

# 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 système](#)

[Hiérarchie réseau](#)

[Constructions système](#)

### [Workflows](#)

#### [Groupes de configuration](#)

[Exemples de déploiement de groupes de configuration](#)

[Cas d'utilisation 1 : client du secteur public](#)

[Cas d'utilisation 2 : client de détail](#)

[Associer](#)

[Déploiement](#)

[Réutilisabilité](#)

#### [Catalogue d'applications](#)

#### [Groupes de stratégies](#)

[Priorité des applications et SLA](#)

[Mode simple](#)

[Mode avancé](#)

[Qualité de service](#)

[Routage sensible aux applications](#)

[Politique de 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](#)

[Portée](#)

[Détails d'accès](#)

[Marche à suivre](#)

[Prérequis](#)

[Workflow de l'outil de conversion](#)

[Post-Conversion](#)

[Considérations](#)

[20.12 Considérations](#)

[Informations connexes](#)

---

## Introduction

Ce document est 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.

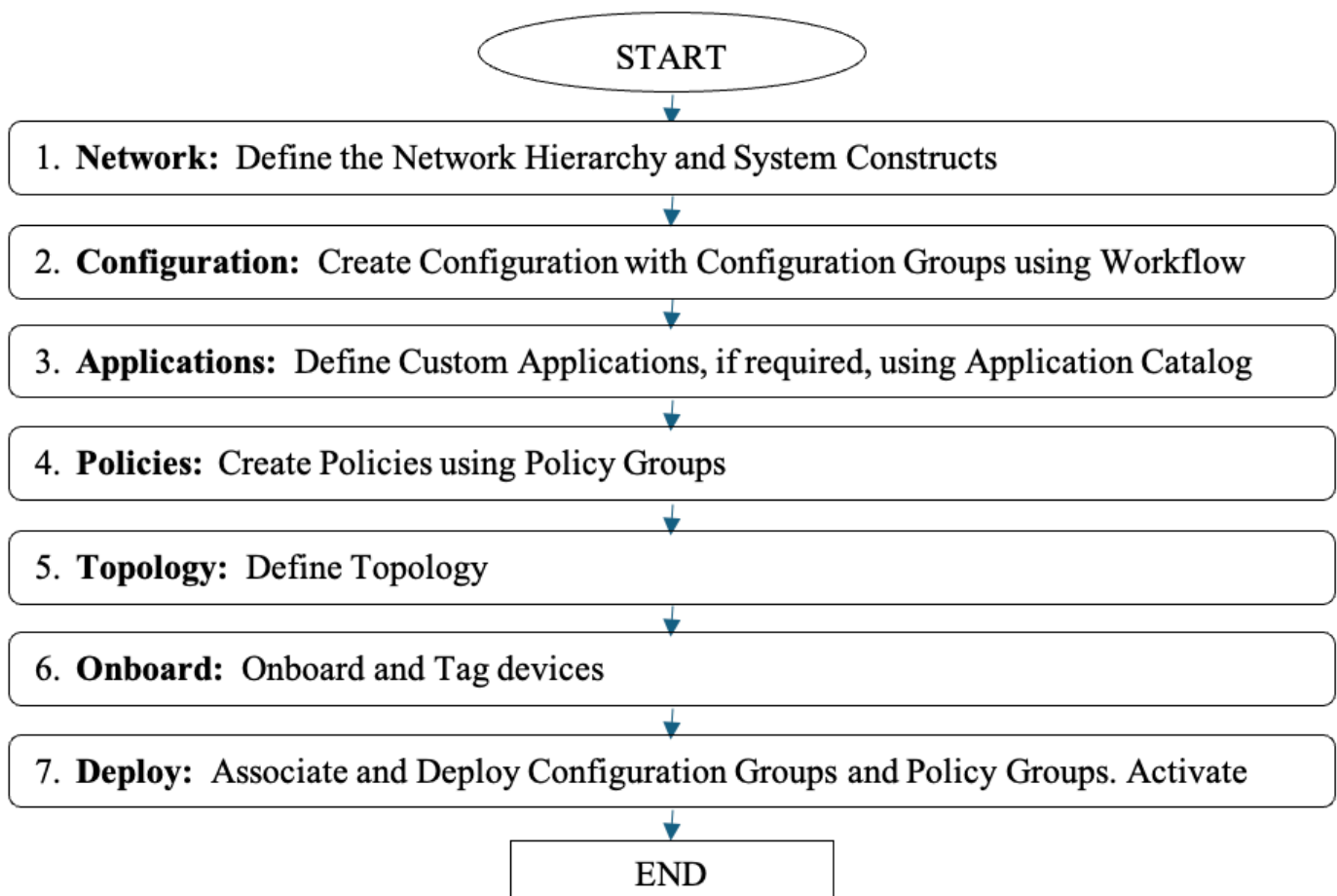
L'objectif principal de ce document est de servir de guide pour commencer à utiliser de nouvelles constructions pour la configuration, les politiques et l'intégration, avec la version 20.12. Le document ne couvre pas les explications des caractéristiques individuelles.

### Nouveaux déploiements

Pour utiliser correctement la nouvelle approche de configuration, vous devez exécuter les étapes suivantes :

1. Réseau : définition de la hiérarchie réseau et des 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. Stratégies : créer des stratégies à l'aide de groupes de stratégies
5. Topologie : définition de la topologie
6. Intégrée : périphériques intégrés et balises

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 de conversion](#) pour convertir les configurations/stratégies existantes en nouvelles configurations/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 UX a été introduit dans Catalyst SD-WAN Manager et d'autres produits Cisco, afin d'assurer la cohérence de l'expérience utilisateur et de fournir une apparence commune à tous les produits.
- Configuration : configuration et création et déploiement simplifiés de politiques grâce à des workflows intuitifs basés sur les intentions et à l'utilisation des valeurs par défaut intelligentes recommandées par Cisco.
- Surveillance : informations complètes sur les performances et l'état du réseau et des applications grâce à de nouveaux widgets et à 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 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 :



Search



Global (15 of 15 nodes)



AMER



BR1\_SanJose



BR2\_NewYork



BR6\_Dallas



APJC



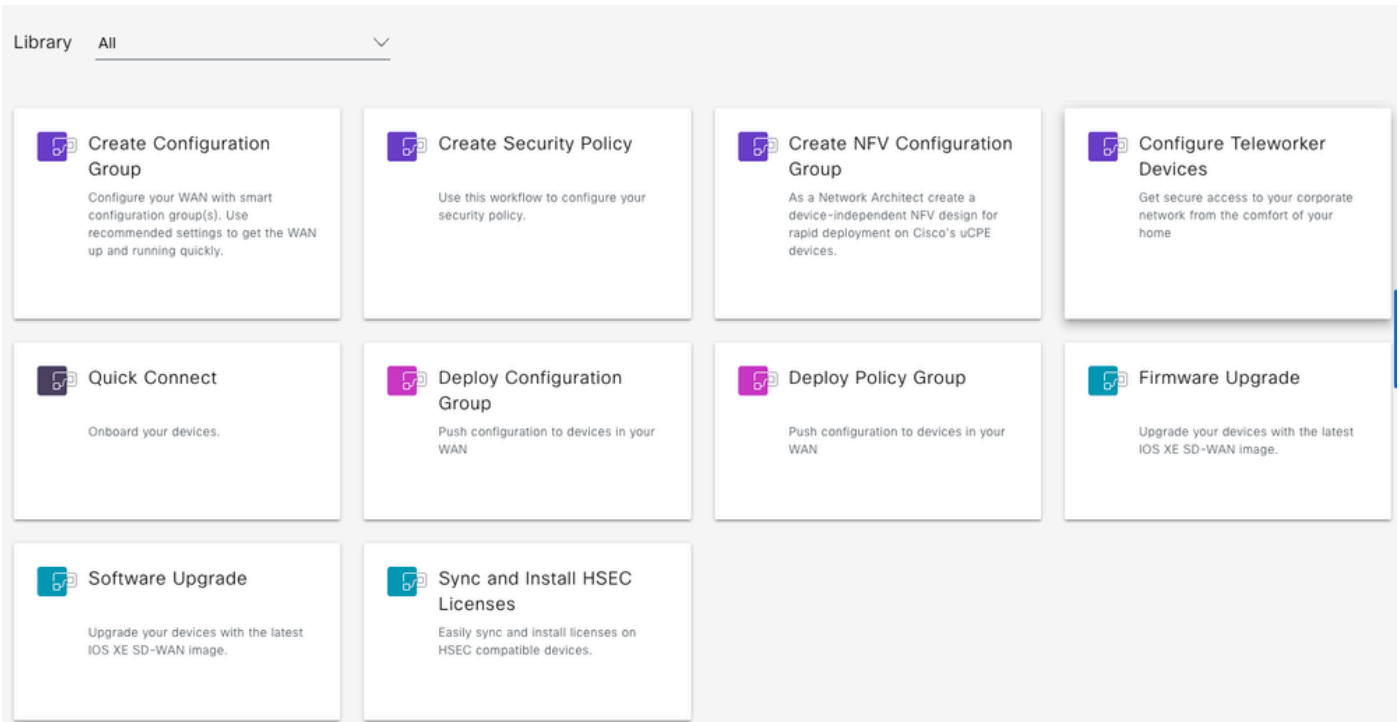
BR3\_Mumbai



BR4\_Singapore

- 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.

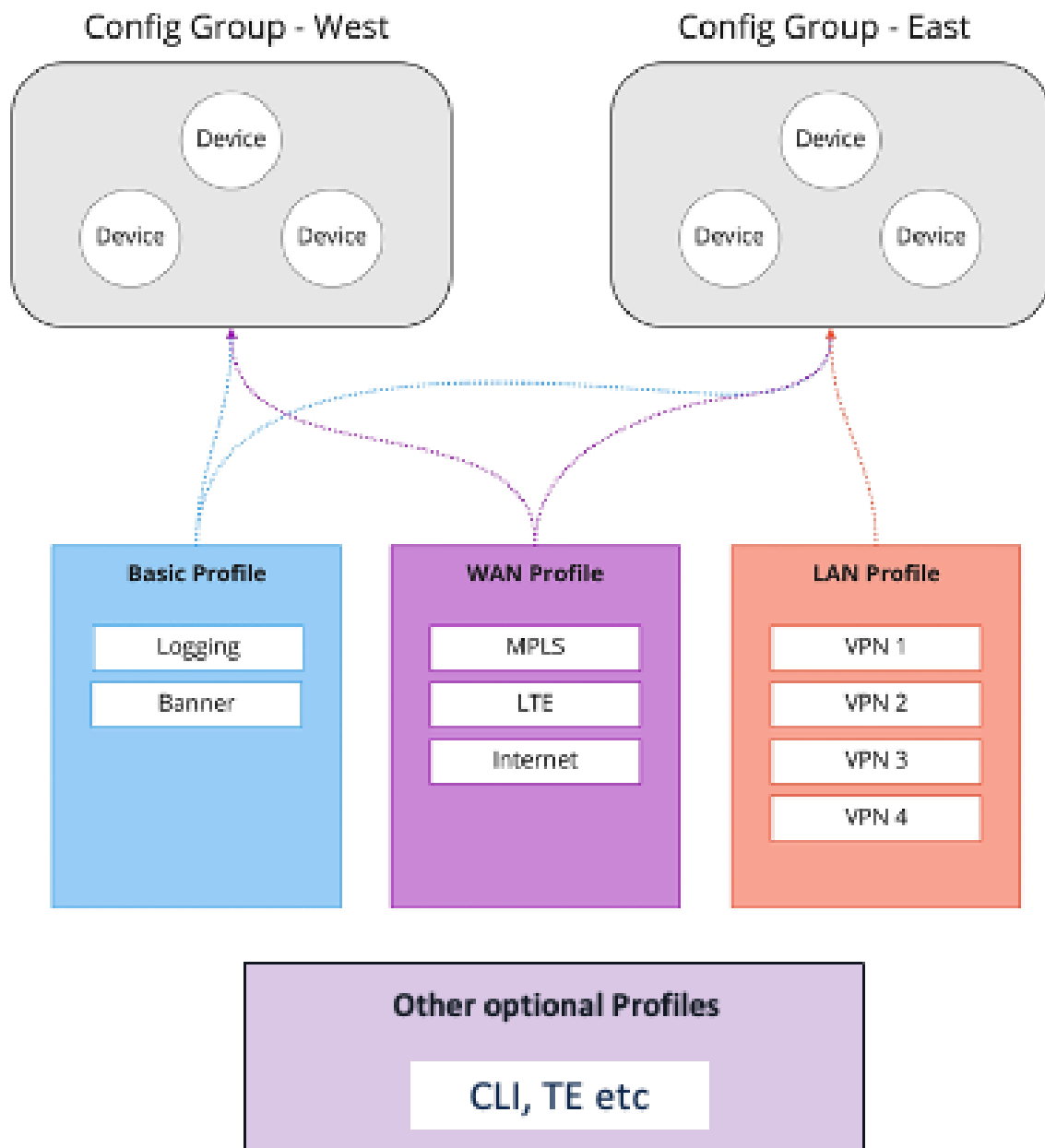


Bibliothèque de workflows

## Groupes de configuration

Configuration Groups est une nouvelle approche de la configuration du fabric basée sur les 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.

Par exemple, East/West, Americas/APJC/EMEAR, Retail Store/Distribution Center

### Profils de fonctionnalités

- « Compartiments » flexibles de configuration pouvant être partagés entre plusieurs groupes de configuration.
- Créer des profils de fonction en fonction des fonctions requises
- Rassemblez les profils pour finaliser la configuration des périphériques, comme les blocs de

construction

- Création, enregistrement et réutilisation

Par exemple, Basic Profile, WAN Profile, LAN Profile

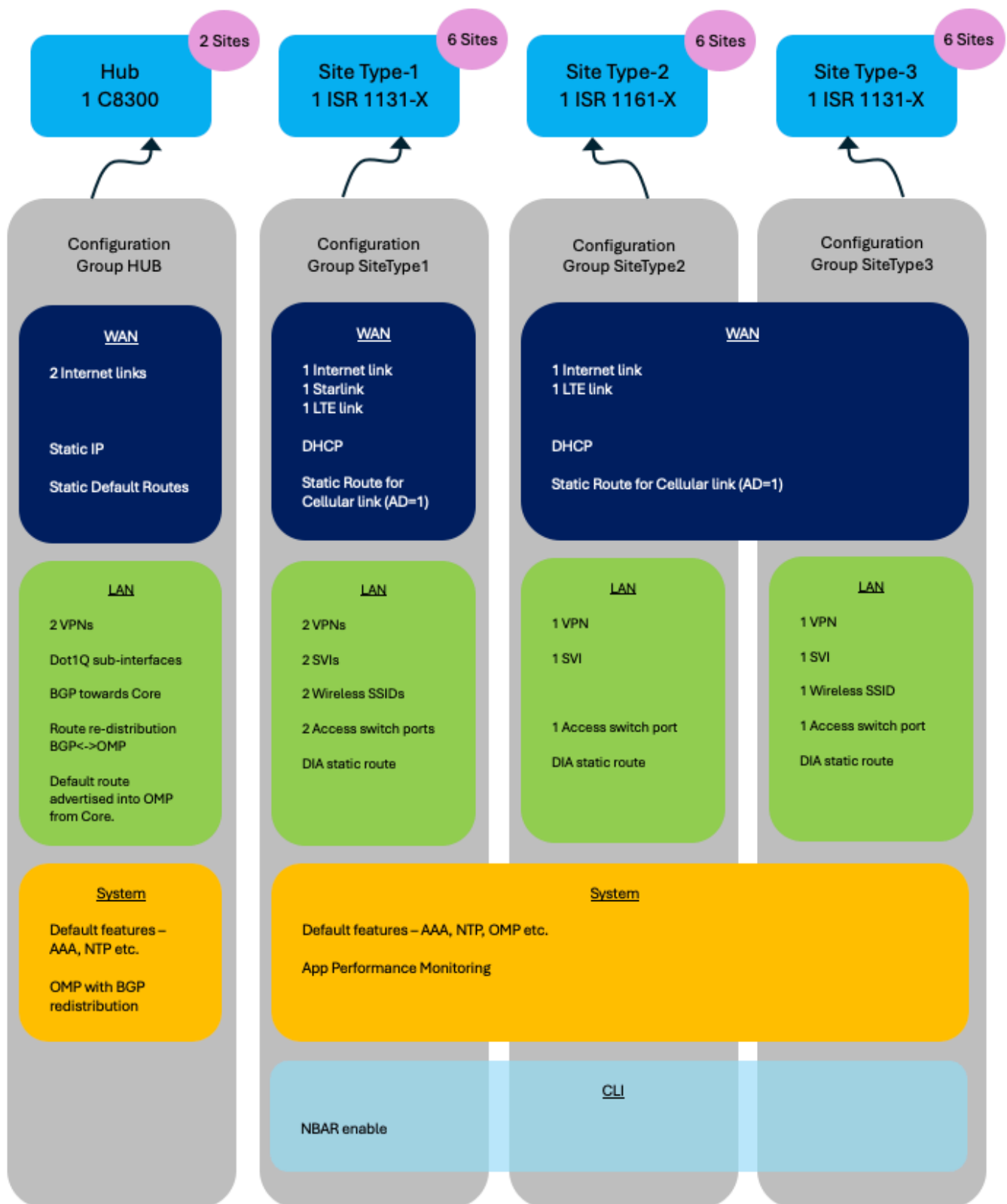
## Exemples de déploiement de groupes de configuration

Remarque :

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

Exemple d'utilisation 1 : client du secteur public





Exemple d'utilisation 1 - Groupes de configuration

HUB du groupe de configuration

Exécutez le workflow Créer un groupe de configuration.



## Create Configuration Group

Configure your WAN with smart configuration group(s). Use recommended settings to get the WAN up and running quickly.

Option de workflow Créer un groupe de configuration

Profil WAN

## 2 Internet links

Static IP

Static Default Routes

Exemple d'utilisation 1 : profil WAN 1

À l'aide du workflow, vous pouvez générer la configuration complète du profil WAN pour ce cas 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

# LAN

2 VPNs

Dot1Q sub-interfaces

BGP towards Core

Route re-distribution

BGP<->OMP

Default route

advertised into OMP

from Core.

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.

**NOTE:**

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

# System

Default features –  
AAA, NTP etc.

OMP with BGP  
redistribution

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.

**NOTE:**

La configuration avancée, comme la redistribution OMP-BGP et toute autre modification apportée aux fonctionnalités du système, comme 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

## WAN Profile

1 Internet Link

1 Starlink

1 LTE link

DHCP

Static Route for Cellular  
link (AD=1)

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.

**NOTE:**

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.

## LAN Profile

2 VPNs

2 SVIs

2 Wireless SSIDs

2 Access switch ports

DIA static route

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.



NOTE:

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

**System Profile**  
**Default features - AAA,  
NTP, OMP etc.**  
**Application Performance  
monitoring**

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.

NOTE:

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

# CLI Profile NBAR enable

## 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

Pour 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.

### Groupe de configuration SiteType2

Exécutez le workflow Créer un groupe de configuration.

### Profil WAN

# WAN Profile

1 Internet link  
1 LTE link  
DHCP  
Static Route for Cellular  
link (AD=1)

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.

**NOTE:**

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

# LAN Profile

## 1 VPN

## 1 SVI

## 1 Access switch port

## DIA Static route

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.

#### NOTE:

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

Groupe de configuration SiteType3

Exécutez le workflow Créer un groupe de configuration.

Profil WAN

Identique à Configuration Group SiteType2

Profil LAN

# LAN Profile

1 VPN

1 SVI

1 Wireless SSID

1 Access switch port

DIA Static route

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.

NOTE:

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.

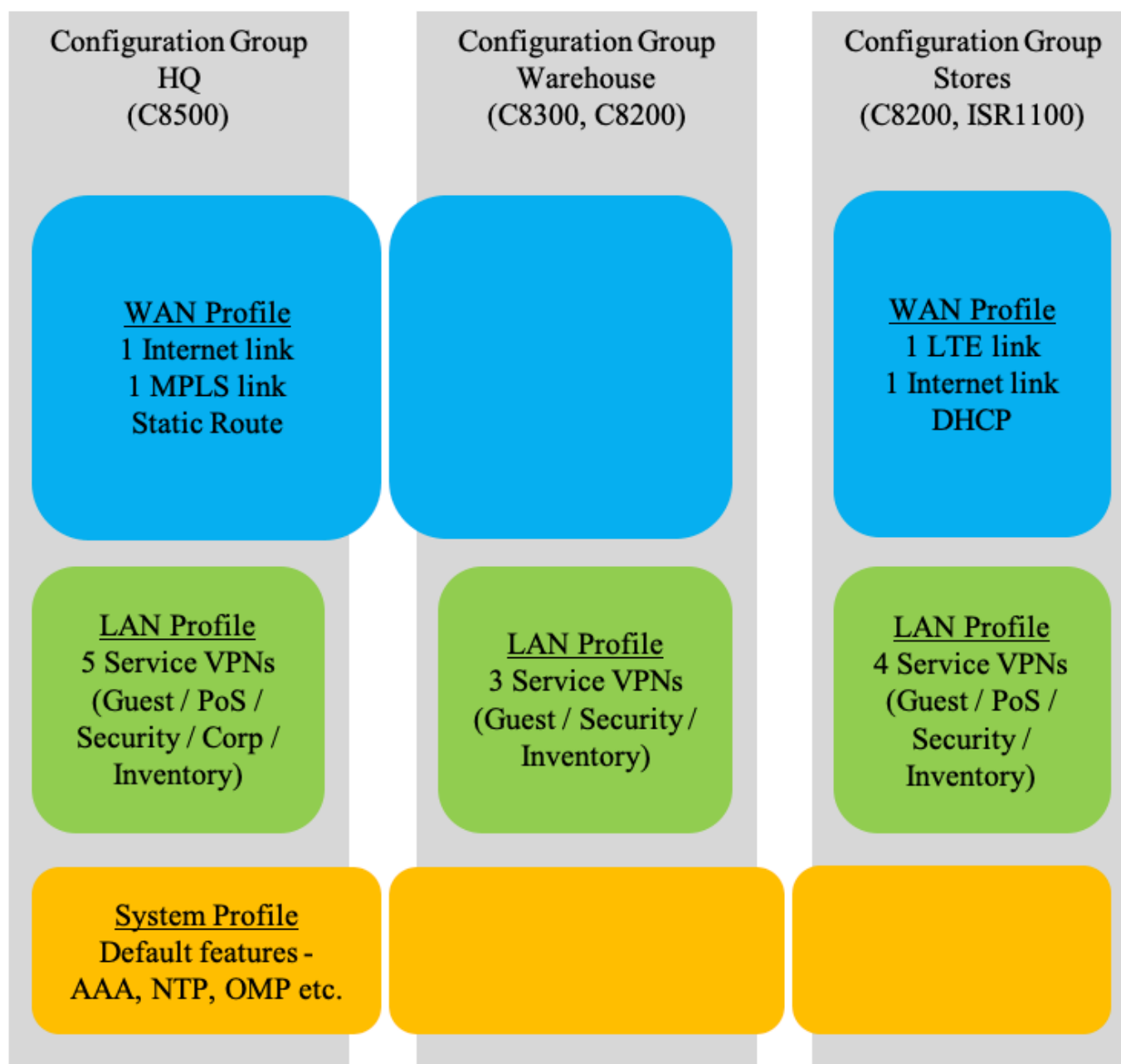
Profil système

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.

NOTE:

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.

NOTE:

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 passez en revue les étapes du workflow.

[Go Back to Configuration Group list](#)

### US-WEST-SITES [Edit](#)

Description: US-WEST-SITES

DEVICE SOLUTION sdwan	MODIFIED BY Chbsalaji	LAST UPDATED Dec 14, 2023 06:27:32
--------------------------	--------------------------	---------------------------------------

Feature Profiles **Associated Devices**

Devices (2) [Export](#)

0 selected [Associate Devices](#) [Remove Devices](#) [Add and Edit Rules](#) [Change Device Values](#) [Deploy](#) As of: Jul 15, 2024 10:23 AM

<input type="checkbox"/>	Chassis Numbers	Site Name	Hostname	Tags	Config Locked	System IP	Site ID	Device Status	Added by Rule	Last Configured	Up To Date
<input type="checkbox"/>	C8K-A51EAB60-5D3D-35C1-0051-A1D4416C1202	SITE_1	Site1-Edge	-	Yes	1.1.1.1	1	In Sync	false	Dec 14, 2023, 6:27:32 AM	True
<input type="checkbox"/>	C8K-010E1D37-0F1B-F8DF-E71A-9D58D665FD10	SITE_3	Site3-Edge	-	Yes	3.3.3.1	3	In Sync	false	Dec 14, 2023, 6:27:32 AM	True

Associer un périphérique - Groupes de configuration

## Déploiement

Exécutez le workflow Déployer le groupe de configuration.



# Deploy Configuration Group

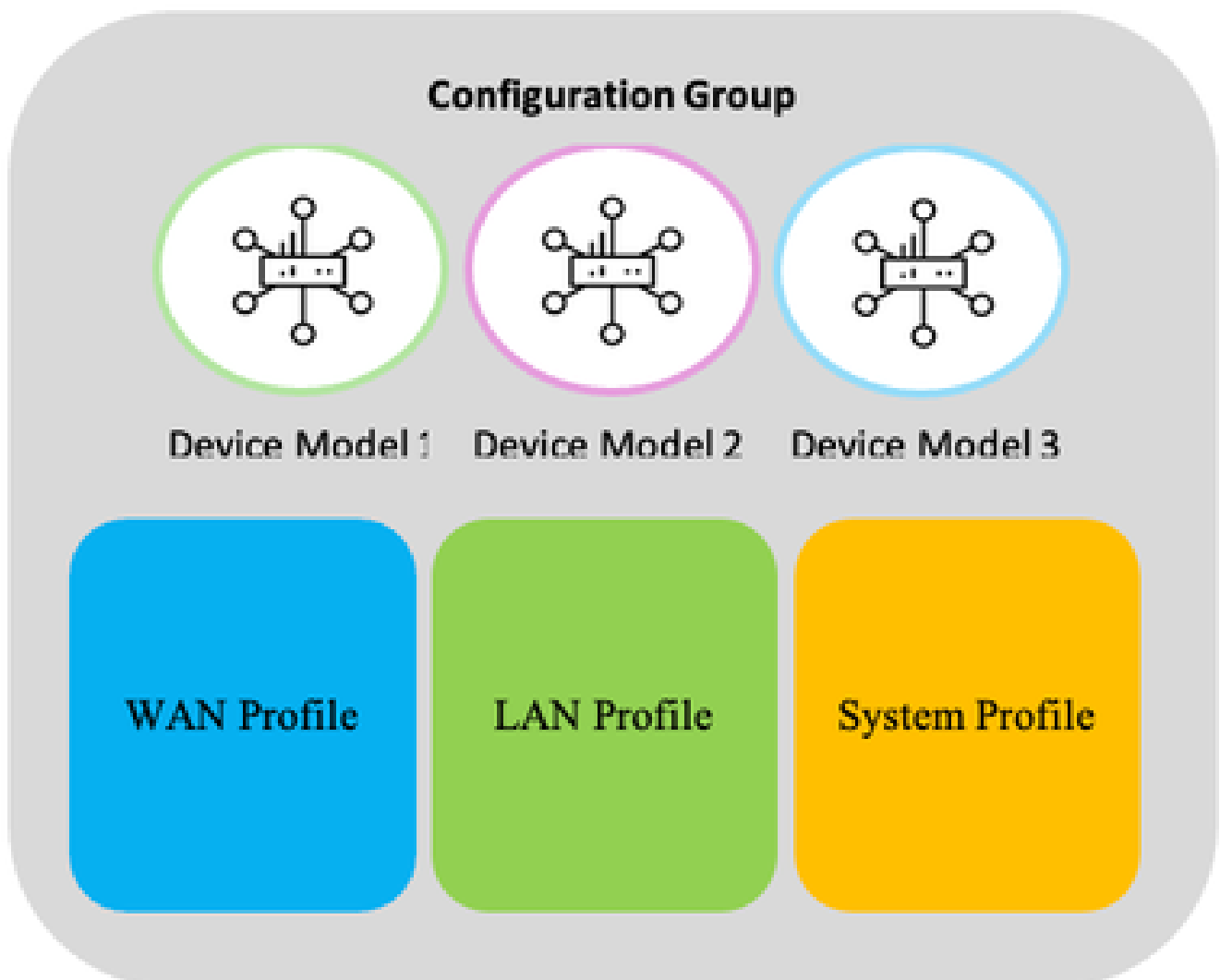
Push configuration to devices in your WAN

**NOTE:**

- 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, alors 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 de l'étape Ajouter/Vérifier la configuration du périphérique.

## Réutilisabilité

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

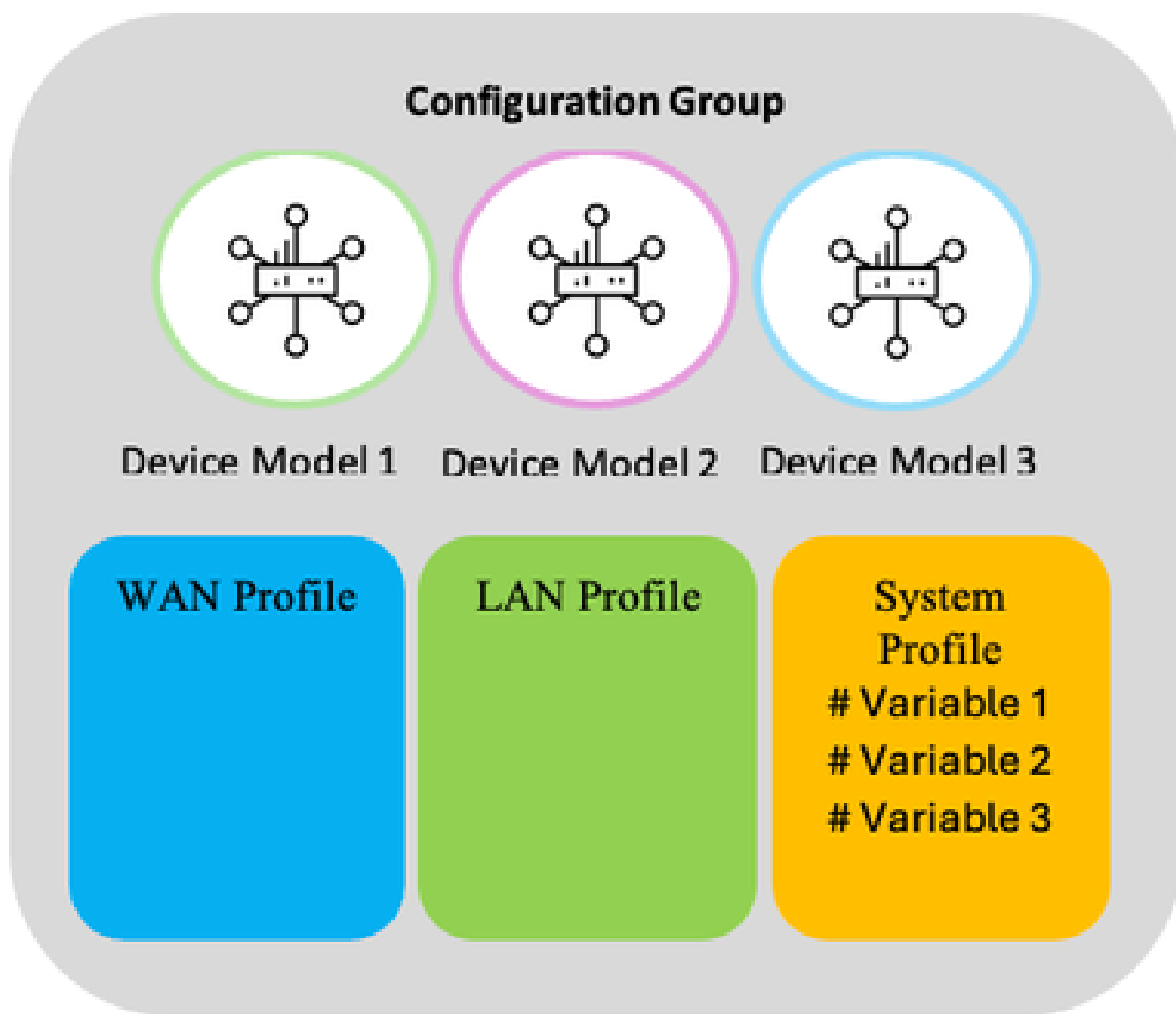


**NOTE:**

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. Utiliser les variables de configuration - valeurs spécifiques au périphérique

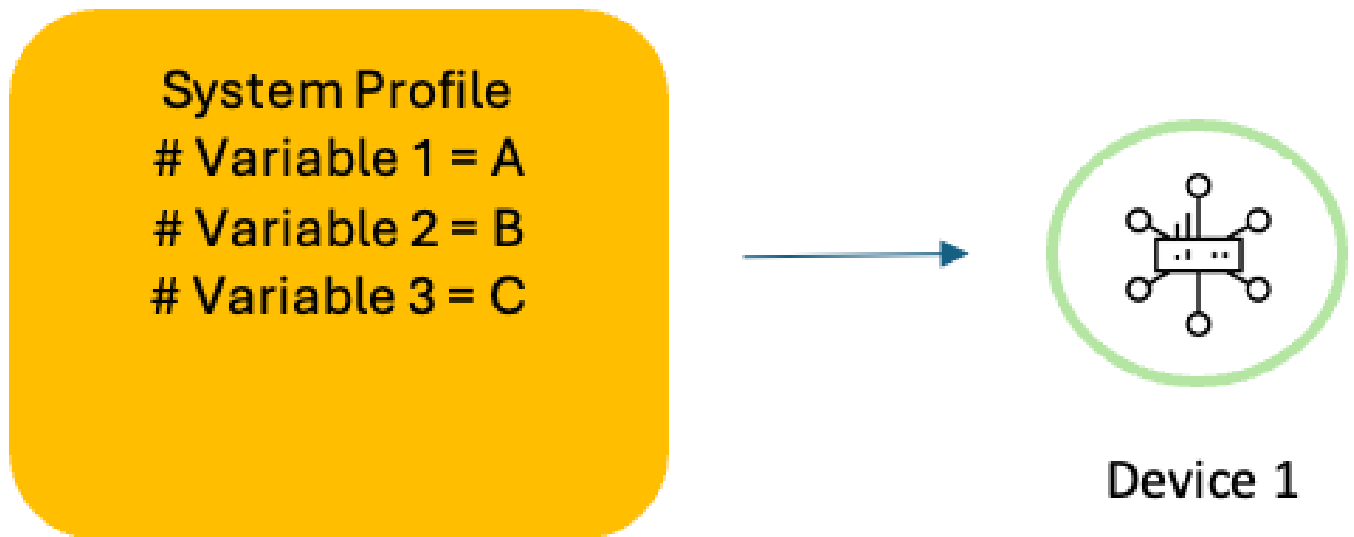


Groupe de configuration - Variables propres au périphérique

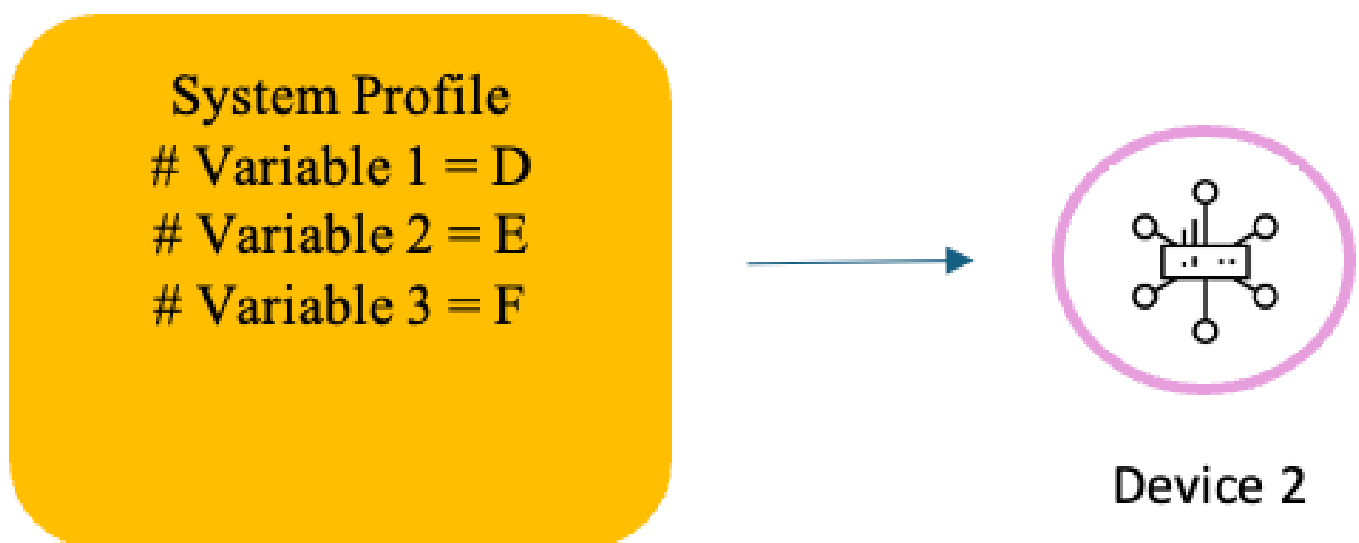
Un profil de fonctionnalité peut avoir une configuration spécifique au périphérique, similaire aux variables de modèle.

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

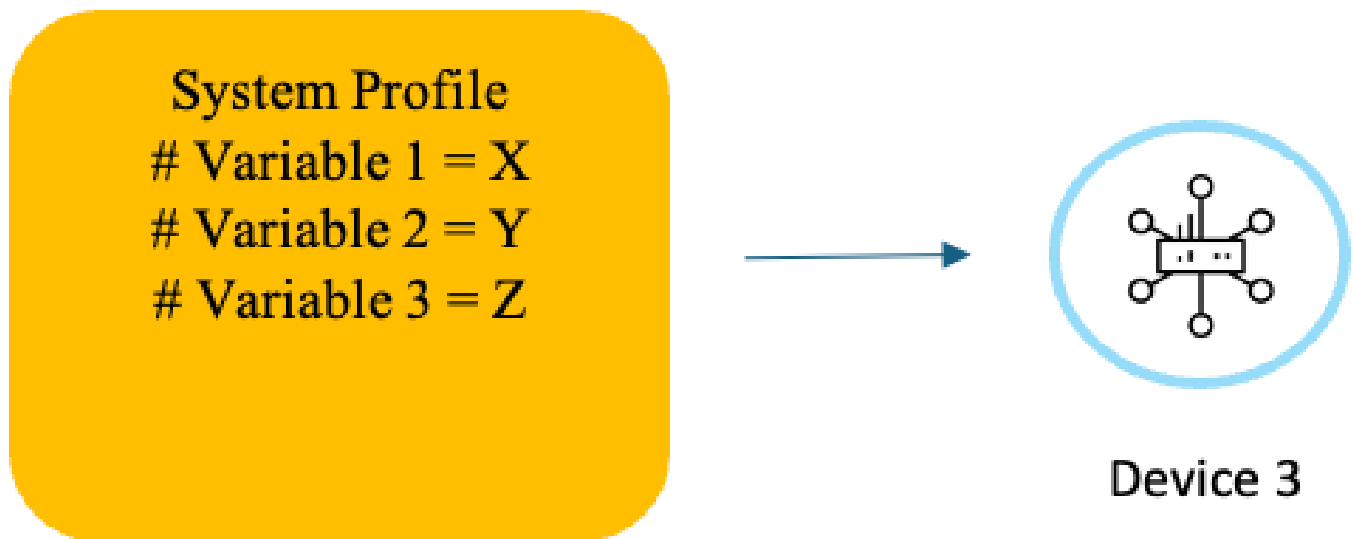
Ces valeurs spécifiques au périphérique peuvent être fournies au moment du déploiement. Et il peut être différent pour différents périphériques.



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

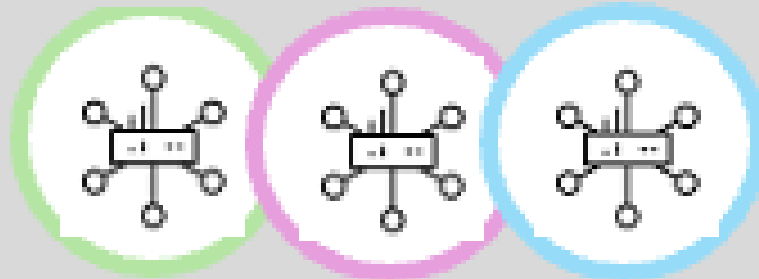
### 3. Réutilisation des profils de fonction

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.

# Configuration Group



**WAN  
Profile  
1**

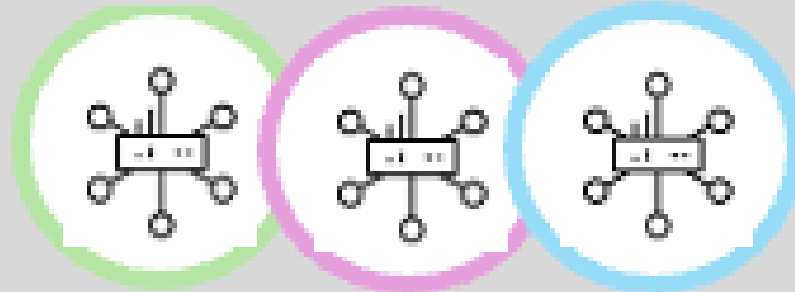
**LAN  
Profile  
1**

**System  
Profile  
1**

Réutilisation des profils de fonction - 1

Profil LAN 1

# Configuration Group



**WAN  
Profile  
1**

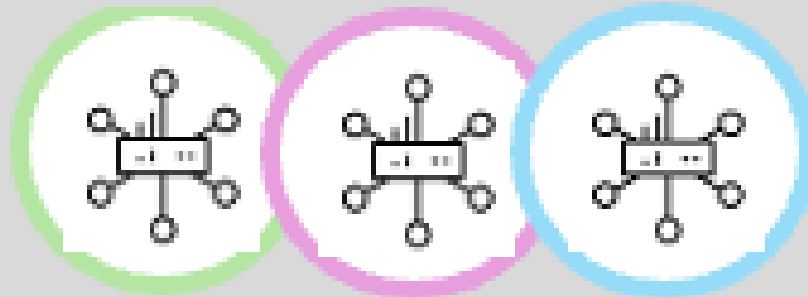
**LAN  
Profile  
2**

**System  
Profile  
1**

Réutilisation des profils de fonction - 2

Profil LAN 2

# Configuration Group



**WAN  
Profile**

**1**

**LAN  
Profile**

**3**

**System  
Profile**

**1**

Réutilisation des profils de fonction - 3

Profil LAN 3

## Catalogue d'applications

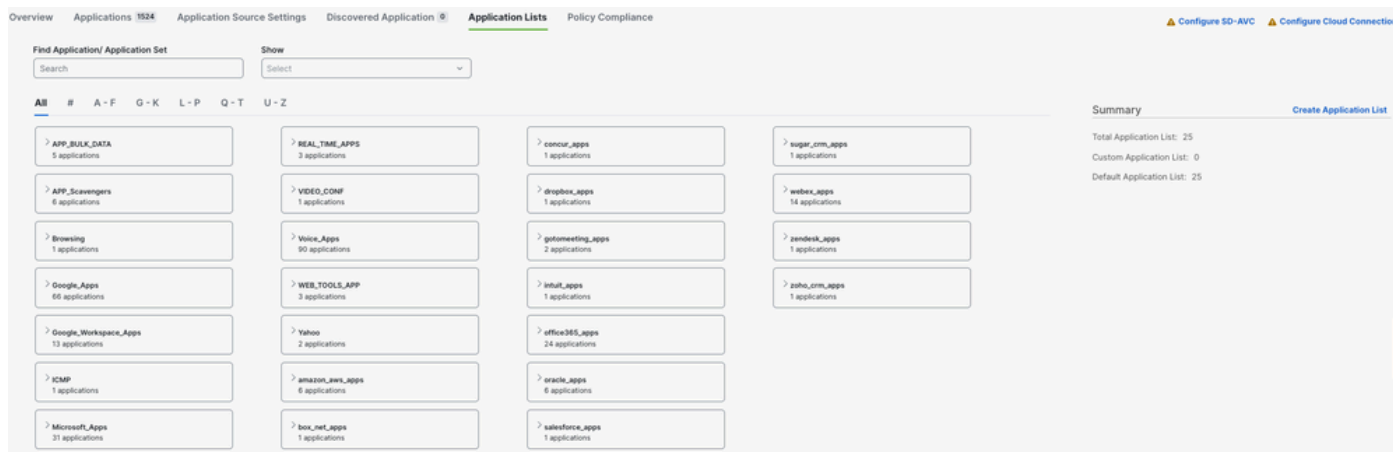
Les périphériques traditionnels étaient capables de manipuler les flux de trafic par la mise en correspondance conditionnelle des adresses IP source et/ou de destination, des ports source/de destination et des protocoles. Étant donné que de plus en plus d'applications dépendent du DNS ou sont intégrées 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



mis à jour rapidement, ce qui est important lorsque les fournisseurs de cloud modifient les emplacements d'hébergement ou les 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 affecte 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 d'un groupe de configuration sur un périphérique sont des conditions préalables au déploiement d'un groupe de stratégies sur ce périphérique.

Cisco Catalyst SD-WAN Select Resource Group Configuration · Policy Group of Interest

Policy Group 3 Application Priority & SLA 7 Embedded Security 6 Secure Internet Gateway 4 DNS Security 1

As of: 12 August 2024 at 10:24

Search

Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
US-West-Policy	US-West-Policy						

**US-West-Policy**

Policy Group Name \*  
US-West-Policy

Description  
US-West-Policy

Policy

Application Priority  
App-Visibility

Embedded Security  
US-West-Security

Secure Internet Gateway  
Please Select one

DNS Security  
Please Select one

Deployment  
Associated to: 2 Device(s)

Save Deploy

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.

**SDWAN Fabric Traffic Policy**

Priority	Preferred Path	When SLA not met	Backup Path
<b>Gold</b> Business Relevant	Select Preferred Path	Default to Best Path	Not Applicable
<b>Silver</b> Default	Select Preferred Path	Default to Best Path	Not Applicable
<b>Bronze</b> Business Irrelevant	Select Preferred Path	Default to Best Path	Not Applicable

**Internet Offload Traffic**

Policy	Application List	Fallback to Routing
<b>Secure Internet Gateway</b>	Select Application List	<input type="checkbox"/>
<b>Direct Internet Access</b>	Select Application List	<input type="checkbox"/>

**Apply Policy**

Target	Direction	VPN	Interface
	Enter Direction	Select VPN	Enter Interfaces

[View](#) [Variable](#)

Mode simple

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

#### NOTE:

1. L'action par défaut est DROP
2. Les critères de correspondance peuvent être Applications uniquement. Si vous avez besoin de préfixes, utilisez le mode avancé

Mode avancé

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

Search Traffic Policy [Add Traffic Policy](#)

**BH\_DIA\_traffic (3)** [Edit Policy](#) [Delete Policy](#) [Add Rules](#) [Delete All Rules](#)

VPN: Employee Direction: service

Search Rule by Name or Order

NAME	MATCH	ACTION
> 1 DNS	Destination Port - 53	Count - DNS_Counter Nat Use Vpn - true
> 2 traffic	App List - O365	Count - O365_Counter Nat Fallback - true Nat Use Vpn - true
> 3 Allow_All		Count - SIG_Counter Secure Internet Gateway - true

Rules per page 10 < 1 > Go to: 1 / 1

**SLA Class** **QoS Queue**

No SLA Class added, add your first SLA Class in Traffic Policy

Mode avancé

NOTE:

1. L'action 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 :

Advanced Layout



---

**SLA Class**

**QoS Queue**

---

[+ Add QoS Policy](#)

No Qos Class added, add your first Qos Class in Traffic Policy

Ajouter une stratégie QoS

### Queueing Model

Policy Name \*

Target Interface \*

Value Variable

Queue	Forwarding Class	Bandwidth %	Drops	Scheduling Type
0	Select one		Tail	Low Latency Queuing (LLQ)
1	Select one	40 %	Random Early	Weighted Round Robin (WRR)
2 (default)	Select one	20 %	Random Early	Weighted Round Robin (WRR)
3	Select one	30 %	Random Early	Weighted Round Robin (WRR)

Bandwidth

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.

Policies > Application Priority & SLA

#### Basic\_4Queue\_QoS\_Policy (Total Traffic Policy: 1)

Additional Settings Advanced Layout

NAME	MATCH	ACTION
1 Match_Voice_Traffic	Dscp - 46	Base Action - accept Count - voice Forwarding Class - VOICE Log - true
2 Match_Critical_Apps	App List - Microsoft_Apps	Base Action - accept Count - critical_apps Forwarding Class - CRITICAL_DATA Log - true
3 Match_Bulk_Data_Traffic	Destination Data Prefix List - DC_File_Servers Destination Port - 21	Base Action - accept Count - bulk_data Forwarding Class - BULK_DATA Log - true
4 Match_All_Other		Base Action - accept Forwarding Class - DEFAULT

VOICE  
bandwidth 10%

CRITICAL\_DATA  
bandwidth 40%

BULK\_DATA  
bandwidth 20%

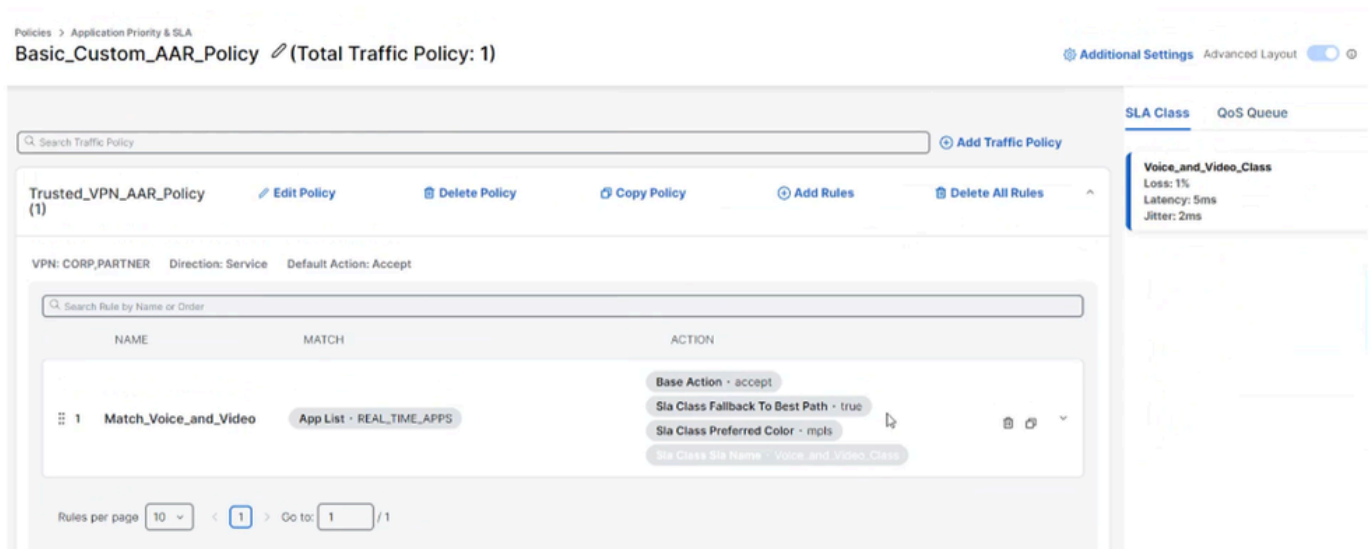
DEFAULT  
bandwidth 30%

Politique QoS 2

### Routage sensible aux applications

Vous pouvez définir des classes SLA et les utiliser dans une politique de trafic pour réaliser

## l'objectif d'une politique AAR.



Politique AAR

## Visibilité des applications/flux

Pour 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.

## Politique de trafic

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

⊕ Add Traffic Policy

MyTrafficPolicy (1) [Edit Policy](#) [Delete Policy](#) [Add Rules](#) [Delete All Rules](#)

VPN: Corporate\_Users,Local\_Internet\_for\_Guests,Physical\_Security\_Devices Direction: all

NAME	MATCH	ACTION
1 Rule1		

Sequence: 1  Protocol: IPv4

Match [Add Match](#)

Action [Add Action](#)

Base Action

Accept  Drop

[Cancel](#) [Save Match and Actions](#)

## Politique Du Trafic

### NOTE:

Si une politique de priorité d'application et de SLA est créée en mode simple, puis basculée en mode avancé, certaines options de correspondance ne sont pas disponibles pour la sélection. Exemple : le préfixe de données de destination est grisé.

Pour rendre ces options disponibles, changez le protocole de BOTH à IPv4 ou IPv6 selon les besoins.

## Sécurité intégrée

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

## 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.

### NOTE:

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

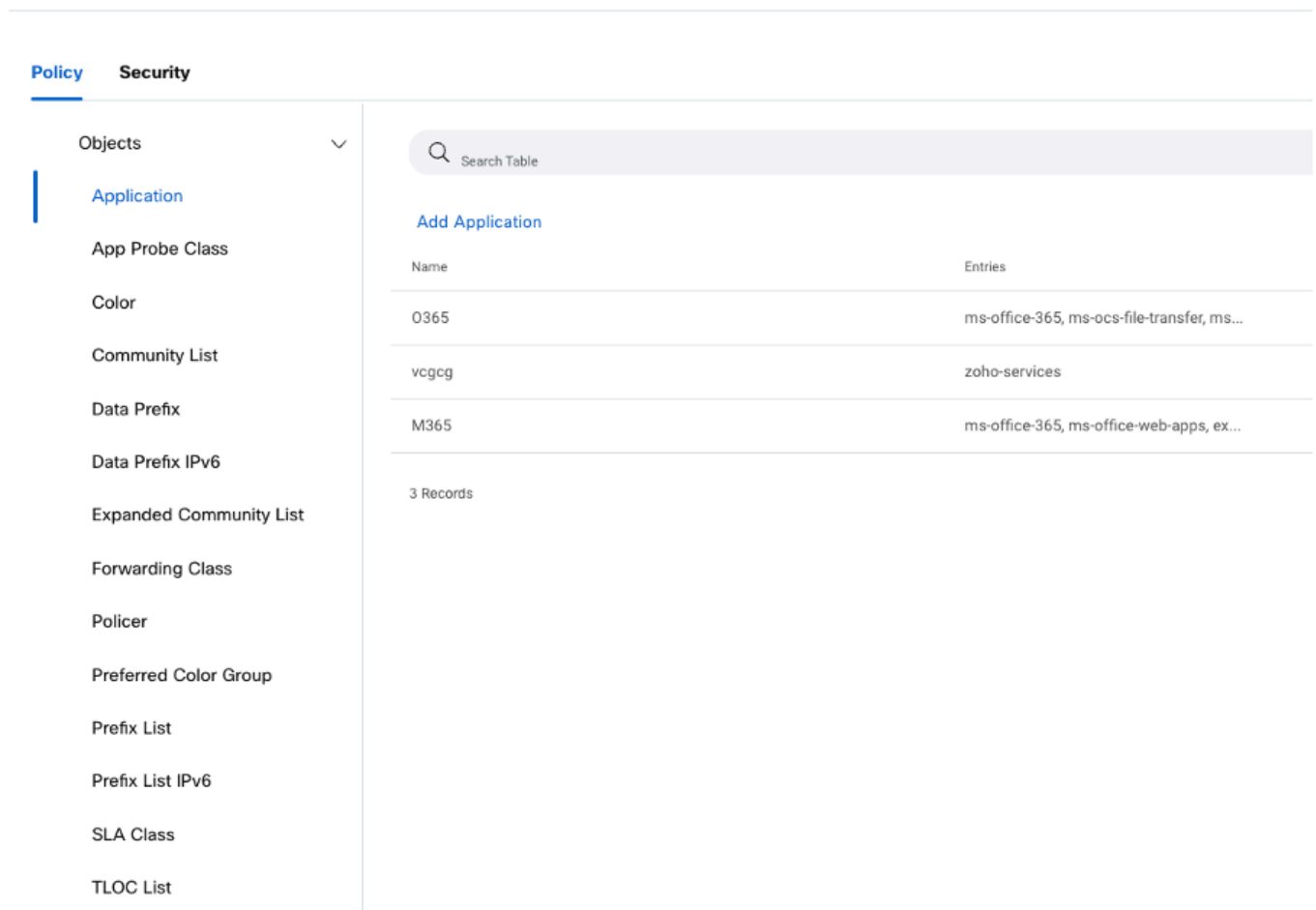
## Sécurité DNS

Définissez les paramètres permettant 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, listes VPN, listes de sites, 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.



The screenshot shows a web interface for configuring security policies. The 'Policy' tab is selected, and the 'Security' section is active. On the left, a sidebar lists various object types under 'Objects', with 'Application' selected. The main area displays a table of application objects with a search bar and an 'Add Application' button. The table has two columns: 'Name' and 'Entries'. Three records are shown:

Name	Entries
0365	ms-office-365, ms-ocs-file-transfer, ms...
vcgcg	zoho-services
M365	ms-office-365, ms-office-web-apps, ex...

Below the table, it indicates '3 Records'.

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

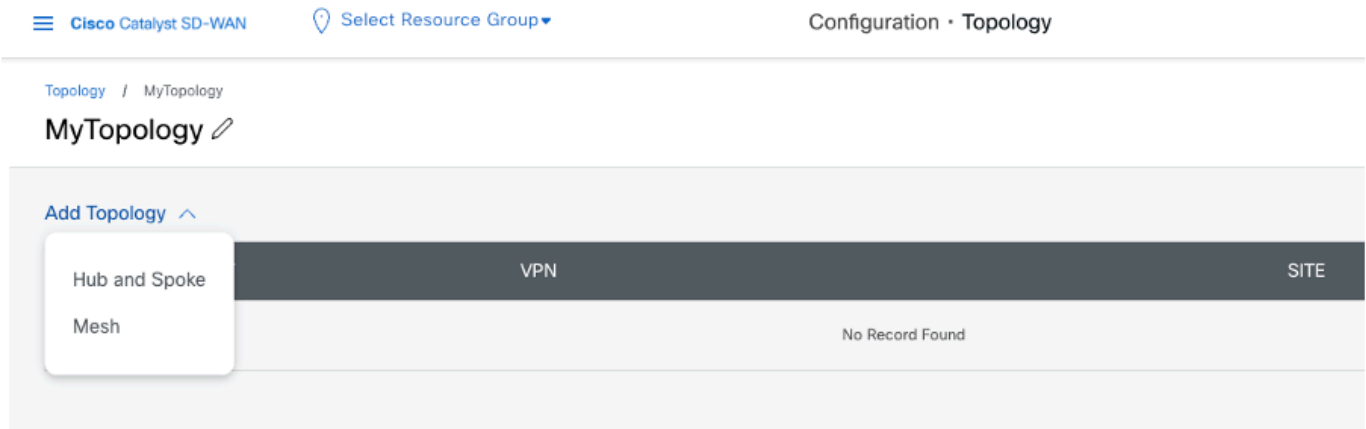


groupes de configuration.

## 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 des VPN du workflow de topologie affiche une instance de VPN d'entreprise uniquement.

Une fois que vous avez sélectionné Corporate VPN, le SD-WAN Manager détermine les ID VPN en fonction de la topologie.

Disons qu'il y a 2 périphériques dans 2 sites :

1. Périphérique1 du 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 aura 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 aura l'ID VPN 10 uniquement.

Si seul le site 200 fait partie de la topologie, SD-WAN Manager crée une liste VPN qui aura 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 intégrer 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.



# Quick Connect

Onboard your devices.

Workflow de connexion rapide



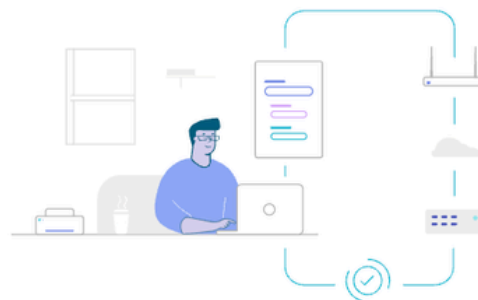
## Welcome to Quick Connect

Before getting started, ensure that you have the following configured:

- Organization Name
- Certificate Authorization
- vSmart, vBond, vManage controllers (as applicable)

[Haven't configured them yet? Do it here.](#)

Note : This workflow supports adding up to 25 devices at a time.  
For more devices, use device template to configure.



Get Started

Don't show this to me again

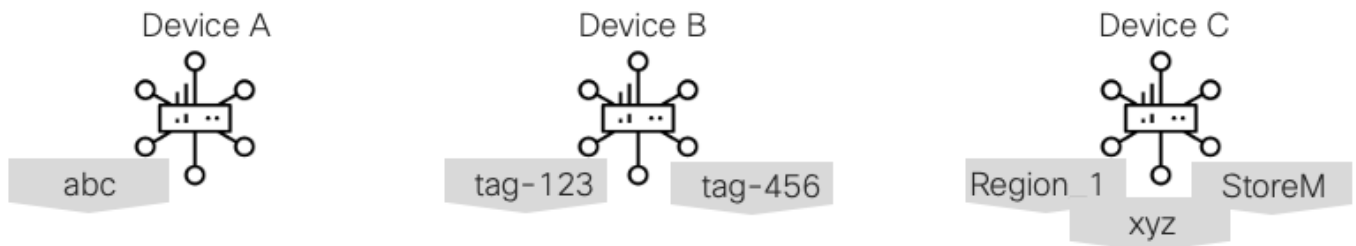
Description du workflow de connexion rapide

# 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/supprimées des périphériques.

## Règles de balise dans le groupe de configuration

Dans la page Groupe de configuration -> Périphériques associés, vous pouvez ajouter/modifier des règles de balise.

## Illustration

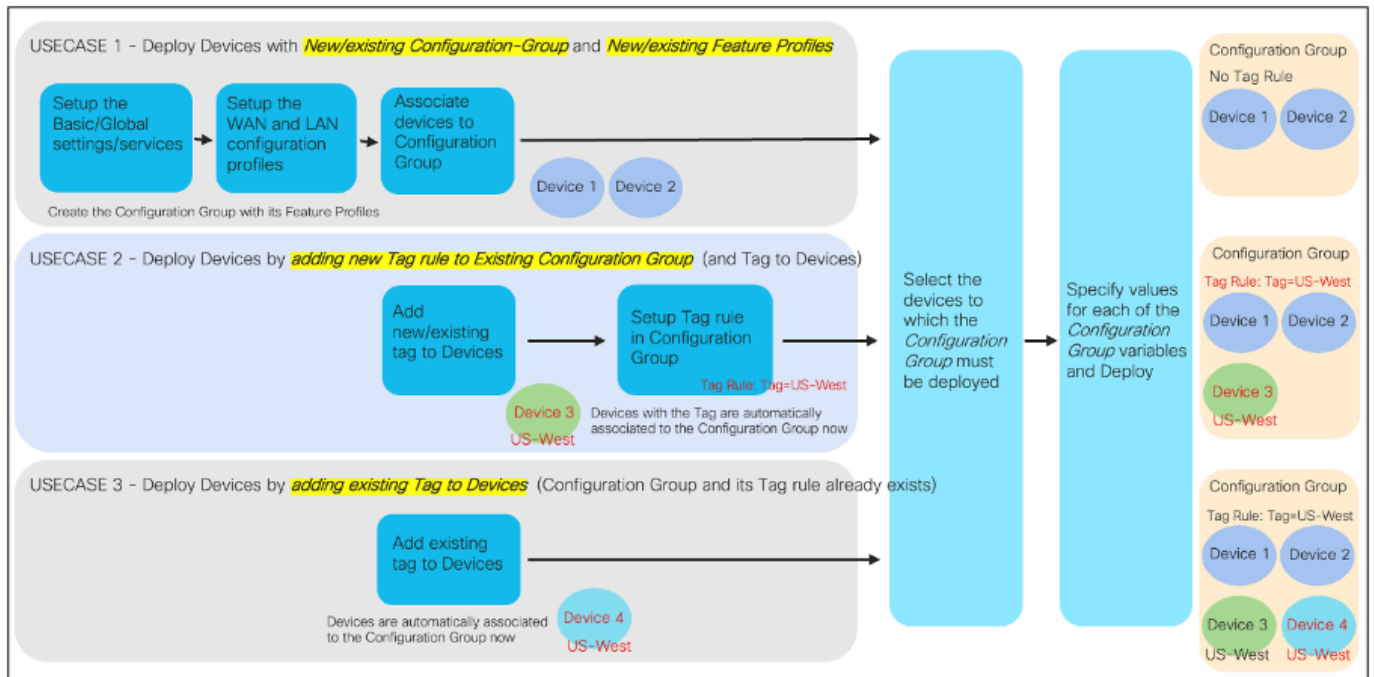


Illustration de balisage

## 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 propose quelques recommandations aux clients qui souhaitent bénéficier 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 les points de suspension (...) situés à droite du groupe de périphériques et sélectionnez « Export CSV » (Exporter CSV) dans la zone Configuration à Templates (Configuration à modèles).
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 d'attache, mais ne reçoit aucune modification ultérieure apportée 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. Vous obtenez ainsi un aperçu des parties du groupe de configuration qui ne correspondent pas à l'instance précédente, ou des variables qui ont été modifiées à partir du 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'alphabetiser 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, nous modifions simplement la façon dont la configuration des politiques est créée (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 priorité d'application et 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 services sécurisés, 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 des configurations mises à jour aux périphériques de périphérie (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 stratégie (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 du composant Application Priority & SLA.

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

NOTE:

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 stratégie (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 pour la simplicité et pour réduire la confusion parmi le personnel opérationnel.

## Outil de conversion

### Portée

L'outil de conversion effectue une conversion 1 à 1 des modèles en groupes de configuration. L'outil collecte les modèles à partir d'une instance de SD-WAN Manager, les convertit en groupes de configuration (y compris les profils et les parcelles de fonctionnalités) et télécharge les nouvelles constructions converties vers le SD-WAN Manager.

\* La conversion des politiques en groupes de politiques devrait être disponible dans l'outil de conversion en octobre 2024.

### Détails d'accès

Une version bêta de l'outil est disponible. Veuillez contacter [sdwan-ux-conversion-tool@cisco.com](mailto:sdwan-ux-conversion-tool@cisco.com) pour plus d'informations.

### Marche à suivre

#### Prérequis

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.

#### Workflow de l'outil de conversion

Étape 1	Connectez-vous à l'outil à l'aide des identifiants fournis par Cisco. (Remarque : il ne s'agit pas d'informations d'identification CCO. Contactez <a href="mailto:sdwan-ux-conversion-tool@cisco.com">sdwan-ux-conversion-tool@cisco.com</a> pour plus de détails).
Étape 2	Sélectionnez le workflow « Outil de conversion » depuis la page d'accueil. · Si vous avez déjà effectué ce workflow et que vous disposez du fichier JSON avec les configurations converties, vous devez sélectionner le workflow « Télécharger à partir d'un fichier ».

Étape 3	<p>Connexion:</p> <p>Indiquez l'adresse IP ou l'URL de votre gestionnaire SD-WAN, ainsi que les informations d'identification utilisateur.</p> <ul style="list-style-type: none"> <li>· L'utilisateur doit avoir un accès en lecture/écriture.</li> <li>· Les champs Port et Sous-domaine sont facultatifs.</li> </ul>
Étape 4.	<p>Importer :</p> <p>Cliquez sur le bouton Collecter pour récupérer toutes les constructions héritées (modèles de périphériques, modèles de fonctionnalités, stratégies et leurs constructions associées) à partir de SD-WAN Manager.</p> <ul style="list-style-type: none"> <li>· Une fois collecté, vous devez télécharger le fichier JSON contenant toutes les configurations. Ce fichier doit être utilisé au cours de cette étape ultérieurement au lieu d'être à nouveau collecté à partir du gestionnaire SD-WAN.</li> </ul>
Étape 5.	<p>Sélectionnez :</p> <p>Sélectionnez les modèles et stratégies que vous souhaitez convertir en leurs nouveaux équivalents. Cliquez sur « Migrer » pour convertir les constructions sélectionnées.</p>
Étape 6.	<p>Transformation:</p> <p>Cette page affiche toutes les constructions nouvellement converties. Une fois prêt, cliquez sur « Upload » pour transférer ces configurations vers le gestionnaire SD-WAN.</p> <ul style="list-style-type: none"> <li>· Si vous n'êtes pas encore prêt à passer à SD-WAN Manager, vous pouvez télécharger ces configurations converties sous forme de fichier JSON et utiliser le workflow « Upload from a file » ultérieurement.</li> </ul>
Étape 7.	<p>Résumé:</p> <p>À ce stade, les configurations sont diffusées et créées dans le gestionnaire SD-WAN. Au fur et à mesure de la diffusion des configurations, vous pouvez voir la barre de progression. Une fois le téléchargement terminé, vous pouvez voir le résumé des configurations téléchargées.</p> <ul style="list-style-type: none"> <li>· Vous pouvez utiliser les liens rapides « Groupes de configuration », « Profils de fonctionnalités » et « Groupes de stratégies » pour afficher les nouvelles constructions dans votre gestionnaire SD-WAN.</li> </ul>

	<ul style="list-style-type: none"><li>· En cas d'erreur ou d'erreur, le retour arrière est également disponible à cette étape. L'exécution d'une restauration supprime toutes les constructions transmises au gestionnaire SD-WAN au cours de ce workflow/de cette session.</li></ul>
--	---

## Post-Conversion

Vos nouvelles constructions sont maintenant prêtes à l'emploi. Exécutez les étapes de la section « Déploiements existants » pour migrer vos périphériques vers les groupes de configuration nouvellement convertis.

## Considérations

- Les conversions fournies par l'outil sont destinées à servir de guide. Veuillez analyser et tester avant de procéder au déploiement dans un environnement de production.
- 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 des constructions héritées sont copiés sur les constructions nouvellement converties.
- 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.

## 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	Possibilité de copier/dupliquer des profils de fonctionnalité, stratégie non prise

	<p>en charge. Un ensemble de scripts Python peut accomplir cette tâche et se trouve :</p> <p><a href="https://github.com/dbrown92700/configGroups/">https://github.com/dbrown92700/configGroups/</a></p>
5	<p>Un profil d'objet de stratégie doit être associé au groupe de configuration avant de créer un lot de fonctionnalités lié à la configuration de stratégie (stratégies localisées). Exemple : ACL</p>
6	<p>Import CSV for interface variables insère des points-virgules dans la chaîne et échoue</p>
7	<p>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)</p>
8	<p>Cloud OnRamp pour SaaS continue d'utiliser les modèles/politiques hérités.</p>
9	<p>TrustSec / SGT pris en charge avec le profil CLI uniquement</p>
10	<p>Prise en charge de UC Voice / DSP Farm / SRST avec profil CLI uniquement (à partir de 20,13 dans le paquet UI)</p>

## Informations connexes

- Cisco SD-WAN et réseau cloud YouTube Channel : <https://www.youtube.com/@CiscoSDWANandCloudNetworking>
- UX2.0 - Simplification opérationnelle : 1. Configuration d'un site de routeur unique : <https://www.youtube.com/watch?v=98z-d3knd>
- [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.