requises ou si une configuration avancée telle que la surveillance des performances des applications est requise, elles doivent être configurées après le workflow, en modifiant manuellement le groupe Configuration.

Magasins de groupes de configuration :

Exécutez le workflow Créer un groupe de configuration.

Profil WAN :

Le workflow permet de générer la plupart de la configuration du profil WAN de ce cas d'utilisation.



Remarque : L'interface cellulaire pour la liaison LTE, y compris le routage, doit être configurée après le workflow, en modifiant manuellement le groupe Configuration.

Profil LAN :

À l'aide du workflow, toute la configuration du profil LAN de ce cas d'utilisation peut être générée.

Les entités telles que les sous-interfaces Dot1Q réelles et toute autre entité marquée comme

spécifique au périphérique peuvent être spécifiées avec des valeurs réelles lors du déploiement du groupe de configuration sur les périphériques.

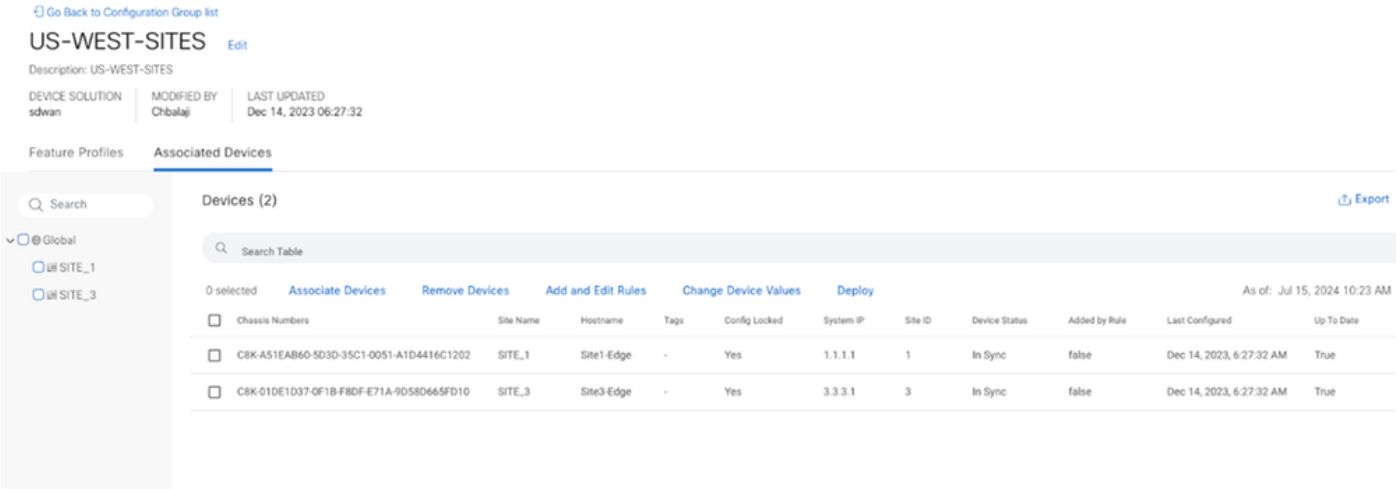
Profil système :

Identique à Configuration Group HQ et Warehouse.

Associer

Dans la page Configuration Group edit (Configuration -> Configuration Groups), vous pouvez associer des périphériques au groupe de configuration.

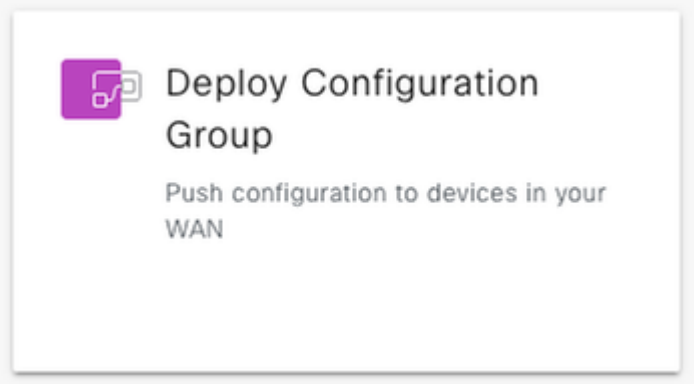
Cliquez sur Associer des périphériques et parcourez les étapes du workflow.



Associer un périphérique - Groupes de configuration

Déploiement

Exécutez le workflow Déployer le groupe de configuration.



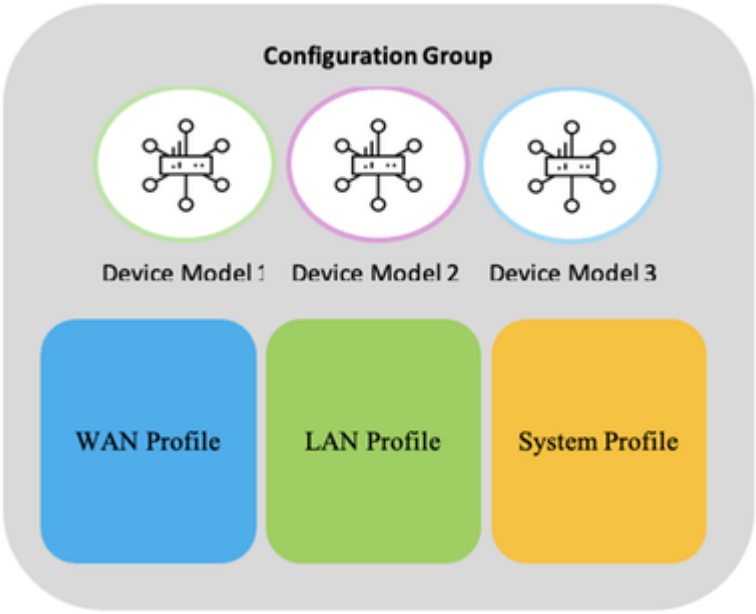
Déployer le workflow de groupe de configuration

Remarque :

- Dans le groupe de configuration, la modification des valeurs du périphérique modifie uniquement la valeur dans la base de données du gestionnaire et n'applique PAS les modifications à un périphérique. Si vous voulez que la modification ait lieu immédiatement, vous devez déployer les modifications.
- L'exportation des valeurs des variables de périphérique (sous forme de fichier CSV) peut être effectuée dans le workflow Déployer à l'étape Ajouter/Vérifier la configuration du périphérique.

Réutilisabilité

1. Les groupes de configuration sont indépendants du modèle de périphérique.



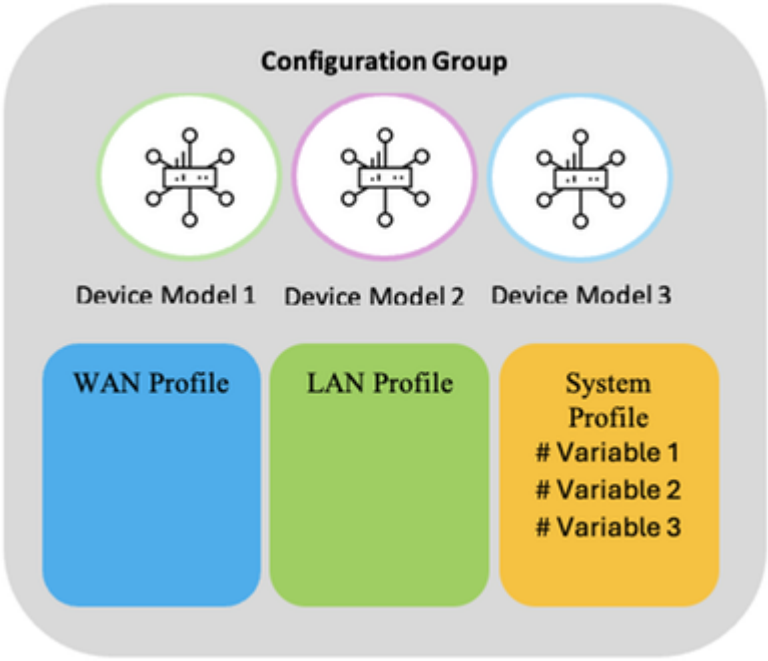
Groupe de configuration - Modèle de périphérique agnostique

Remarque : Si une configuration particulière n'est pas prise en charge sur un modèle de périphérique, la transmission correspondante du lot de fonctionnalités n'a pas lieu et un message approprié est affiché dans le cadre de la tâche de déploiement.

Exemple : Un périphérique ne prend pas en charge le Wi-Fi, mais le groupe de configuration contient un colis Wi-Fi. Au moment du déploiement, la configuration du paquet Wi-Fi est ignorée et le message de la tâche de déploiement informe que le push de configuration Wi-Fi a été ignoré.

---

2. Utilisez les variables de configuration - valeurs spécifiques au périphérique.

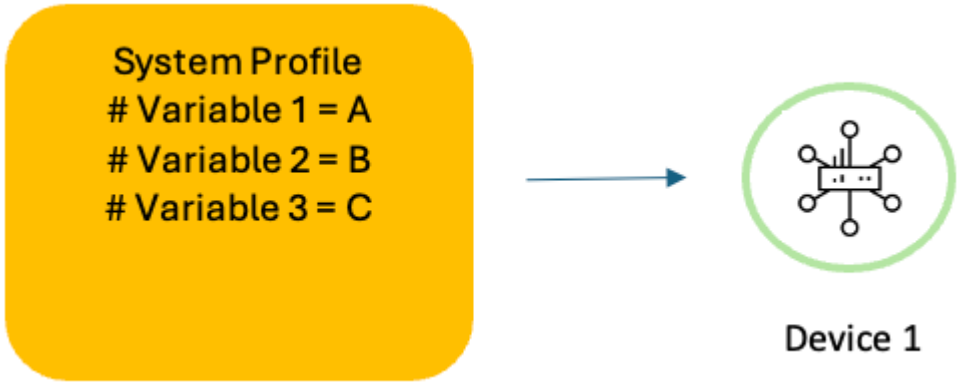


Groupe de configuration - Variables propres au périphérique

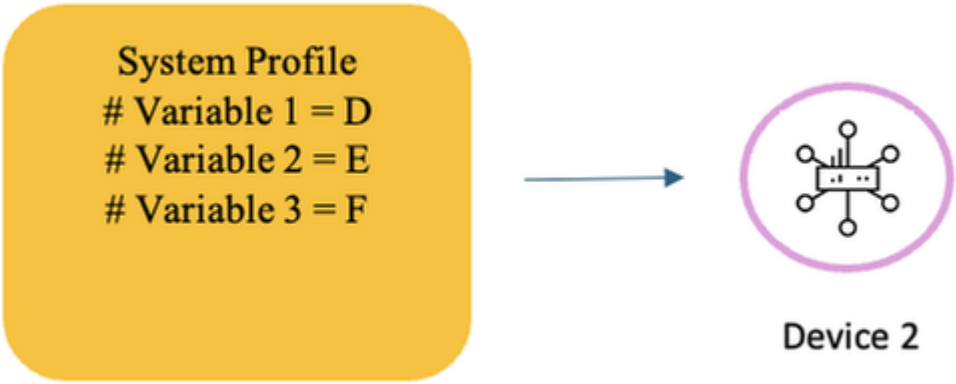
Un profil de fonctionnalité peut avoir une configuration spécifique au périphérique, similaire aux variables de modèle.

Exemple : Adresse IP de l'interface, numéros de port, nom de l'interface, etc.

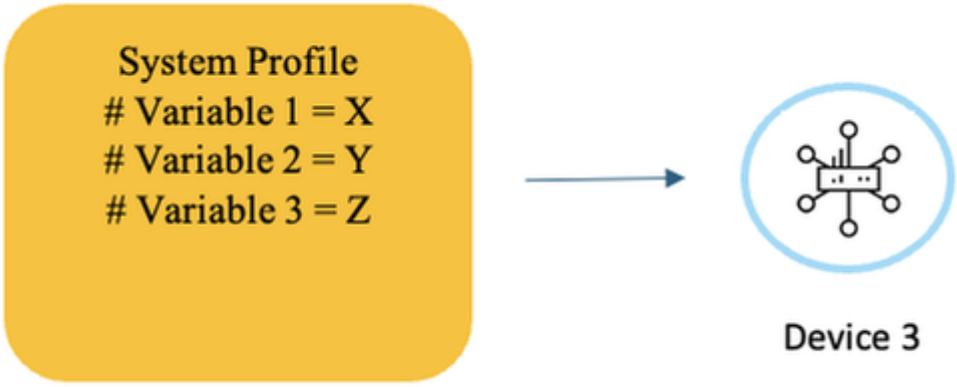
Ces valeurs spécifiques au périphérique peuvent être fournies au moment du déploiement. Et il peut être différent pour différents périphériques.



Groupe de configuration - Variables propres au périphérique - Exemple 1



Groupe de configuration - Variables propres au périphérique - Exemple 2



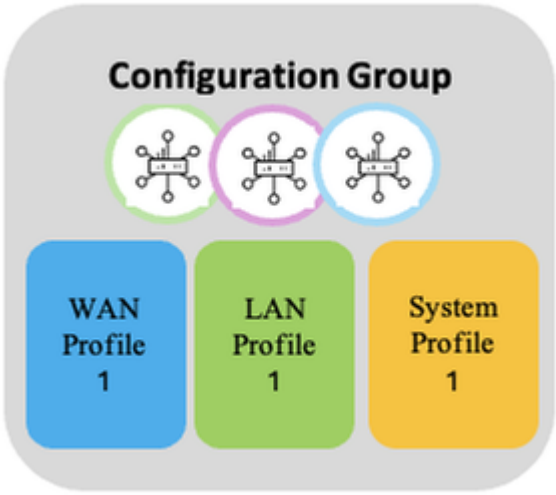
Groupe de configuration - Variables propres au périphérique - Exemple 3

3. Réutilisation des profils de fonction.

Les profils de fonction peuvent être réutilisés dans plusieurs groupes de configuration.

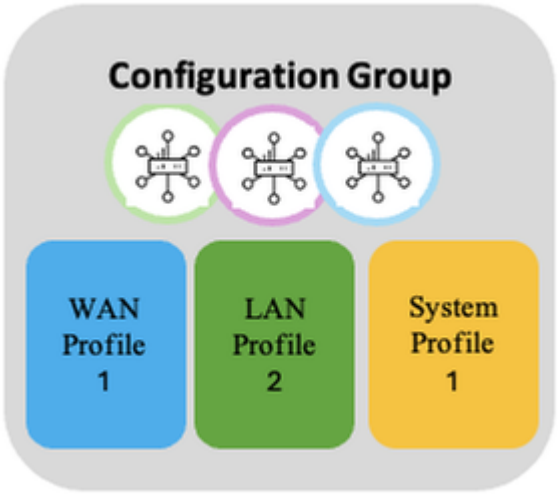
Illustration :

Pour plusieurs périphériques, si les configurations WAN et système sont identiques et qu'elles diffèrent uniquement dans la configuration LAN, par exemple, les profils WAN et système peuvent être réutilisés dans leurs groupes de configuration tout en ayant un profil LAN différent dans chacun d'eux.



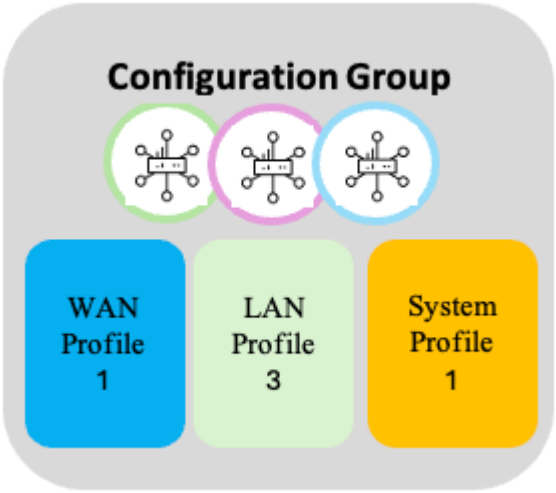
Réutilisation des profils de fonction - 1

Profil LAN 1



Réutilisation des profils de fonction - 2

Profil LAN 2



Réutilisation des profils de fonction - 3

Profil LAN 3

Profil d'objet de stratégie

Le profil d'objet de stratégie contient tous les groupes d'intérêt ou listes qui sont utilisés avec les stratégies localisées (ACL, stratégie de routage, etc.) dans les groupes de configuration, les stratégies dans les groupes de stratégies et la topologie.

Il s'agit d'un profil partagé (global) qui est utilisé dans les groupes de configuration, les groupes de stratégies et la topologie.

Minuteur de restauration

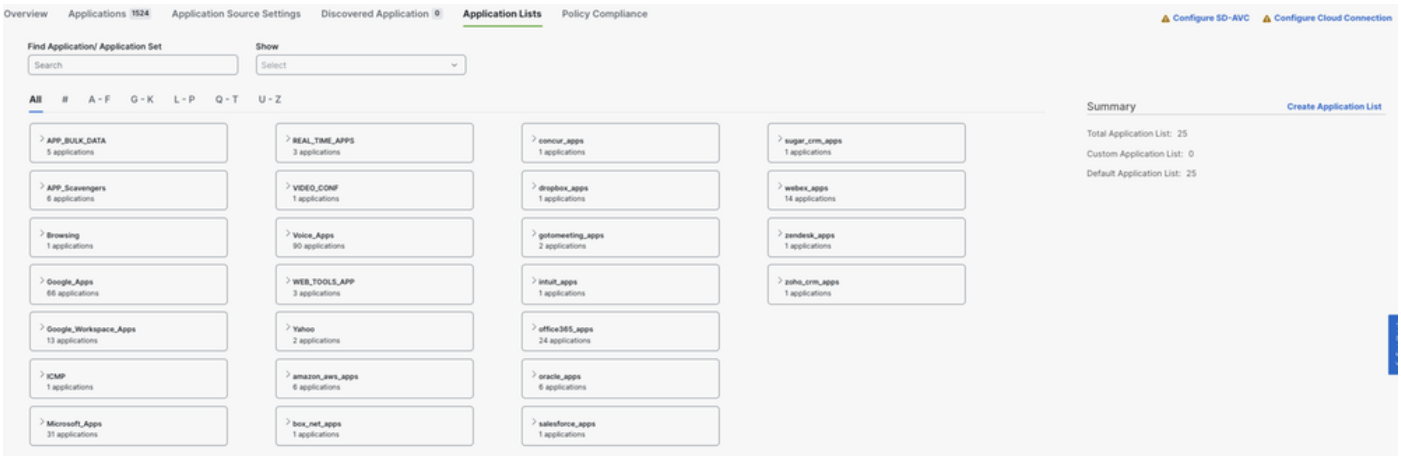
Le temporisateur de retour arrière est fixé à 5 minutes avec les groupes de configuration (en raison de l'utilisation d'un nouveau modèle d'extraction sur NETCONF, il n'est plus nécessaire de le configurer).

Catalogue d'applications

Les périphériques traditionnels étaient capables de manipuler les flux de trafic par la mise en correspondance conditionnelle des adresses IP source et/ou de destination, des ports source/de destination et des protocoles. Étant donné que de plus en plus d'applications dépendent du DNS ou sont intégrées au protocole HTTP, il est plus difficile d'identifier avec précision le trafic réseau au niveau des applications.

Le moteur NBAR (Network Based Application Recognition) de Cisco permet de classer plus de 1 500 applications, ce qui permet aux ingénieurs réseau de classer et de manipuler les flux de trafic avec plus de granularité. Catalyst SD-WAN Manager de Cisco offre la possibilité de se connecter à un référentiel d'applications Cisco où les signatures des applications peuvent être mises à jour rapidement ; ce qui est important lorsque les fournisseurs de cloud changent d'emplacement d'hébergement ou de modèles de trafic.

Le catalogue d'applications permet de créer des applications personnalisées en fonction de la correspondance du nom du serveur, de l'adresse IP, des ports ou du protocole. L'application est ensuite définie en fonction d'une famille d'applications, d'un groupe d'applications, d'une classe de trafic et d'une pertinence commerciale spécifiques.



Catalogue d'applications

Les applications peuvent être déplacées vers la pertinence commerciale et/ou la classification de trafic appropriées. Lors de l'enregistrement des modifications, les définitions sont mises à jour dans la base de données.

Remarque : Les classifications d'applications sont globales et une modification du catalogue d'applications a un impact sur toutes les classifications de périphériques.

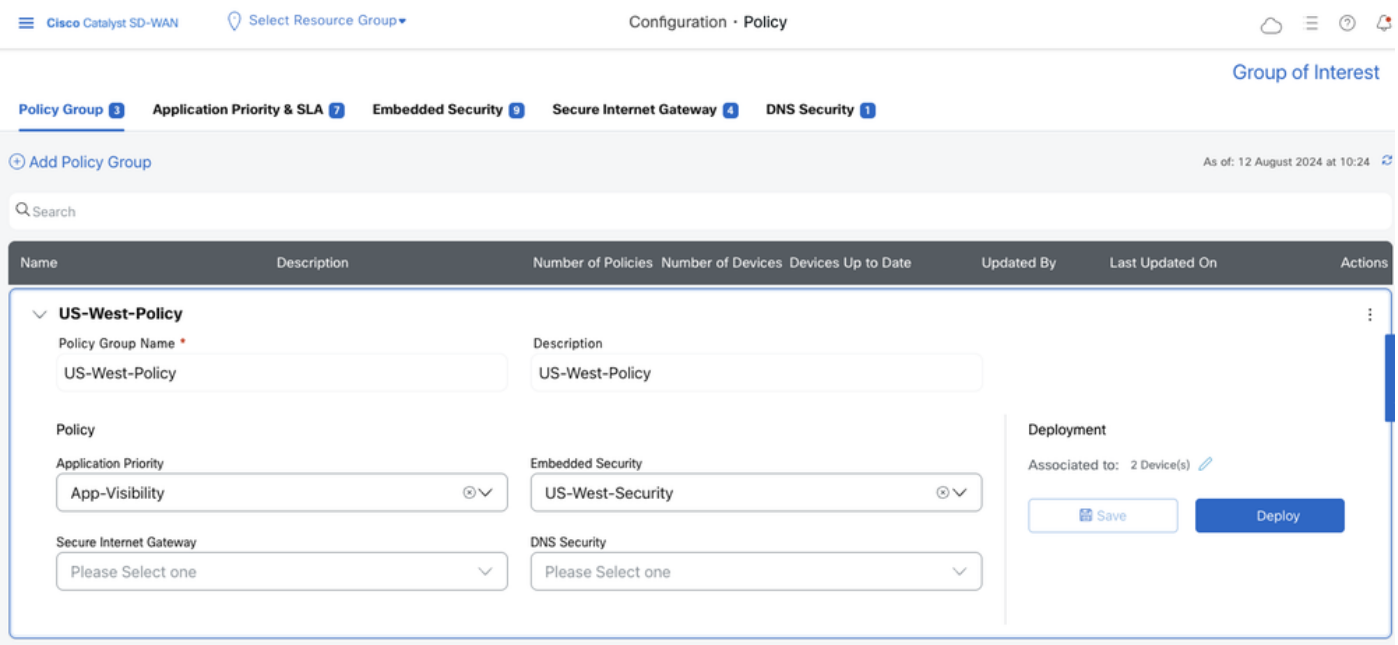
Groupes de stratégies

Tout comme les groupes de configuration, un groupe de stratégies est un regroupement de stratégies déployées sur des périphériques associés au groupe de stratégies

https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/Policy-Groups/policy-groups/m-policy-groups.html.

Le groupe de politiques aborde la création et le déploiement de politiques en fonction de l'intention. Une interface utilisateur et un workflow simplifiés facilitent la création d'une stratégie, le regroupement des stratégies et le déploiement sur les périphériques.

Prérequis : l'association et le déploiement du groupe de configuration sur un périphérique sont des conditions préalables au déploiement du groupe de stratégies sur ce périphérique.



Groupes de stratégies

Priorité des applications et SLA

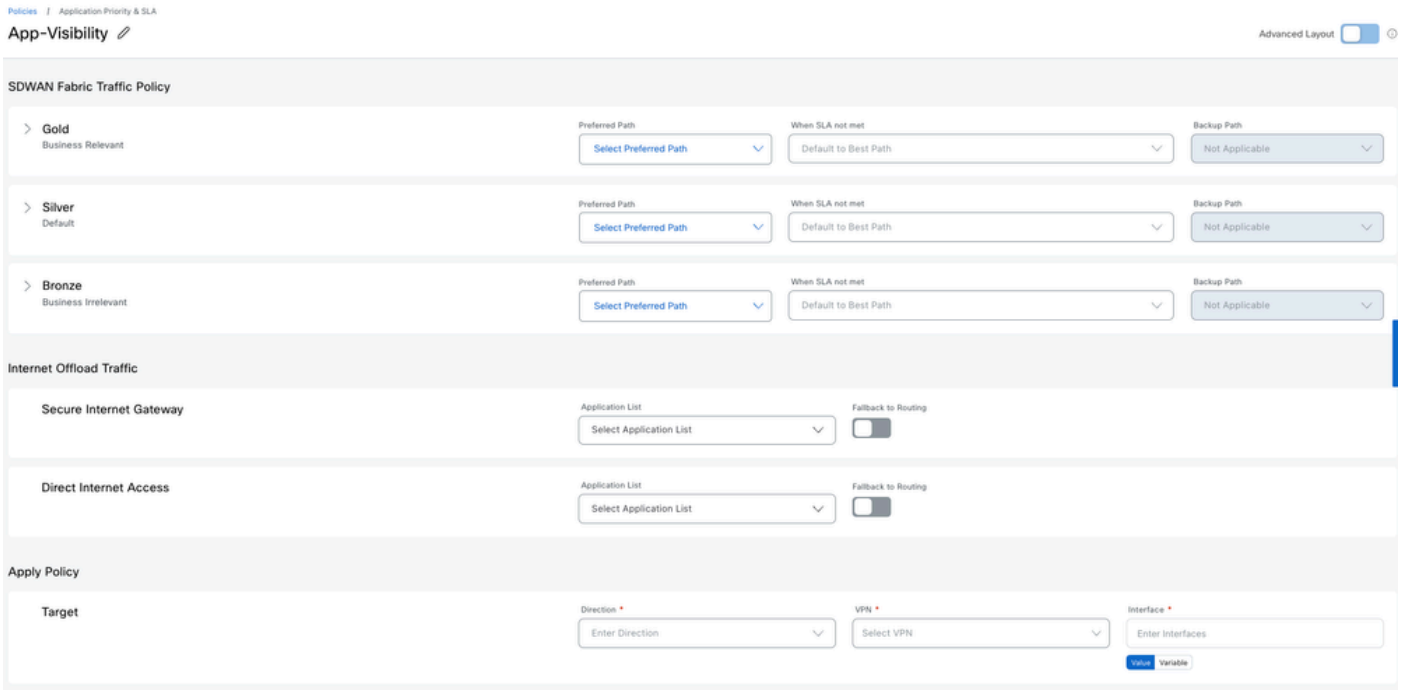
Dans le cadre de cette stratégie, vous pouvez spécifier :

- Routage sensible aux applications et politique SLA
- stratégie QoS
- Politique de données de trafic
- politique DIA
- politique de voies navigables intérieures

Deux modes sont proposés.

Mode simple

Il s'agit du mode par défaut.



Mode simple

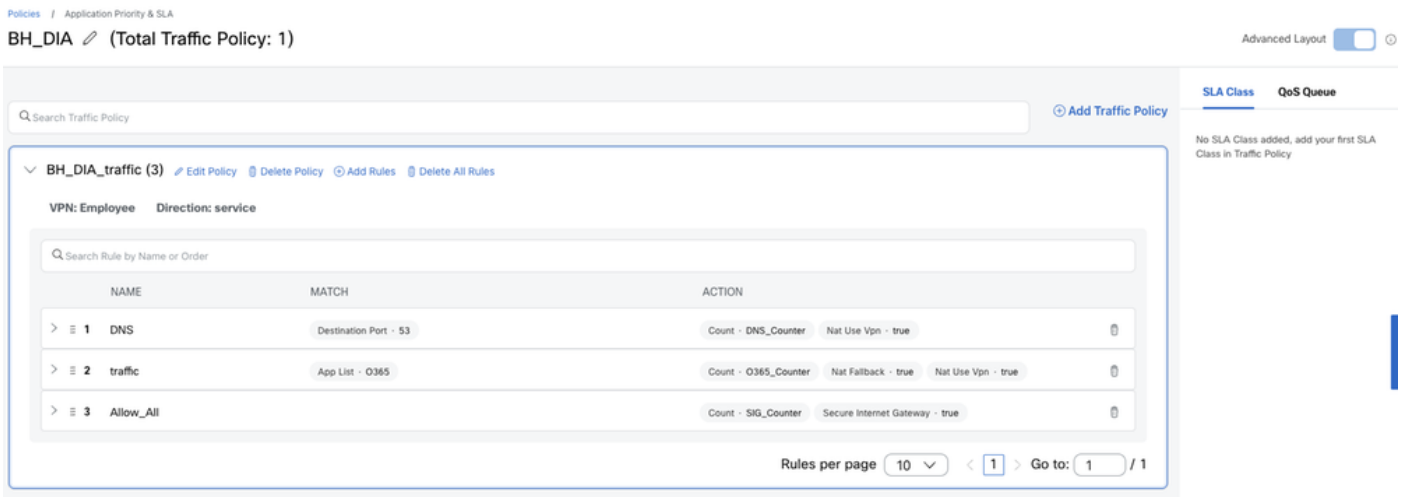
Il s'agit d'un moyen simple et rapide de définir la priorité d'application et le SLA de votre réseau.

Remarque : 1. L'action de stratégie par défaut est DROP.

2. Les critères de correspondance ne peuvent être que des applications. Si vous avez besoin de préfixes, utilisez le mode avancé

Mode avancé

Il s'agit d'un mode complet et flexible.



Mode avancé

Remarque :

1. L'action de stratégie par défaut est DROP.

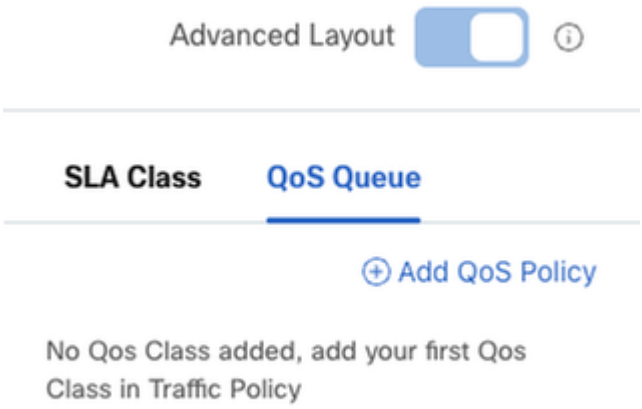
2. La liste d’applications et la classe de trafic sont essentiellement une liste d’applications.

L'une ou l'autre peut être utilisée pour faire correspondre une liste d'applications. Le mappage des applications à la classe de trafic peut être effectué dans le catalogue d'applications.

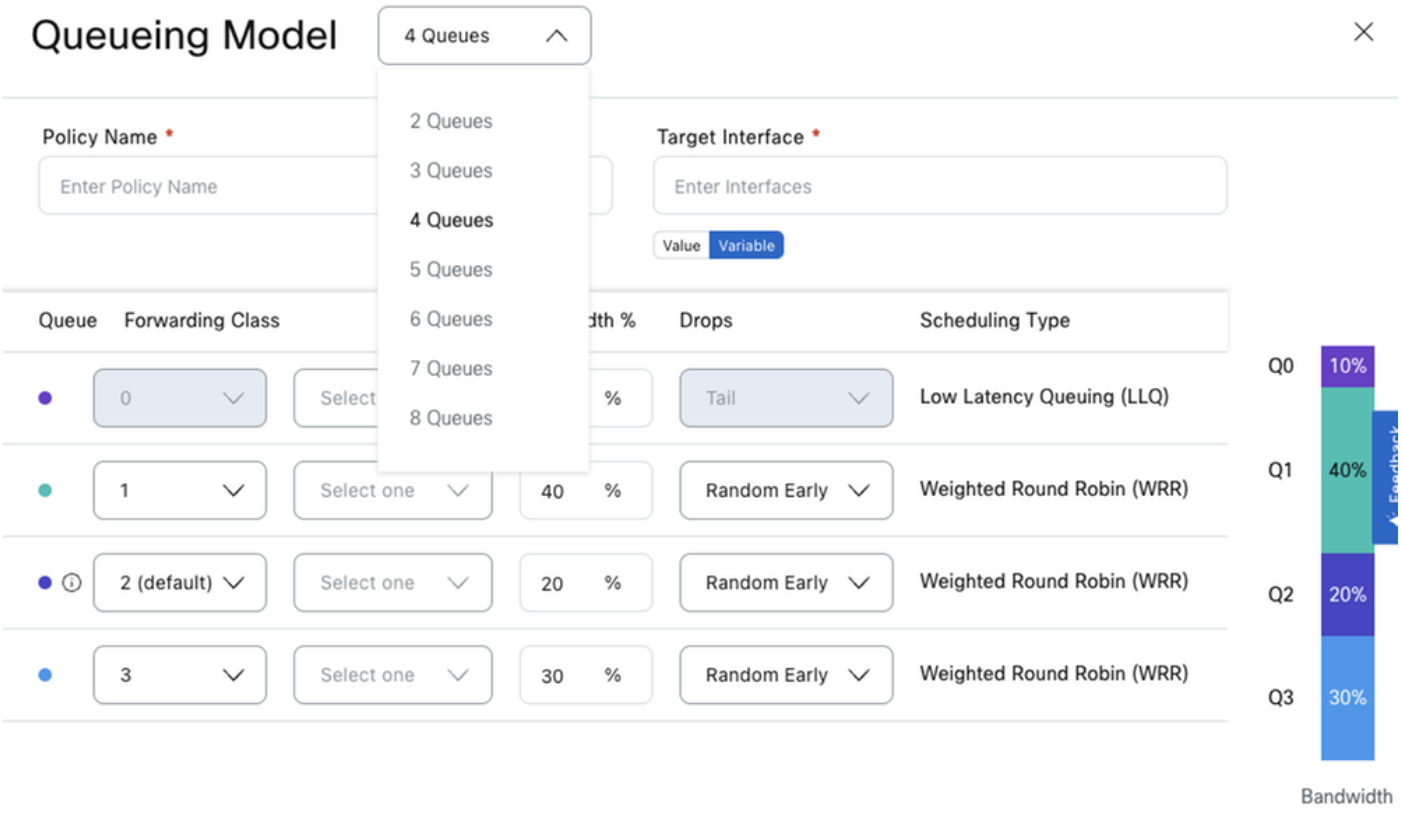
Le mode simple génère des règles à l'aide de l'une ou des deux options, tandis que le mode avancé fournit uniquement la liste des applications.

Qualité de service

Dans l'option QoS Queue, vous pouvez ajouter une stratégie QoS :



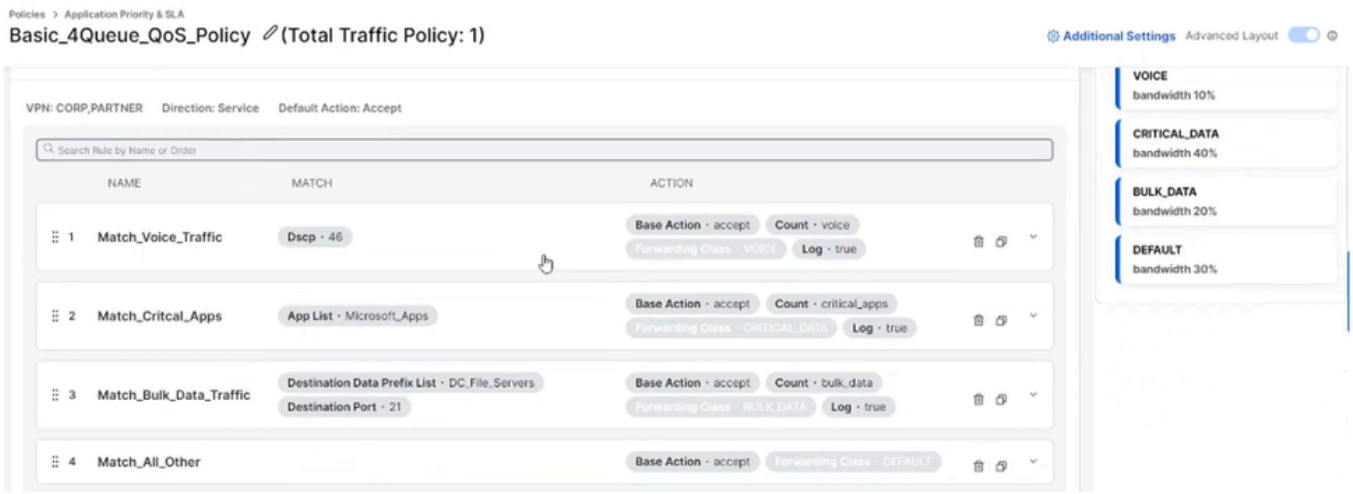
Ajouter une stratégie QoS



Modèles de file

Vous pouvez ensuite définir la stratégie de données de trafic (Ajouter une stratégie de trafic).

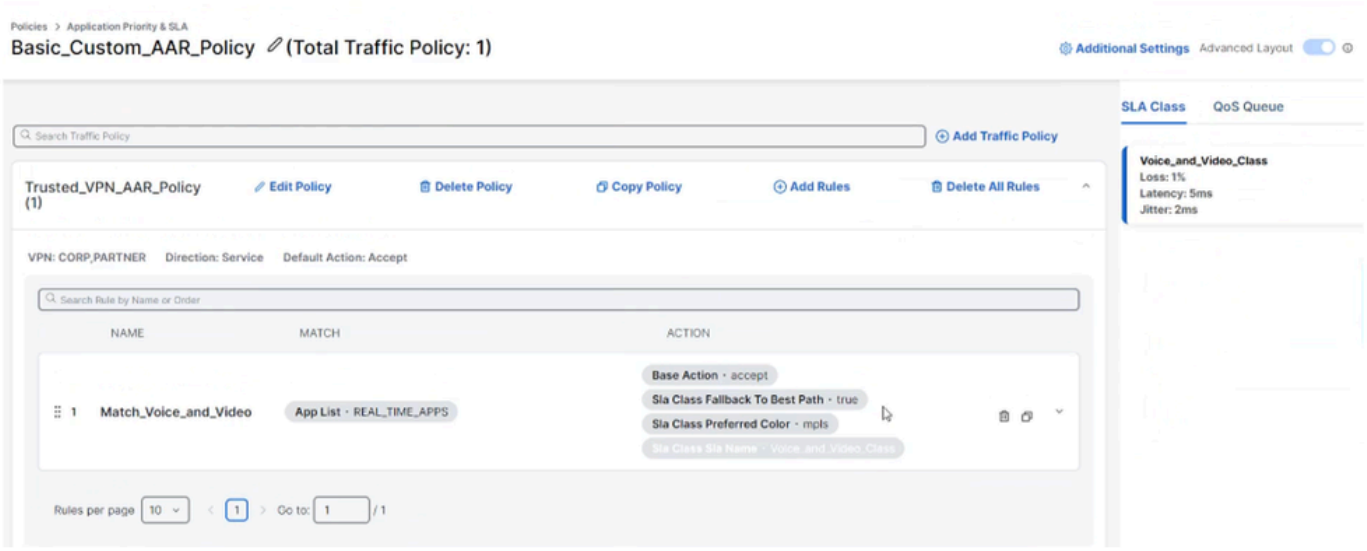
Ajoutez des règles correspondant au trafic souhaité et redirigez-les vers les classes de transfert appropriées.



Politique QoS 2

Routage sensible aux applications

Vous pouvez définir des classes SLA et les utiliser dans une politique de trafic afin de réaliser l'intention d'une politique AAR.



Politique AAR

Visibilité des applications/flux :

Afin d'activer la visibilité des applications et des flux, utilisez le profil/colis CLI dans le groupe de configuration.

(Dans les versions 20.13 et ultérieures, il est disponible sous Paramètres avancés dans Groupe de stratégies).

Cependant, dans la version 20.12, si une stratégie AAR est configurée, alors la visibilité sur les applications/flux est activée. Il n'est pas nécessaire de configurer ce paramètre à l'aide du profil/colis CLI.

Comment ajouter la configuration « ip nbar protocol-discovery » aux interfaces VPN de service ?

À partir de 20h15 :

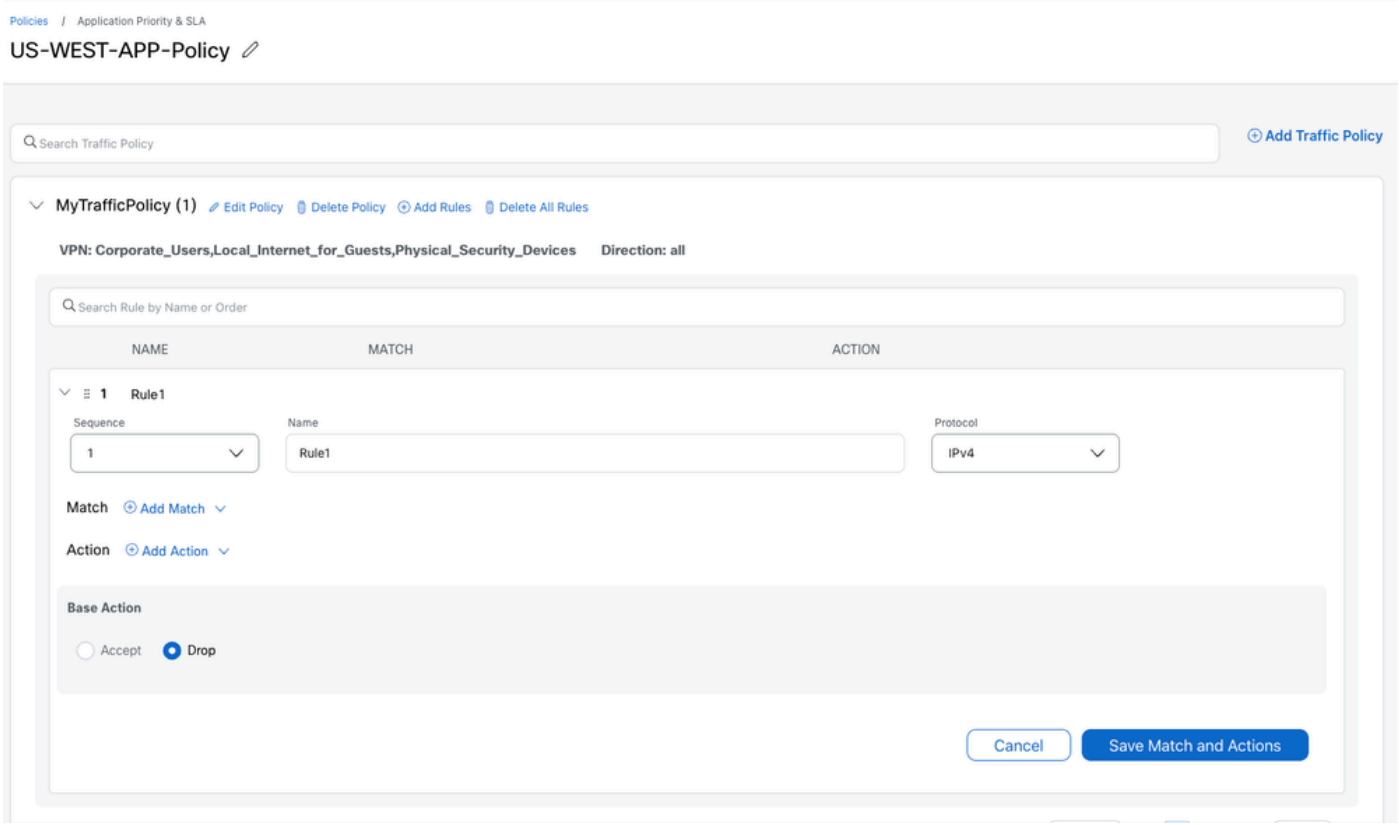
Lorsque la visibilité sur les applications est activée (à partir de Priorité d'application et Stratégie SLA -> Paramètres supplémentaires), la configuration « ip nbar protocol-discovery » est poussée vers toutes les interfaces VPN de service. Aucune étape supplémentaire n'est requise.

Jusqu'à 20 h 14 :

L'ajout d'un paquet de surveillance des performances de l'application dans le profil système active la configuration « ip nbar protocol-discovery » sur toutes les interfaces VPN de service. Si vous souhaitez le faire pour une interface VPN de service spécifique uniquement, cela peut être fait via un profil CLI.

Politique Du Trafic

La politique de trafic peut également être utilisée pour créer une politique DIA, une redirection SIG, etc. Ajoutez des règles si nécessaire.



Politique Du Trafic

Remarque : Si une priorité d'application et une stratégie SLA sont créées en mode simple, puis basculées en mode avancé, certaines options de correspondance ne sont pas disponibles. Exemple : Le préfixe de données de destination est grisé.
Afin de rendre ces options disponibles, changez le protocole de BOTH à IPv4 ou IPv6 selon les besoins.

Sécurité intégrée

Définit la stratégie de sécurité pour le pare-feu de nouvelle génération intégré, IPS, les programmes malveillants et le filtrage du contenu.

Pour plus d'informations, reportez-vous à :
Guide de configuration de la sécurité SD-WAN de Catalyst

Passerelle Internet sécurisée/Périphérie de service sécurisé

Définit les paramètres requis pour établir des tunnels vers le contenu basé sur le cloud et les entités de sécurité, telles que Cisco Secure Access.

Remarque : Avec l'approche de configuration héritée, ce modèle était disponible en tant que modèle de fonctionnalité.

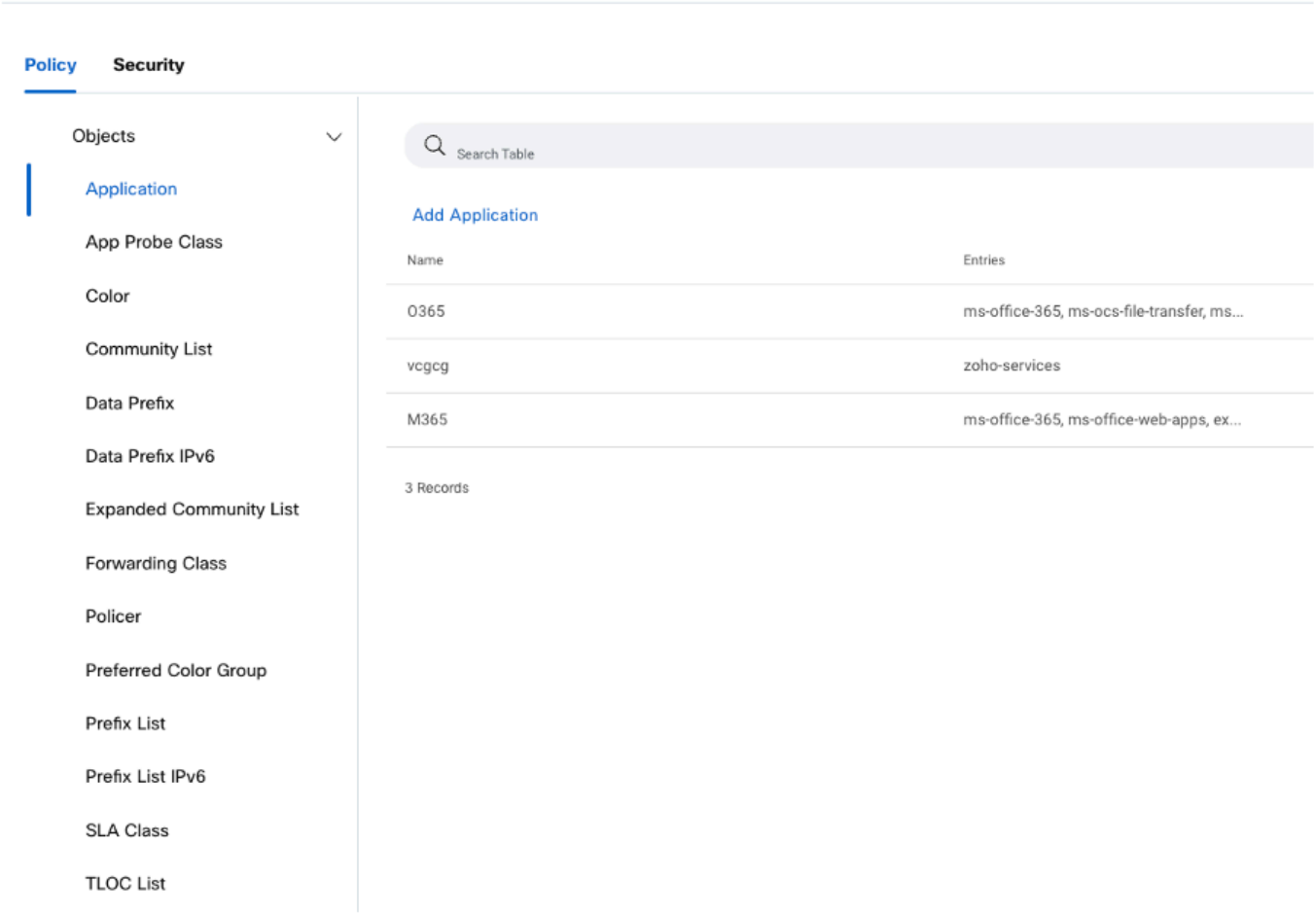
Sécurité DNS

Définissez les paramètres afin de permettre l'utilisation de services de sécurité DNS basés sur le cloud pour le filtrage de contenu.

Groupes d'intérêt

Définissez les listes d'objets à utiliser dans vos stratégies. Exemple : Listes d'applications, liste de préfixes, etc.

En outre, pour les stratégies de sécurité, définissez vos profils comme les profils d'inspection avancés, la stratégie de déchiffrement SSL, etc.



Groupes de politiques - Groupes d'intérêt

Associer et déployer

Comme pour les groupes de configuration, associez les périphériques au groupe de stratégies et déployez-les.

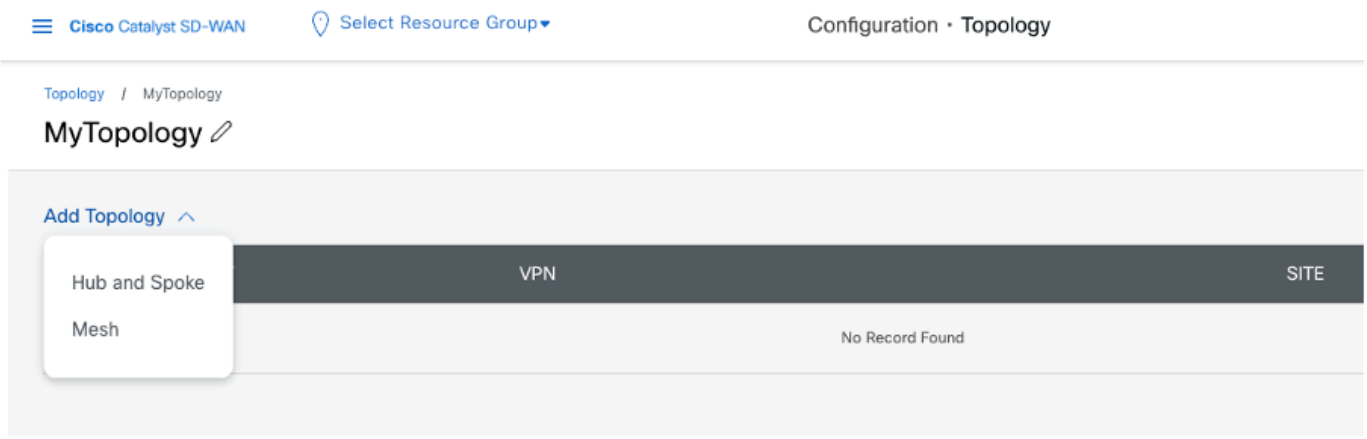
Stratégies localisées

Les stratégies localisées telles que ACL, Route, Device access policy, etc., sont définies dans les groupes de configuration.

Topologie

Définissez votre topologie de réseau.

Commencez par un maillage global ou Hub-n-Spoke et personnalisez-le si nécessaire.



Menu Topologie

Topologie et VPN

Gardez à l'esprit ces modifications de conception lors de la création de la topologie et de la spécification des VPN.

La nouvelle conception permet le mappage dynamique du nom VPN vers l'ID VPN, au lieu du mappage 1:1.

Mappage d'un nom VPN sur plusieurs ID VPN

Illustration :
Supposons qu'il existe un VPN portant le nom Corporate dans deux groupes de configuration différents.

L'un a l'ID VPN 10 et l'autre a l'ID VPN 20.

La liste VPN du workflow de topologie affiche une seule instance de VPN d'entreprise.

Une fois que vous avez choisi Corporate VPN, le SD-WAN Manager détermine les ID VPN en fonction de la topologie.
Supposons qu'il existe deux périphériques sur deux sites :

1. Périphérique1 sur le site 100 avec Corporate comme VPN 10
2. Périphérique2 sur le site 200 avec Corporate comme VPN 20

Si le site 100 et le site 200 font tous deux partie de la topologie, SD-WAN Manager crée une liste VPN qui a les deux ID VPN (10 et 20).
Si seul le site 100 fait partie de la topologie, SD-WAN Manager crée une liste VPN qui a l'ID VPN 10 uniquement.
Si seul le site 200 fait partie de la topologie, SD-WAN Manager crée une liste VPN qui a l'ID VPN 20 uniquement.

Mappage de plusieurs noms VPN sur le même ID VPN

Vous pouvez configurer plusieurs stratégies de topologie avec le même nom VPN qui sont mappées à différents ID VPN sur différents sites.

Le gestionnaire SD-WAN détermine le mappage réel en fonction de la topologie associée à chaque site.

Illustration :

Deux utilisateurs peuvent créer deux groupes de configuration différents.

L'un spécifie l'ID VPN 100 comme Finance VPN et l'autre le spécifie comme Engineering VPN.

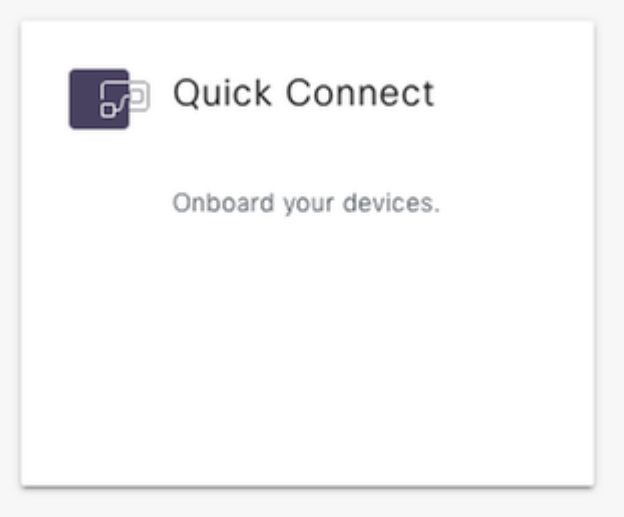
Ils peuvent ensuite créer une topologie à l'aide de leurs noms VPN respectifs.

Intégration

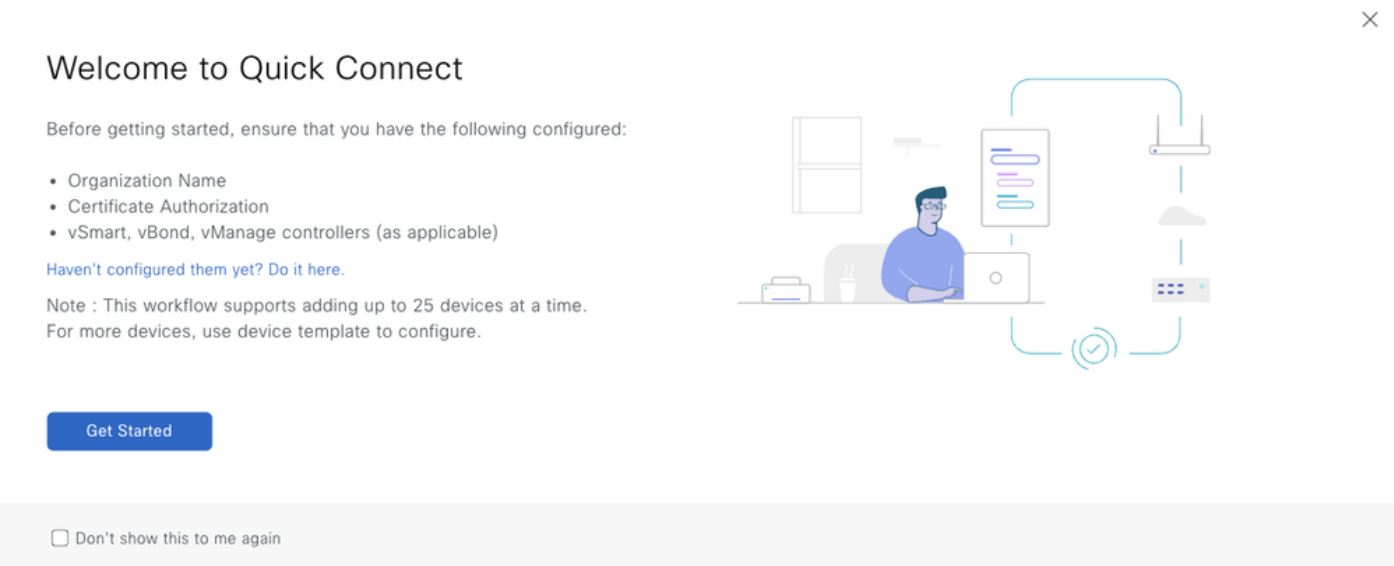
Pour l'intégration de vos routeurs physiques, utilisez le workflow de connexion rapide.

À l'aide de ce workflow, prédéfinissez le nom d'hôte, l'adresse IP du système et le nom/l'ID du site pour les périphériques à intégrer. Le gestionnaire les génère automatiquement, mais vous pouvez les modifier si vous le souhaitez. Vous pouvez également marquer les périphériques qui peuvent ensuite être utilisés pour associer automatiquement les périphériques aux groupes de configuration.

Pendant le processus d'intégration ZTP PnP, les périphériques établissent les connexions du tunnel du plan de contrôle vers le gestionnaire SD-WAN. SD-WAN Manager transmet désormais la configuration de fabric prédéfinie aux périphériques et ces derniers se connectent au fabric SD-WAN.



Workflow de connexion rapide



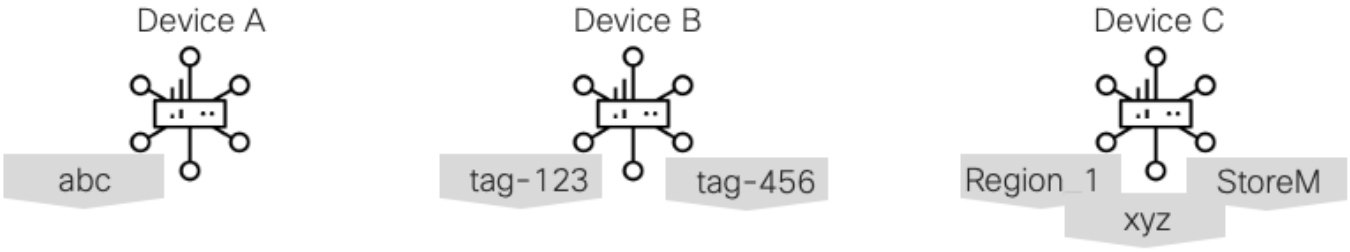
Description du workflow de connexion rapide

Marquage

Les périphériques peuvent être associés à des balises définies par l'utilisateur.

Les balises peuvent être utilisées pour regrouper, décrire, rechercher ou gérer des périphériques.

Les balises permettent de regrouper des périphériques qui peuvent ensuite être utilisés dans d'autres fonctionnalités.



Exemples de balisage

Exemple : Association de groupes de configuration à des périphériques.

Les règles de groupe de configuration peuvent être définies pour permettre aux périphériques avec des balises spécifiques d'être automatiquement associés à ce groupe de configuration.

Ajouter une balise

Dans Configuration > Devices, les balises peuvent être créées/ajoutées à/supprimées des périphériques.

Règles de balise dans le groupe de configuration

Dans la page Groupe de configuration > Périphériques associés, les règles de balise peuvent être ajoutées/modifiées.

Illustration

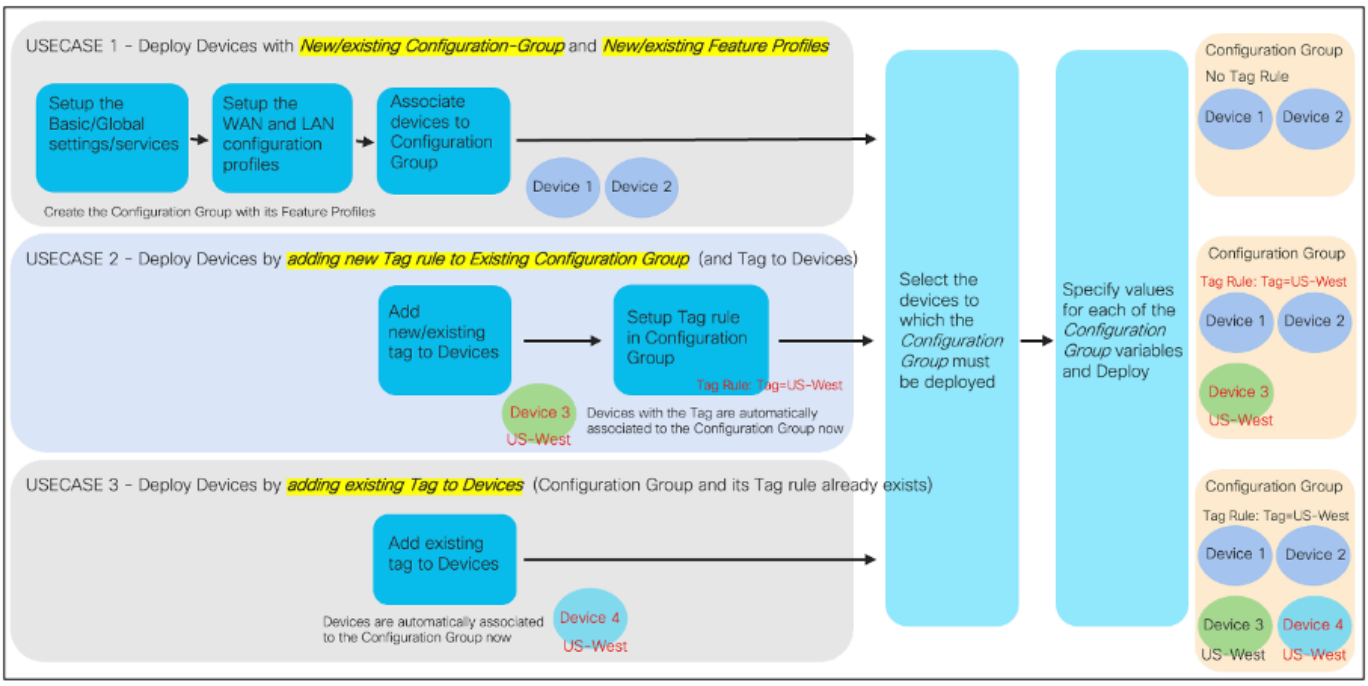


Illustration de balisage

Déploiements existants

Dans le réseau SD-WAN, les périphériques qui utilisent la configuration et les stratégies héritées peuvent coexister avec les périphériques utilisant la configuration et les stratégies simplifiées.

Cette section offre quelques recommandations aux utilisateurs qui souhaitent tirer parti de la configuration et des stratégies simplifiées. Elle propose également quelques recommandations.

La première étape consiste à migrer les périphériques des modèles de périphériques vers les groupes de configuration. Une fois cette opération effectuée, des groupes de stratégies et/ou une topologie peuvent être déployés.

Groupes de configuration

Les modèles de périphériques et les groupes de configuration fournissent la configuration des périphériques de périphérie. Il est donc facile pour la coexistence de se produire. Les étapes de migration d'un modèle de périphérique vers un groupe de configuration sont les suivantes :

Étape 1.	Extrayez une copie des valeurs de périphérique à partir des modèles de périphérique. Pour ce faire, cliquez sur le bouton à Modèles, puis sur les points de suspension (...) à droite du groupe de périphériques et choisissez Export CSV.
Étape 2.	Créez un groupe de configuration (manuellement ou avec l'outil de conversion).
Étape 3.	Détachez le modèle de périphérique du périphérique. À ce stade, le périphérique conserve la configuration au point de fixation ; mais ne reçoit pas les modifications futures apportées au modèle de périphérique (ni aux modèles de fonctionnalité de composant).
Étape 4.	Associez le ou les périphériques au nouveau groupe de configuration.
Étape 5.	Déployez les périphériques associés au groupe de configuration. Pour faciliter ce processus, ouvrez le fichier CSV exporté et modifiez les en-têtes de colonne CSV pour qu'ils correspondent aux nouvelles variables du groupe de configuration.
Étape 6.	Une fois l'écran de saisie des variables du périphérique affiché, vous pouvez prévisualiser la configuration du périphérique. Cela vous donne un aperçu des parties du groupe de configuration qui ne correspondent pas à l'instance précédente ; ou les variables qui ont changé depuis le modèle de périphérique.

Le maintien d'un système d'attribution de noms cohérent pour les variables simplifie les paramètres spécifiques aux périphériques. Si toutes les valeurs de périphérique se trouvent dans un seul fichier CSV, vous ne devez renommer les en-têtes de colonne qu'une seule fois.



Remarque : Il existe un script python qui fonctionne avec les fichiers CSV pour les modèles de périphériques ou les groupes de configuration afin de consolider et d'alphabétiser les en-têtes de colonne. Le script est disponible ici :

https://github.com/BradEdgeworth/CSVMerger.

Groupes de stratégies

Les périphériques configurés via des groupes de configuration peuvent utiliser une stratégie

centralisée ou migrer vers un groupe de stratégies. mais pas les deux en même temps pour la même application. En substance, l'objectif est de conserver la même politique sous-jacente pour les périphériques de périphérie. Les groupes de stratégies combinent les stratégies AAR et de données d'origine en un seul composant Application Priority et SLA PG. En substance, la manière dont la configuration des politiques est créée est modifiée (mais pas envoyée au gestionnaire SD-WAN).

Il est important de noter que vous ne pouvez pas avoir de politique de données ou de politique AAR pour référencer une liste de sites avec un site qui a la priorité d'application et le composant SLA car ils configurent tous les deux le même paramètre.

Il est possible d'avoir une stratégie centralisée avec seulement une référence de stratégie de contrôle (un site qui utilise un groupe de stratégies avec une priorité d'application et un SLA) pendant qu'ils configurent différents composants d'une stratégie centralisée.

Les étapes de migration d'un périphérique d'une stratégie centralisée vers un groupe de stratégies sont les suivantes :

Étape 1.	Créez les composants de groupe de stratégies nécessaires (Priorité d'application et SLA, Sécurité intégrée, Passerelle Internet sécurisée/Périphérie de service sécurisée, Sécurité DNS.
Étape 2.	Créez le groupe de stratégies et associez les composants nécessaires.
Étape 3.	Dissociez l'ID de site de toutes les listes de sites qui sont des références dans AAR ou des politiques de données. À ce moment, le gestionnaire SD-WAN envoie une configuration mise à jour aux contrôleurs qui suppriment ensuite toutes les instructions de politique de données actives du ou des périphériques de périphérie. Notez que cela peut provoquer des flux de trafic non souhaités à ce stade.
Étape 4.	Associez le ou les périphériques au groupe de stratégies et enregistrez le groupe de stratégies.
Étape 5.	Déployez le groupe de stratégies sur les périphériques sélectionnés. À ce stade, le gestionnaire SD-WAN envoie les configurations mises à jour aux périphériques Edge (pour QoS/SIG) et aux contrôleurs ; afin que les contrôleurs puissent envoyer des politiques de données mises à jour aux périphériques de périphérie.

Remarque : Bien que les groupes de stratégies puissent coexister avec une stratégie centralisée, il est recommandé de conserver cette dernière (pour les stratégies AAR et de données) lors de la conversion des périphériques de périphérie en groupes de configuration. Ensuite, commencez la migration de la stratégie centralisée vers les groupes de stratégies pour une fonctionnalité au sein de la priorité d'application et du composant SLA.

Cela est fait pour la simplicité et pour réduire la confusion parmi le personnel opérationnel.

Remarque : Le moteur de groupe de stratégies stocke les éléments dans un format différent. Par conséquent, une liste de préfixes utilisée dans une stratégie centralisée doit être recréée dans le groupe de stratégies. Cela peut se produire pour d'autres choses comme les listes de sites, etc.

Topologie

Les périphériques configurés via des groupes de configuration peuvent utiliser une stratégie centralisée ou migrer vers une topologie. En substance, l'objectif est de conserver la même politique de contrôle sous-jacente pour les contrôleurs SD-WAN. La topologie est la dernière itération des politiques de contrôle.

Il est important de noter qu'une stratégie de contrôle ne peut pas faire référence à une liste de sites avec un site auquel est associée une topologie, car les deux sites configurent le même paramètre.

Il est possible d'avoir une politique centralisée avec seulement une politique de données et/ou une politique AAR, et une politique de topologie pendant qu'ils configurent différents composants.

Étapes de migration d'un périphérique d'une stratégie centralisée vers un groupe de stratégies :

Étape 1.	Créez les composants de topologie nécessaires.
Étape 2.	Dissocier les côtés de l'ancienne liste de topologies dans la stratégie centralisée.

Étape 3.	Dissociez l'ID de site de toutes les listes de sites référencées dans AAR ou dans les politiques de données. À ce stade, le gestionnaire SD-WAN envoie une configuration mise à jour aux contrôleurs, qui suppriment ensuite toute configuration topologique active pour les sites en cours de migration. Notez que cela peut provoquer des flux de trafic non intentionnels à ce stade.
Étape 4.	Activez la topologie. À ce stade, le gestionnaire SD-WAN envoie des configurations mises à jour aux contrôleurs et modifie toutes les routes transmises aux périphériques de périphérie.



Remarque : Bien que la topologie puisse coexister avec une stratégie centralisée, il est recommandé de conserver cette dernière (pour la topologie et la manipulation de route) lors de la conversion des périphériques de périphérie en groupes de configuration. Ensuite, commencez la migration de la stratégie centralisée vers la topologie pour modifier les topologies et manipuler le routage.

Cela est fait par pure simplicité et afin de réduire la confusion parmi le personnel opérationnel.

Outil de conversion de configuration

Portée

L'outil de conversion de configuration convertit les modèles et les stratégies en groupes de configuration, groupes de stratégies et topologie. Il collecte la configuration des modèles et des stratégies à partir d'un gestionnaire SD-WAN cible, la convertit en leur groupe de configuration, groupe de stratégies et équivalents topologiques, et télécharge la nouvelle configuration vers le gestionnaire SD-WAN cible. L'outil prend actuellement en charge la conversion de 20.12 à 26.1.

Détails d'accès

L'outil de conversion de configuration est disponible sur le portail SD-WAN (anciennement appelé SSP).

Marche à suivre

L'outil de conversion dispose de deux options : 1) connexion directe à un gestionnaire SD-WAN et 2) exportation et importation sur le gestionnaire SD-WAN.

Flux de travail SD-WAN connecté au gestionnaire

Avec ce workflow, des modèles et des politiques seront collectés et une nouvelle configuration sera créée directement sur le gestionnaire SD-WAN. Ce flux de travail est destiné aux gestionnaires SD-WAN connectés au cloud.

Conditions préalables

- Avant d'utiliser l'outil, assurez-vous que votre gestionnaire SD-WAN exécute 20.12.x. Sinon, effectuez la mise à niveau vers la version 20.12 avant de continuer.
- Le gestionnaire SD-WAN cible doit être accessible via Internet.
- Si le SD-WAN Manager est sur moins de 20.15, il doit accepter le trafic entrant de 74.207.103.254.
- Si le gestionnaire SD-WAN est activé à partir de la version 20.15, l'autorisation d'accès aux services et services cloud doit être activée (via Paramètres).

Étape 1.	Connectez-vous au portail SD-WAN à l'aide de vos identifiants CCO. · Si vous êtes un administrateur de compte Smart, vous êtes normalement connecté au portail SD-WAN. Choisissez Configuration Conversion dans le menu de gauche afin d'entrer dans le workflow. · Si vous n'êtes pas un administrateur de compte Smart, vous obtenez une page 403 Interdit avec un lien vers l'outil intitulé « Conversion de la configuration » en bas de la page. Cliquez sur le lien afin d'accéder à l'outil.
Étape 2.	Détails: Sélectionnez votre superposition dans la liste. Cliquez sur le bouton Suivant. Si votre gestionnaire SD-WAN est activé sous une version antérieure à 20.15, vous serez invité à fournir des informations supplémentaires. Fournissez l'adresse IP ou l'URL de votre SD-WAN Manager avec les informations d'identification de l'utilisateur et cliquez sur Next. · L'utilisateur doit avoir un accès en lecture/écriture. · Le port (443 par défaut) est facultatif.

Étape 3.	Importer : Il existe deux options pour récupérer la configuration existante (modèles et stratégies) : 1. Cliquez sur le bouton Collecter afin de récupérer toutes les configurations (modèles de périphériques, modèles de fonctionnalités, stratégies et leurs constructions associées) à partir de SD-WAN Manager. Cette étape peut prendre quelques minutes pour les jeux de configuration volumineux. · Une fois collecté, vous pouvez télécharger un fichier JSON contenant tous les éléments de configuration. Ce fichier peut être utilisé au cours de cette étape ultérieurement au lieu d'être à nouveau collecté à partir du gestionnaire SD-WAN. 2. Téléchargez un fichier JSON contenant des modèles et des stratégies précédemment produits à partir de cette étape.
Étape 4.	Sélectionnez : Sélectionnez les modèles de périphériques que vous souhaitez convertir. ·NOTE: Seuls les modèles de périphériques auxquels des périphériques sont connectés peuvent être convertis. Les stratégies activées ou associées à un modèle de périphérique sélectionné pour la conversion sont automatiquement converties. Cliquez sur Convert afin de convertir les éléments de configuration choisis.
Étape 5.	Convertir : Cette page affiche tous les éléments de configuration nouvellement convertis. Vérifiez les éléments créés et leur état. Si l'état d'un élément est Partiel, consultez l'icône d'information afin de comprendre pourquoi. Cliquez sur Rapport pour télécharger le rapport avec toutes les informations à référencer ultérieurement. Une fois prêt, cliquez sur Upload et cliquez sur Confirm afin de créer ces nouvelles configurations dans SD-WAN Manager.
Étape 6.	Résumé: À cette étape, les nouveaux éléments de configuration sont créés dans le gestionnaire SD-WAN. Au fur et à mesure de la création des configurations, vous pouvez voir la barre de progression. Une fois le téléchargement terminé, vous voyez un résumé des configurations

	téléchargées et de leur état. · En cas d'erreur ou d'erreur, les options Annuler le téléchargement (pendant la création) et Retour arrière (après la création) sont disponibles à cette étape. L'exécution d'une annulation du téléchargement ou de la restauration supprime tous les éléments de configuration créés dans le gestionnaire SD-WAN au cours de ce workflow/de cette session. Si vous quittez ce flux de travail, vous ne pouvez pas annuler ces modifications ultérieurement. Vous devez supprimer manuellement les éléments indésirables. · Les variables de périphérique CSV ont également été converties. Cliquez sur Variables Package, puis sur Télécharger le package de variables converties pour télécharger un fichier .zip avec les fichiers CSV pour votre nouvelle configuration. · Cliquez sur Rapport pour télécharger un rapport contenant toutes les informations de cette étape et y faire référence ultérieurement.

Flux De Travail À Air Interdit

Conditions préalables

- Avant d'utiliser l'outil, assurez-vous que votre gestionnaire SD-WAN exécute 20.12.x. Sinon, effectuez la mise à niveau vers la version 20.12 avant de continuer.
- Les gestionnaires SD-WAN doivent être sur au moins 20.15.5, 20.18.2, 26.1 ou 26.2.

Étape 1.	Dans SD-WAN Manager, accédez à la page Modèles (Configuration —> Modèles). Cliquez sur Configuration conversion et, dans la fenêtre contextuelle, cliquez sur le bouton Export file. Cela permet de télécharger une archive tar (tar.gz) contenant tous les modèles de périphériques, les politiques et toute autre configuration requise (par exemple, NHM).
Étape 2.	Connectez-vous au portail SD-WAN à l'aide de vos identifiants CCO. · Si vous êtes un administrateur de compte Smart, vous êtes normalement connecté au portail SD-WAN. Choisissez Configuration Conversion dans le menu de gauche afin d'entrer dans le workflow. · Si vous n'êtes pas un administrateur de compte Smart, vous obtenez une page 403 Interdit avec un lien vers l'outil intitulé « Conversion de la configuration » en bas de la page. Cliquez sur le lien afin d'accéder à l'outil.

Étape 3.	Téléverser: Téléchargez le fichier archive tar exporté à l'étape 1. Cliquez sur Next. ·NOTE: C'est le seul format de fichier acceptable ; une sauvegarde Saster ne fonctionnera pas.
Étape 4.	Sélectionnez : Sélectionnez les modèles de périphériques que vous souhaitez convertir. ·NOTE: Seuls les modèles de périphériques auxquels des périphériques sont connectés peuvent être convertis. Les stratégies activées ou associées à un modèle de périphérique sélectionné pour la conversion sont automatiquement converties. Cliquez sur Convert afin de convertir les éléments de configuration choisis.
Étape 5.	Convertir : Cette page affiche tous les éléments de configuration nouvellement convertis. Vérifiez les éléments créés et leur état. Si l'état d'un élément est Partiel, consultez l'icône d'information afin de comprendre pourquoi. Cliquez sur Rapport pour télécharger le rapport avec toutes les informations à référencer ultérieurement. Une fois prêt, cliquez sur Export afin de générer un fichier d'exportation avec les nouvelles configurations.
Étape 6.	Terminé : Les nouveaux éléments de configuration peuvent désormais être téléchargés. Cliquez sur Download Converted Configurations pour télécharger l'archive tar contenant la nouvelle configuration. Vous allez l'importer dans SD-WAN Manager à l'étape suivante. En outre, les variables de périphérique CSV ont également été converties. Cliquez sur Download the convert variables package pour télécharger un fichier .zip avec les fichiers CSV pour votre nouvelle configuration.
Étape 7.	De retour dans le gestionnaire SD-WAN, accédez à la page Groupes de configuration (Configuration —> Groupes de configuration). Cliquez sur Import et sélectionnez le fichier contenant la nouvelle configuration téléchargée à l'étape précédente. Toutes les nouvelles configurations seront ensuite importées dans le gestionnaire SD-WAN. ·NOTE: Vous pouvez également importer le fichier dans la page Groupes de stratégies (Configuration —> Groupes de stratégies).

Post-Conversion

Votre nouvelle configuration est maintenant prête à être utilisée. Analysez et validez-le avant de le déployer dans un environnement de production. Exécutez les étapes de la section Déploiements existants afin de migrer vos périphériques vers les groupes de configuration, les groupes de stratégies et la topologie nouvellement convertis.

Considérations

- Les conversions fournies par l'outil sont destinées à servir de guide. Analyser et valider les nouvelles configurations avant de les déployer dans un environnement de production.
- L'outil est conçu pour convertir toutes les configurations une seule fois. Il n'est pas conçu pour effectuer des conversions par lots.
- L'outil ne tient pas compte de la capacité indépendante des périphériques des groupes de configuration. Les utilisateurs peuvent analyser leurs modèles avant de choisir lesquels convertir ou analyser les groupes de configuration convertis et associer les périphériques en conséquence pour bénéficier de la fonctionnalité indépendante des périphériques.
- Les noms de variable et les valeurs globales de la configuration d'origine sont copiés dans la configuration nouvellement convertie. Les CSV pour les valeurs spécifiques aux périphériques sont convertis en CSV pour les nouveaux groupes de configuration et de stratégie.
- L'outil ne convertit pas la configuration CLI en configuration basée sur l'interface utilisateur. Les modèles de fonctionnalités CLI seront convertis en profil de fonctionnalités complémentaires CLI. La stratégie centralisée CLI n'est pas prise en charge.
- L'outil n'applique pas la configuration aux périphériques. Après avoir effectué les conversions, l'utilisateur est chargé de détacher les périphériques des modèles et de les associer aux nouveaux groupes de configuration.

Communiquer avec le service de soutien à la clientèle

Pour tout problème lié à l'outil de conversion de configuration, envoyez un e-mail à sdwan-conversiontool-support@cisco.com.

20.12 Considérations

No.	Description article
1.	La configuration DNS doit être poussée via le profil de module complémentaire CLI lors du déploiement du groupe de configuration sur une périphérie

	exécutant une version antérieure à 17.12.
2.	La création de la topologie nécessite la sélection de sites au lieu de choisir une zone définie dans NHM.
3.	Le workflow Créer un groupe de configuration ne crée pas de VPN512 et d'interface dans ce VPN, dans le profil WAN. Si vous en avez besoin, vous pouvez le créer manuellement en modifiant le groupe Configuration.
4.	La possibilité de copier/dupliquer la stratégie dans le groupe de stratégies n'est pas prise en charge. Un ensemble de scripts Python peut accomplir cette tâche et se trouve dans : https://github.com/dbrown92700/configGroups/.
5.	La configuration de l'optimisation de la QoE d'application (TCP Opt et DRE) et de la correction des pertes (FEC et Pkt Dup) continue d'utiliser des modèles/stratégies hérités. Configurable également via le profil CLI dans les groupes de configuration/stratégie (20.14 dans le paquet UI).
6.	Cloud OnRamp pour SaaS continue d'utiliser les modèles/politiques hérités.
7.	TrustSec/SGT pris en charge avec le profil CLI uniquement.
8.	Batterie UC Voice/DSP/SRST prise en charge avec profil CLI uniquement (à partir de la version 20.13 dans le paquet UI).

Informations connexes

- Cisco SD-WAN et canal YouTube pour la mise en réseau cloud
- Configuration simplifiée - Simplification de la configuration SD-WAN
- 1. Créer une configuration de site en quelques clics à l'aide du workflow
- 2. Catalogue de configuration - Catalogue des configurations validées et gérées par Cisco pour le WAN
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.