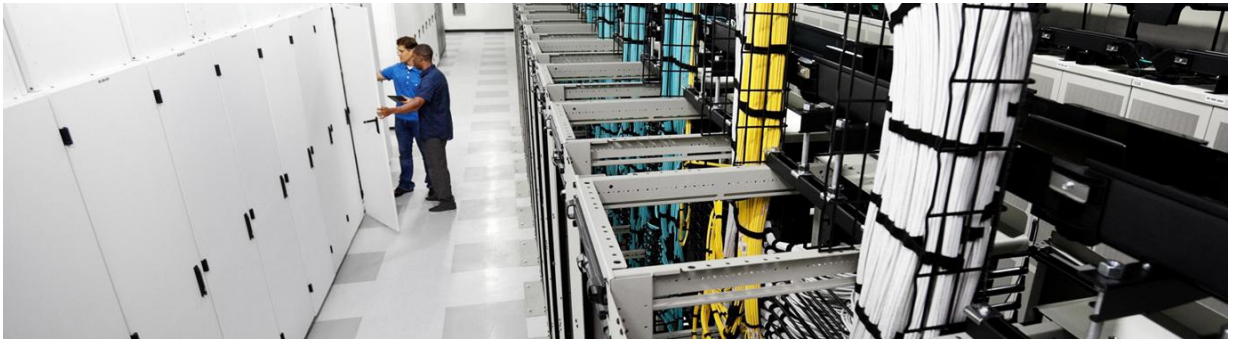


# Principes d'une infrastructure axée sur les applications



## Présentation

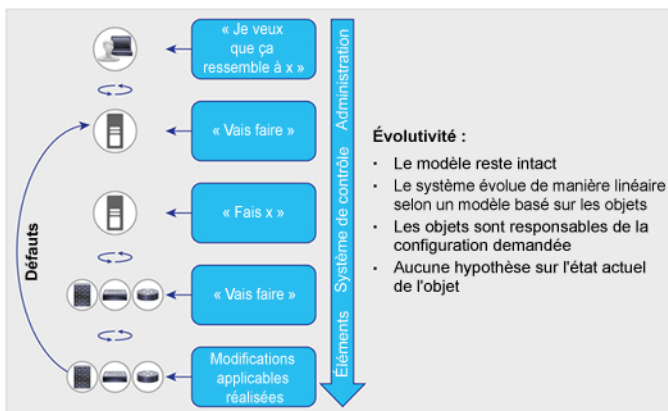
L'une des principales innovations apportées dans l'infrastructure axée sur les applications (ACI) réside dans l'introduction d'une interface présentant un niveau d'abstraction élevé. Cela permet de représenter la connectivité des composants applicatifs avec les politiques de haut niveau qui la régissent. Simple d'utilisation pour les développeurs d'applications, le modèle améliore simultanément l'automatisation et la sécurité.

## Théorie des politiques de l'ACI

Le modèle de politique de l'ACI est un modèle orienté objet basé sur la théorie de la promesse. Celle-ci s'appuie sur un contrôle évolutif des objets intelligents, contrairement aux modèles impératifs plus traditionnels pensés comme des systèmes de gestion descendants. Dans ces derniers, le gestionnaire central doit être informé des commandes de configuration des objets sous-jacents et de l'état actuel de ces objets.

La théorie de la promesse, quant à elle, repose sur la capacité des objets sous-jacents à gérer les changements d'état de configuration initiés par le système de contrôle comme des « changements d'état souhaités ». Les objets sont alors chargés de transmettre directement les exceptions ou les défaillances au système de contrôle. Cette approche réduit la charge et la complexité du système de contrôle et offre une meilleure évolutivité. En outre, elle autorise les objets sous-jacents à transmettre des demandes de changement d'état. Ces demandes peuvent les concerner ou impliquer d'autres objets de niveau inférieur (figure 1).

**Figure 1.** Approche de la théorie de la promesse pour le contrôle d'un système de grande envergure



Dans ce modèle théorique, l'infrastructure axée sur les applications conçoit un modèle d'objet pour le déploiement d'applications, ces dernières en constituant le point central. Historiquement, les applications étaient limitées par les capacités du réseau et par des configurations visant à prévenir leur utilisation abusive. Des concepts tels que l'adressage, le VLAN et la sécurité sont depuis toujours intimement liés, ce qui limite l'évolutivité et la mobilité des applications. Alors que les applications sont redessinées pour la mobilité et l'évolutivité web, cette approche traditionnelle empêche leur déploiement rapide et homogène.

Le modèle de politique de l'ACI ne dicte rien concernant la structure du réseau sous-jacent. Conformément à la théorie de la promesse, il fait appel à un élément périphérique, appelé iLeaf, pour gérer la connexion à différents périphériques.

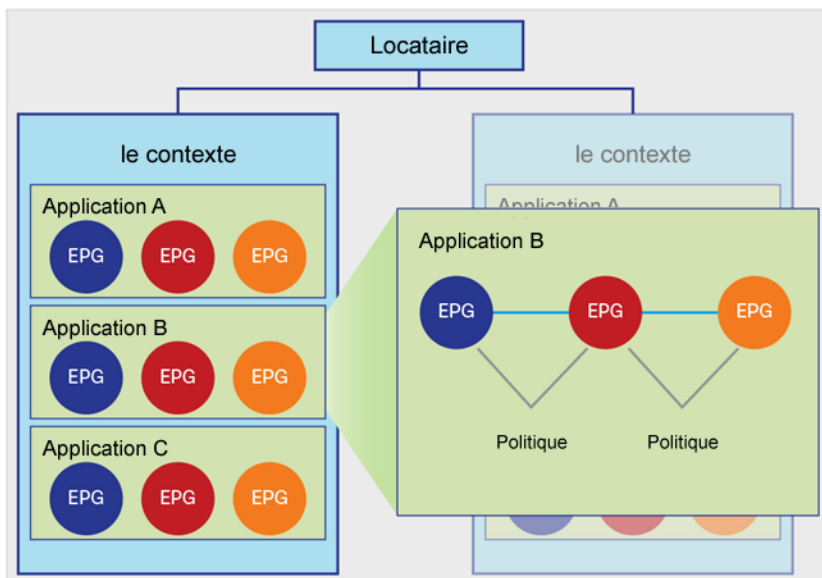
### Modèle d'objet

Au niveau supérieur, le modèle d'objet de l'ACI repose sur un groupe d'un ou plusieurs locataires, ce qui permet de séparer l'administration de l'infrastructure réseau des flux de données. Les locataires peuvent être des clients, des unités commerciales ou des groupes, selon les besoins de l'entreprise. Ainsi, une entreprise peut utiliser un seul locataire pour l'ensemble de son organisation, tandis qu'un fournisseur de services Cloud pourra utiliser un ou plusieurs locataires pour certains de ses clients.

Il est également possible de distinguer les locataires en fonction de contextes, liés directement à des instances Virtual Routing and Forwarding (VRF), ou d'espaces IP séparés. Selon ses besoins commerciaux, chaque locataire peut avoir un ou plusieurs contextes. Ces derniers permettent de distinguer de manière plus détaillée les besoins organisationnels et de transfert d'un locataire spécifique. Les contextes utilisent des instances de transmission séparées. Dans ce cas, l'adressage IP peut être dupliqué dans des environnements multilocataires.

Au sein du contexte, le modèle fournit une série d'objets qui définissent l'application. Les objets englobent les terminaux, les groupes de terminaux et les politiques qui définissent leur relation (figure 2). Il est important de noter que les politiques représentent ici bien plus qu'un simple ensemble de listes de contrôle d'accès. Elles incluent les filtres entrants et sortants, les paramètres de qualité du trafic, ainsi que les règles de marquage et de redirection.

Figure 2. Modèle d'objet logique



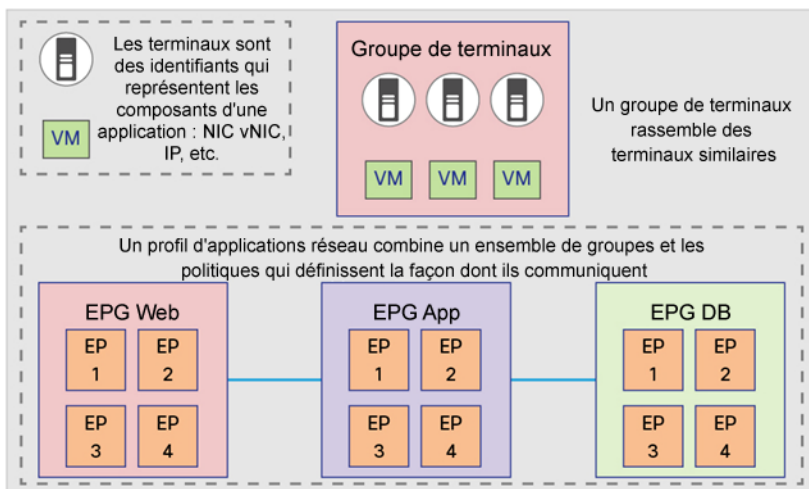
La figure 2 montre un locataire comprenant deux contextes et les applications qui les composent. Les groupes de terminaux illustrés composent un niveau d'application ou un groupement d'applications logique. Par exemple, l'application B (développée sur le côté droit) peut se composer d'un niveau web (bleu), d'un niveau application (rouge) et d'un niveau base de données (orange). La combinaison des groupes de terminaux et des politiques qui définissent leur interaction est dénommée profil d'applications réseau dans le modèle ACI.

### Groupes de terminaux

Un groupe de terminaux rassemble des terminaux similaires représentant un niveau d'application ou un ensemble de services. Il s'agit d'un groupement logique d'objets nécessitant une politique similaire. Par exemple, les composants du niveau web d'une application peuvent constituer un groupe de terminaux. Un terminal est défini par sa carte d'interface réseau, sa carte virtuelle d'interface réseau, son adresse IP ou son nom DNS. Le système est suffisamment évolutif pour permettre la prise en charge de futures méthodes d'identification des composants applicatifs.

Les groupes de terminaux peuvent également représenter des entités telles que des réseaux externes, des services réseau, des dispositifs de sécurité et des solutions de stockage réseau. Selon le modèle de déploiement d'applications utilisé, il s'agit d'ensembles d'un ou de plusieurs terminaux offrant une fonction similaire ou de groupements logiques offrant une multitude d'options d'utilisation (figure 3).

**Figure 3.** Relations au sein des groupes de terminaux



La flexibilité des groupes de terminaux permet de les personnaliser en fonction des modèles de déploiement choisis par le client. Ils sont utilisés pour définir les éléments auxquels la politique s'applique. La politique est appliquée entre les groupes de terminaux au sein du fabric de réseau, définissant ainsi la façon dont ils communiquent entre eux. Cette approche est conçue pour pouvoir être étendue aux futurs groupes de terminaux.

Voici quelques exemples d'utilisation des groupes de terminaux :

- Groupe défini par des VLAN réseau traditionnels : tous les terminaux connectés à un VLAN spécifique sont placés dans un même groupe
- Groupe défini par un Virtual Extensible LAN (VXLAN) : tous les terminaux connectés à un VXLAN spécifique sont placés dans un même groupe
- Groupe mappé sur un groupe de ports VMware
- Groupe défini par son adresse IP ou sous-réseau : par exemple, 172.168.10.10 ou 172.168.10
- Groupe défini par un nom ou une plage DNS : par exemple, example.foo.com ou \*.web.foo.com

L'utilisation des groupes de terminaux offre flexibilité et évolutivité. L'objectif est de fournir les outils de construction d'un modèle de réseau d'application mappé sur le schéma de déploiement de l'environnement réel. La définition des terminaux est évolutive, ce qui garantit la prise en charge des futures améliorations produit et l'adaptation aux exigences du secteur.

Le modèle des groupes de terminaux offre plusieurs avantages en matière de gestion. Il permet d'appliquer une politique uniforme à des objets uniques, pour des outils d'orchestration et d'automatisation d'un niveau supérieur. Les outils ne doivent pas nécessairement opérer sur les terminaux individuels pour modifier les politiques. Ce fonctionnement permet de garantir la cohérence entre les terminaux du même groupe, quel que soit leur emplacement sur le réseau.

### Application des politiques

La relation entre les groupes de terminaux et les politiques peut être appréhendée comme une matrice, dans laquelle un axe représente le groupe de terminaux sources (sEPG) et l'autre le groupe de terminaux de destination (dEPG). Les politiques appliquées sont placées à l'intersection des sEPG et dEPG appropriés. La matrice est le plus souvent incomplète, car de nombreux EPG n'ont pas besoin de communiquer avec les autres (figure 4).


**Figure 4.** Matrice d'application des politiques

		Destination		
		EPG A	EPG B	EPG N
Source	EPG A			Politique 2 Politique 4
	EPG B	Politique 1		
	EPG N		Politique 3	

Les politiques se composent de filtres de qualité de service, de contrôle des accès, d'insertion de services, etc. Les filtres sont des règles spécifiques définissant la politique entre deux groupes. Ils se composent de règles entrantes et sortantes (autoriser, refuser, rediriger, enregistrer, copier et marquer). Il est possible d'utiliser des fonctions utilisant des caractères génériques dans les définitions des politiques (figure 5). Pour l'application des politiques, la correspondance la plus spécifique est généralement prioritaire.

**Figure 5.** Règles d'application des caractères génériques

EPG source	EPG de dest.	Application	Commentaires
Complet	Complet	Complet	Règles (S,D,A) complètes
Complet	Complet	*	Règles (S, D, *)
Complet	*	Complet	Règles (S, *, A)
*	Complet	Complet	Règles (*, D, A)
Complet	*	*	Règles (S, *, *)
*	Complet	*	Règles (*, D, *)
*	*	Complet	Règles (*, *, A)
*	*	*	Par défaut (refus implicite...)

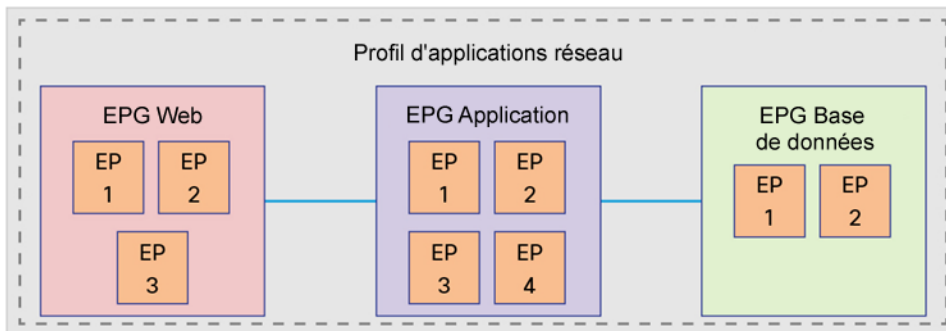


### Profils d'applications réseau

Un profil d'applications réseau englobe un ensemble de groupes de terminaux, leurs connexions et les politiques qui définissent ces dernières. Il correspond à la représentation logique d'une application et de ses interdépendances dans le fabric de réseau.

Les profils d'applications réseau sont conçus pour être modélisés d'une manière logique qui correspond au mode de conception et de déploiement des applications. La configuration et l'application des politiques et de la connectivité sont gérées par le système plutôt que manuellement par un administrateur. La figure 6 montre un exemple de profil d'accès.

**Figure 6.** Profils d'applications réseau



Voici les étapes générales requises pour créer un profil d'applications réseau :

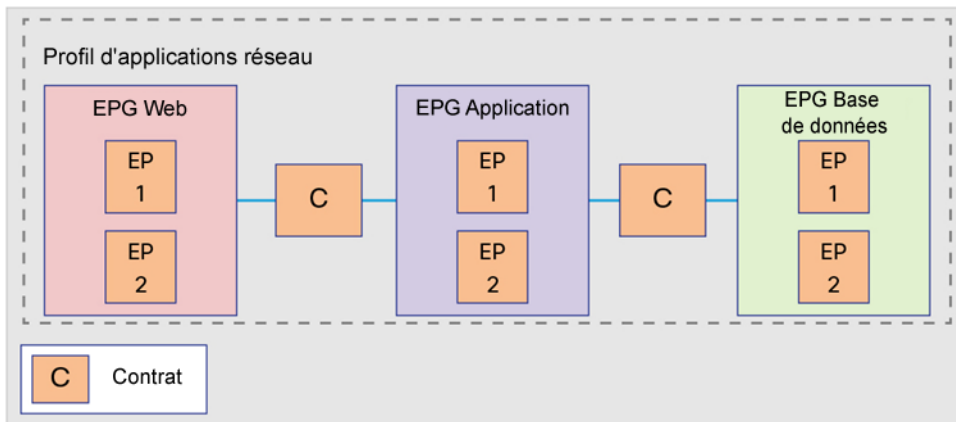
1. Créer des groupes de terminaux (voir précédemment).
2. Créer des politiques qui définissent la connectivité au moyen des règles suivantes :
  - Autoriser
  - Refuser
  - Enregistrer
  - Marquer
  - Rediriger
  - Copier
3. Créer des points de connexion entre les groupes en utilisant des composants de politique appelés « contrats ».

## Contrats

Les contrats définissent des autorisations ou des refus entre entrants et sortants, ainsi que des règles de qualité de service et des politiques (redirections...). Ils permettent de définir le mode de communication d'un groupe de terminaux avec d'autres groupes selon un degré de complexité adapté aux exigences de l'environnement. Bien que les contrats soient appliqués entre les groupes de terminaux, ils sont connectés à ces derniers par le biais de relations de type fournisseur–consommateur. En substance, un groupe de terminaux fournit un contrat que d'autres groupes consomment.

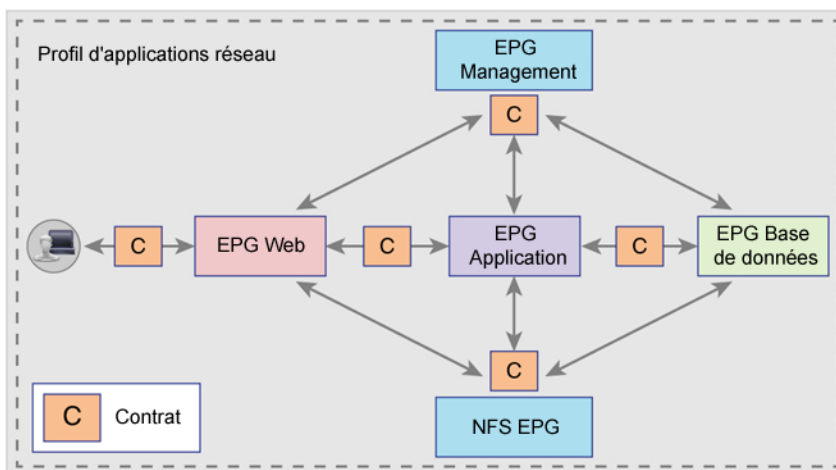
Le modèle fournisseur–consommateur est utile dans de nombreuses applications. Il offre un moyen naturel d'associer un « bouclier » ou une « membrane » à un niveau d'application qui dicte l'interaction de ce niveau avec les autres. Par exemple, si un serveur web fournit des services HTTP et HTTPS, il peut être intégré dans un contrat qui n'autorise que ces derniers. Le modèle fournisseur–consommateur a également pour effet de renforcer la sécurité, en autorisant l'application homogène et simple de mises à jour de politiques à un seul objet plutôt qu'aux multiples liens qu'un contrat peut représenter. Les contrats sont aussi synonymes de simplicité, car ils permettent d'utiliser à plusieurs reprises des politiques définies une seule fois (figure 7).

Figure 7. Contrats



La figure 8 montre la relation entre les trois niveaux d'une application web, la connectivité des groupes de terminaux et les contrats qui définissent leur communication. La somme de tous ces composants forme un profil d'applications réseau. Les contrats sont également réutilisables et assurent la cohérence des politiques pour les services qui communiquent avec plusieurs groupes de terminaux.

Figure 8. Profil complet d'applications réseau



## Conclusion

Ce document entend présenter une vue d'ensemble du modèle de politique d'une ACI et décrire sa nature et l'utilisation de son modèle de politique. Ce modèle intègre plusieurs autres éléments de construction et des objets qui ne sont pas abordés ici pour des raisons de simplicité.

## Informations complémentaires

Veuillez consulter la page <http://www.cisco.com/go/aci>.




---

**Siège social aux États-Unis**  
Cisco Systems, Inc.  
San Jose. CA

**Siège social en Asie-Pacifique**  
Cisco Systems (États-Unis) Pte. Ltd.  
Singapour

**Siège social en Europe**  
Cisco Systems International BV Amsterdam.  
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco, à l'adresse : [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, visitez le site : [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Les autres marques mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat commercial entre Cisco et d'autres entreprises. (1110R)