aruba
a Hewlett Packard Enterprise company

Conception de centre de données ESP

Guide de solution validé

Solution Aruba TME

20 mai 2022

Table des matières

Conception de centre de données ESP

Ce guide est destiné à aider un professionnel de l'informatique à comprendre les considérations de conception suivantes pour un environnement de centre de données :

- Sélection du matériel
- Sélection de logiciels
- Topologie •

Haute disponibilité •

Évolutivité •

Performance des applications •

Sécurité

NOTE:

Pour obtenir les informations les plus récentes sur les solutions ESP Data Center, veuillez consulter les sites suivants :

Programme de guide de solutions validées

Introduction

Le centre de données Aruba ESP (Edge Services Platform) repose sur une technologie qui fournit des outils permettant de transformer le centre de données en une plate-forme de prestation de services moderne et agile qui répond aux exigences des organisations, grandes, petites, distribuées et centralisées. Le système d'exploitation ArubaOS-CX (AOS-CX) simplifie les opérations et la maintenance grâce à un système d'exploitation de commutation commun sur le campus, la succursale et le centre de données, géré depuis le cloud ou sur site et soutenu par l'intelligence artificielle (IA) qui fournit les meilleures pratiques. un accompagnement tout au long du cycle de vie du réseau.

L'Ethernet convergé change la façon dont les hôtes de calcul accèdent au stockage des centres de données modernes. Les réseaux de stockage dédiés (SAN) ne sont plus nécessaires. Les protocoles Ethernet sans perte et de gestion de la bande passante garantissent des lectures et des écritures rapides sur un réseau local IP traditionnel. Les économies de coûts et la simplicité opérationnelle de l'Ethernet convergé sont des moteurs majeurs de transformation.

Dans le même temps, les topologies de réseau se sont virtualisées. Bien que cette virtualisation favorise la flexibilité requise pour répondre aux exigences transformationnelles des centres de données, elle peut ajouter de la complexité à la mise en œuvre et à la gestion. Le centre de données Aruba ESP atténue ces défis grâce à l'automatisation du plan de gestion et aux capacités d'AOS-CX, telles que les sauvegardes de configuration automatisées et les alertes intégrées.

La sécurisation des applications et des hôtes dans un centre de données est essentielle au maintien de la disponibilité des applications, de l'intégrité des données et de la continuité des activités. De nouvelles menaces continuent d'apparaître autour des ransomwares, de l'exfiltration de données et du déni de service. L'application des politiques et de la sécurité implique de nombreux outils et est appliquée à de nombreux niveaux différents. Le nouveau commutateur Aruba série CX 10000 avec Pensando introduit un premier commutateur de centre de données à services distribués du secteur, capable d'exécuter des services de pare-feu en ligne à vitesse filaire dans le commutateur lui-même, en se concentrant sur le niveau élevé de trafic est-ouest typique dans un environnement de centre de données.

Lors de la conception d'un centre de données nouveau ou transformé, la première étape consiste à comprendre la stratégie d'applications cloud de l'organisation. Cela déterminera quelles applications resteront sur site et la bonne taille pour le centre de données. Lors de la création d'un nouveau centre de données destiné à croître et à s'adapter, prévoyez de mettre en œuvre une sous-couche colonne vertébrale prenant en charge les réseaux superposés définis par logiciel. Les plates-formes de commutation Aruba CX 10000, 83xx et 84xx offrent une suite de produits de premier ordre comprenant une variété de configurations de ports à haut débit et une modularité de système d'exploitation de pointe offrant des analyses en temps réel et des performances permanentes.

Objectif de ce guide

Ce guide couvre la conception du réseau du centre de données Aruba ESP, y compris les architectures de référence ainsi que le matériel et les logiciels associés. Il explique les exigences qui ont façonné la conception et les avantages qu'elle offre. Ce guide présente les solutions de centre de données Aruba qui prennent en charge les options pour les charges de travail distribuées et centralisées et fournit des recommandations de bonnes pratiques pour la conception d'une structure de centre de données spine-and-leaf de nouvelle génération utilisant VXLAN et BGP EVPN.

Ce guide suppose que le lecteur possède des connaissances équivalentes à celles d'un associé de commutation certifié Aruba.

Objectifs de conception

L'objectif global est de créer une conception hautement fiable et évolutive, facile à maintenir et à adapter aux besoins changeants de l'entreprise. Les composants de la solution sont limités à un ensemble spécifique de produits requis pour un fonctionnement et une maintenance optimaux. Les principales fonctionnalités abordées par le réseau de centres de données Aruba ESP comprennent :

• Mises à niveau sans temps d'arrêt • Débit élevé • Sécurité • Réseau de stockage convergé • Segmentation flexible • Intégration tierce

Ce guide peut être utilisé pour concevoir de nouveaux réseaux ou pour optimiser et mettre à niveau les réseaux existants. Il ne s'agit pas d'une discussion exhaustive de toutes les options, mais plutôt de présenter les conceptions, fonctionnalités et matériels généralement recommandés.

Public

Ce guide est destiné aux professionnels de l'informatique qui doivent concevoir un réseau de centre de données Aruba ESP. Ces professionnels de l'informatique peuvent remplir divers rôles :

• Ingénieurs système qui ont besoin d'un ensemble standard de procédures pour la mise en œuvre de solutions. • Chefs de projet qui créent des énoncés de travail pour les mises en œuvre Aruba. • Partenaires Aruba qui vendent des technologies ou créent de la documentation de mise en œuvre.

Cas d'utilisation client

Les réseaux de centres de données évoluent rapidement. Le défi le plus urgent consiste à maintenir la stabilité opérationnelle et la visibilité tout en plaçant en toute sécurité les ressources de calcul et de stockage là où elles servent le mieux aux utilisateurs. En outre, les équipes des centres de données sont invitées à prendre en charge le rythme rapide des environnements DevOps, notamment en se connectant directement à l'infrastructure de cloud public. Compte tenu de l'évolution rapide des exigences des centres de données, il est essentiel que les ingénieurs réseau et système disposent des outils dont ils ont besoin pour simplifier et automatiser les configurations d'infrastructure complexes.

Ce guide aborde les cas d'utilisation suivants :

• Conceptions de paiement en fonction de votre croissance qui prennent en charge l'élasticité des charges de travail du réseau et du calcul. • Facilité d'utilisation et agilité pour déployer et gérer rapidement les charges de travail à l'aide de l'orchestration du calcul, de l'hyperviseur et du réseau .

• Opérations améliorées avec une visibilité du centre de données depuis l'hôte de calcul jusqu'à l'infrastructure réseau • Mobilité, sécurité et multilocation des charges de travail à l'aide de technologies de superposition basées sur des normes • Automatisation et gestion de l'infrastructure réseau • Agrégation et prétraitement des données

Conception du réseau du centre de données Aruba ESP

Le centre de données Aruba Edge Services Platform (ESP) propose des conceptions flexibles et hautement fiables qui garantissent un accès efficace aux applications et aux données pour tous les utilisateurs autorisés tout en simplifiant les opérations et en accélérant la fourniture de services.

Le centre de données Aruba ESP comprend les fonctionnalités et capacités clés suivantes :

- Connectivité moderne : concevez des réseaux efficaces et évolutifs en utilisant toute la gamme de densités de ports. et options de vitesse disponibles dans les familles de commutateurs Aruba CX 8xxx et CX 10000.
- Automatisation : la configuration automatisée de la structure permet de créer des données hautes performances et évolutives. les réseaux centraux sont plus efficaces et moins sujets aux erreurs.
- Analyses : les analyses intégrées et dans le cloud garantissent que les alertes ne sont jamais manquées et que les pannes intermittentes sont diagnostiquées

rapidement. • Réseau de stockage : les protocoles avancés permettent un Ethernet sans perte avec réservation de bande passante et gestion de la congestion. •

Intégration de l'hôte : la visualisation du réseau virtuel fait partie de la topologie du réseau physique pour gestion de bout en bout.

La conception du réseau du centre de données Aruba ESP peut contenir un ou plusieurs des éléments suivants :

- Aruba Centre
- Compositeur de tissus Aruba
- Aruba Net
- Gestionnaire de politiques et de services

Pensando • Commutateurs Ethernet Aruba CX 10000 avec Pensando

- Commutateurs Ethernet Aruba CX 8xxx
- Commutateurs Ethernet Aruba CX 6xxx pour la gestion de réseau hors bande (OOB) • Intégration

d'Aruba dans les solutions HPE

Options de conception de réseau de centre de données Aruba ESP

Le centre de données Aruba ESP prend en charge les charges de travail centralisées et distribuées partout au sein d'une organisation . Chaque conception prend en charge le regroupement de liaisons montantes hôtes, offrant débit et résilience pour les charges de travail critiques. Les domaines de couche 2 peuvent être déployés de manière flexible pour répondre aux exigences des applications et à la mobilité des hôtes virtuels.

Les commutateurs Aruba CX fournissent une plate-forme robuste pour les services de couche 3 dans le centre de données. Lorsqu'il est déployé dans une topologie en forme de colonne vertébrale et de feuille, un réseau de centre de données de couche 3 élimine le besoin de protocoles d'évitement de boucles et est optimisé pour une capacité élevée et des performances à faible latence non sursouscrites.

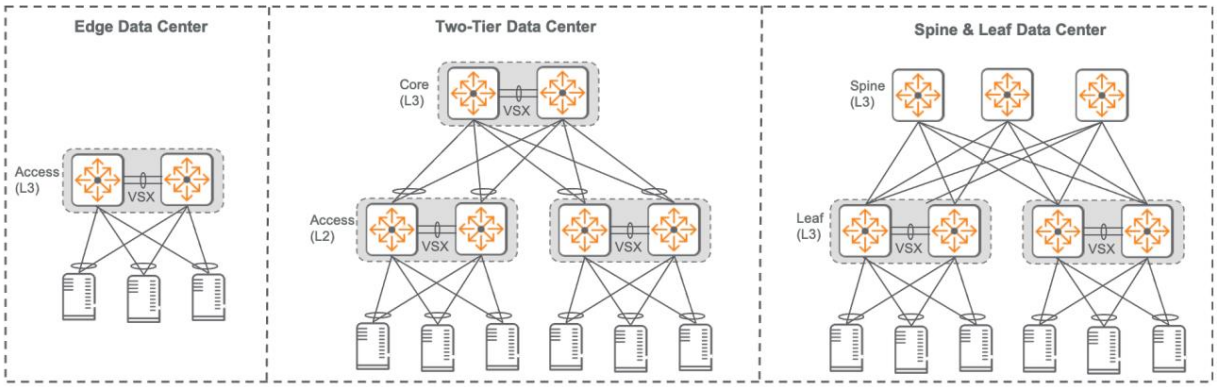

Figure 1 : Conceptions de centres de données Aruba

Présentation du centre de données Edge

Les entreprises qui ont migré la plupart de leurs charges de travail vers le cloud (et qui n'ont pas besoin d'un centre de données sur site) peuvent utiliser les armoires de câblage réseau de leur campus ou les petites salles de serveurs existantes pour déployer des charges de travail en périphérie. Cette conception utilise les mêmes commutateurs AOS-CX pour fournir un accès au serveur qui fournit déjà une connectivité filaire aux utilisateurs et aux appareils Internet des objets (IoT). Le centre de données Edge prend également en charge un accès à large bande passante et à faible latence aux ressources de calcul et de stockage pour les charges de travail distribuées qui peuvent ne pas être bien adaptées aux déploiements cloud.

Présentation du centre de données à deux niveaux

Les entreprises disposant d'importantes charges de travail sur site réparties sur plusieurs groupes de travail auront souvent besoin d'une conception de centre de données traditionnelle à deux niveaux. L'approche à deux niveaux garantit une bande passante et une fiabilité suffisantes à l'aide de protocoles existants tels que Link Aggregation Control Protocol (LACP), Spanning Tree Protocol (STP) et Open Shortest Path First (OSPF). Les hôtes sont hébergés en double sur des commutateurs haut de rack (ToR) à l'aide du groupe d'agrégation de liens (LAG) Virtual Switch Extension (VSX). Chaque commutateur ToR est doublement hébergé sur le noyau. Les boucles sont principalement évitées par l'utilisation de LACP pour regrouper les liaisons redondantes.

Présentation du centre de données Spine-and-Leaf

Entreprises dont les charges de travail sur site augmentent et celles dont les charges de travail sont réparties sur plusieurs centres de données devrait tirer parti de l'efficacité d'une architecture colonne vertébrale et feuille basée sur Clos. Dans la plupart des cas, une migration vers la conception « colonne vertébrale et feuille » doit être associée à la mise en œuvre d'un système virtuel extensible. Topologie de superposition LAN (VXLAN). La conception en forme de colonne vertébrale et de feuille garantit une grande fiabilité grâce à l'utilisation de Liaisons redondantes de couche 3 entre les nœuds feuilles et les commutateurs spine. Routage à trajets multiples à coût égal (ECMP) assure l'équilibrage de charge et un basculement rapide en cas de panne d'un lien ou d'un commutateur.

L'architecture entièrement maillée permet une croissance horizontale simple en ajoutant un autre commutateur de colonne vertébrale au besoin. VXLAN fournit une solution de tunneling de couche 2 sur couche 3, qui permet aux clients moderniser la sous-couche tout en préservant les exigences de service héritées en permettant une installation physique segments de couche 2 dispersés dans la superposition. VXLAN permet également des conceptions hautement segmentées, qui peuvent aller au-delà des VLAN traditionnels lors de la création de groupes de ressources sécurisés et discrets au sein du centre de données.

Ce guide aborde les cas d'utilisation les plus courants d'un réseau de centre de données Aruba spine-and-leaf. Pour Pour les projets plus complexes non couverts dans ce guide, contactez un SE d'Aruba ou un partenaire pour une vérification de la conception .

Architecture de centre de données Aruba ESP pour Spine and Leaf

Aruba ESP est une évolution de l'architecture de bout en bout d'Aruba, fournissant une infrastructure unifiée avec une gestion centralisée tirant parti des opérations d'intelligence artificielle (AIOps) pour une expérience opérationnelle améliorée qui contribue à mettre en œuvre une politique de sécurité Zero Trust. Aruba ESP est le premier du secteur plate-forme spécialement conçue pour les nouvelles exigences de l'Intelligent Edge.

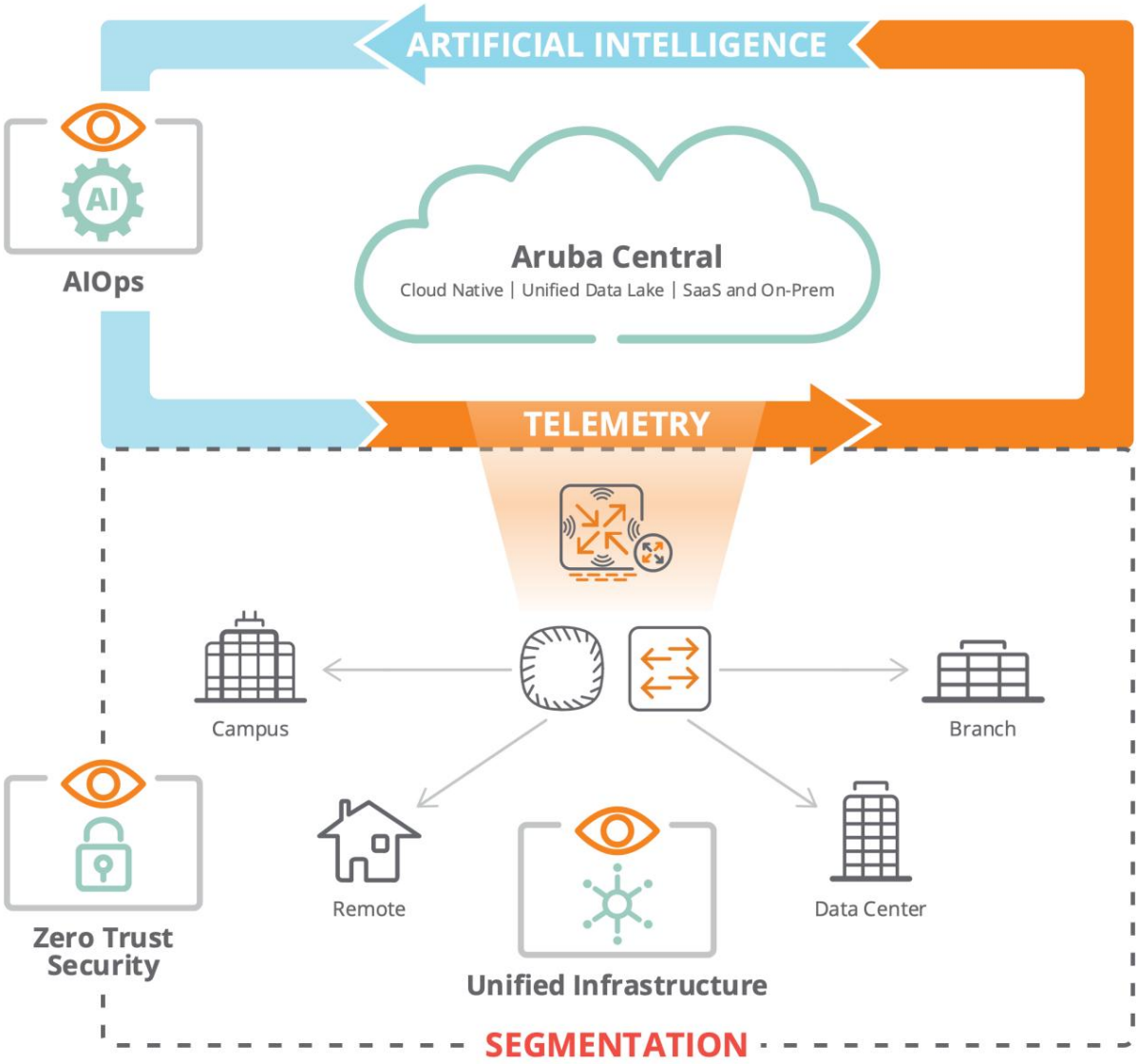

Figure 2 : Architecture ESP

Couches d'architecture Aruba ESP

Aruba ESP propose une large gamme de services, notamment l'intégration, le provisionnement, l'orchestration, la sécurité, l'analyse, le suivi de localisation et la gestion. AI Insights révèle les problèmes avant qu'ils n'affectent les utilisateurs. Une navigation intuitive centrée sur les flux de travail permet à l'organisation d'accomplir des tâches rapidement et facilement à l'aide de vues présentant plusieurs dimensions de données corrélées. Les politiques sont créées de manière centralisée et des fonctionnalités telles que la segmentation dynamique permettent à l'administrateur réseau de les mettre en œuvre sur une infrastructure existante. En effet, l'architecture Aruba ESP est construite en couches distinctes, comme le montre la figure suivante.

Figure 3 : Couches ESP

Couche de connectivité du centre de données Aruba ESP

La couche de connectivité du centre de données Aruba ESP est implémentée sur les commutateurs Ethernet Aruba CX 8xxx et 10000, qui offrent une faible latence et une bande passante élevée sur une plate-forme tolérante aux pannes conçue pour transporter le trafic du centre de données.

Réseau sous-jacent

Le réseau sous-jacent est implémenté à l'aide d'une topologie de tissu à colonne vertébrale et à feuilles. Il est déployé en tant que réseau routé de couche 3. Chaque feuille est connectée à chaque colonne via un port routé et OSPF est le protocole de routage. Les services de couche 2 ne sont pas requis dans la sous-couche mais peuvent être fournis pour les charges de travail utilisant des réseaux de superposition virtuels. La topologie sous-couche spine-and-leaf optimise les performances, augmente la disponibilité et réduit la latence, car chaque feuille ne représente jamais plus d'un saut sur plusieurs chemins à charge équilibrée vers tous les autres commutateurs feuilles.

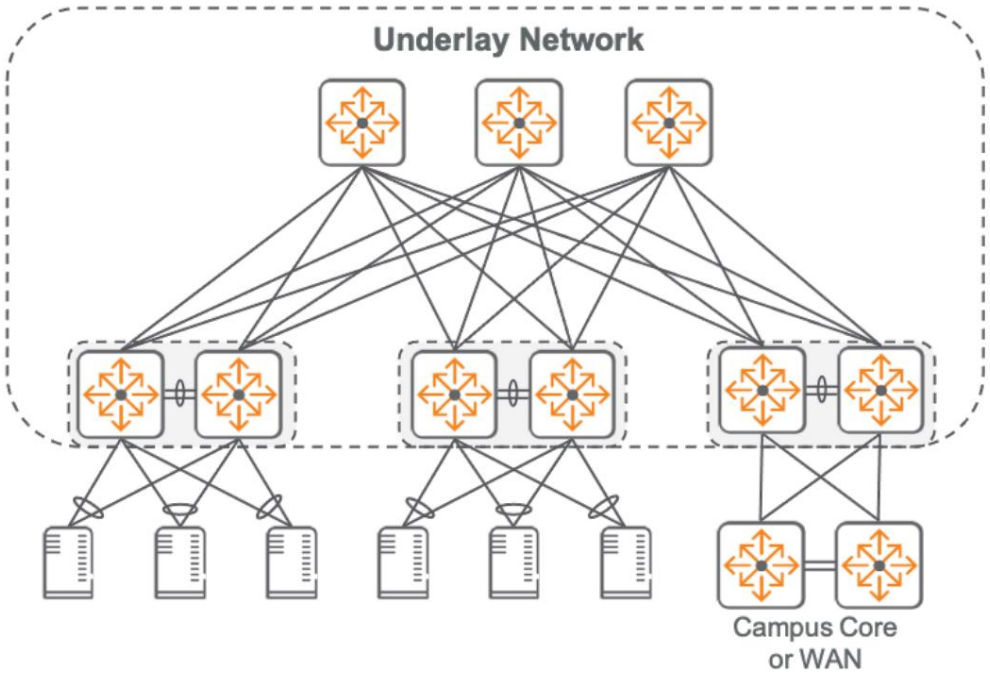

Figure 4 : Réseau sous-jacent

La topologie en forme de colonne vertébrale offre une conception de réseau flexible et évolutive qui peut s'étendre pour s'adapter à un centre de données en pleine croissance sans perturber le réseau existant. Il est facile de commencer avec une petite structure à un ou deux racks qui peut augmenter la capacité sans avoir à remplacer le matériel existant. Ports ToR activés
Les commutateurs feuilles sont utilisés pour ajouter progressivement de la capacité de calcul à un rack. Les ports des commutateurs spine sont utilisé pour ajouter des supports supplémentaires au tissu.

La taille maximale du tissu est déterminée par la densité des ports sur la colonne vertébrale, ce qui constitue un facteur important. considération pour soutenir la croissance future. Un minimum de deux commutateurs de colonne vertébrale est recommandé pour tout tissu de taille pour fournir une haute disponibilité et une tolérance aux pannes. Les commutateurs supplémentaires de la colonne vertébrale augmentent globalement capacité de la structure et réduire le domaine de pannes au cas où une colonne vertébrale devrait être mise hors service.

Couche de stratégie du centre de données Aruba ESP

La couche de stratégie du centre de données Aruba ESP est mise en œuvre par l'utilisation de technologies de superposition et mécanismes de filtrage du trafic pour isoler le trafic des utilisateurs et des applications.

Réseau superposé

Un réseau superposé est implémenté à l'aide de tunnels VXLAN qui fournissent des services réseau virtualisés de couche 2 et de couche 3 aux charges de travail directement connectées aux commutateurs feuilles. Semblable à un VLAN traditionnel ID, un identifiant de réseau VXLAN (VNI) identifie un segment de couche 2 isolé dans une topologie de superposition VXLAN.
Le routage et le pontage intégrés symétriques (IRB) permettent aux réseaux superposés de prendre en charge des réseaux contigus. Transfert de couche 2 et routage de couche 3 entre les nœuds feuilles.

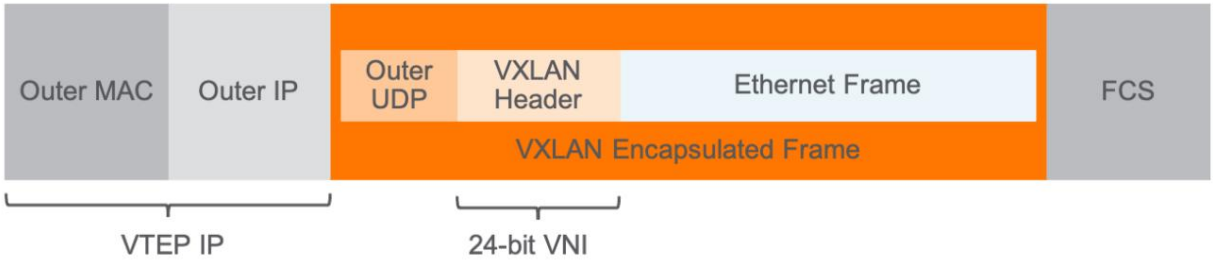

Figure 5 : Cadre VXLAN

Un point de terminaison de tunnel VXLAN (VTEP) est la fonction au sein des commutateurs feuilles qui gère l'origine et la terminaison des tunnels point à point formant un réseau superposé. Un seul VTEP logique est implémenté lorsque des commutateurs feuilles redondants sont déployés dans un rack. Les commutateurs Spine assurent le transport IP pour les tunnels de superposition mais ne participent pas à l'encapsulation/décapsulation du trafic VXLAN.

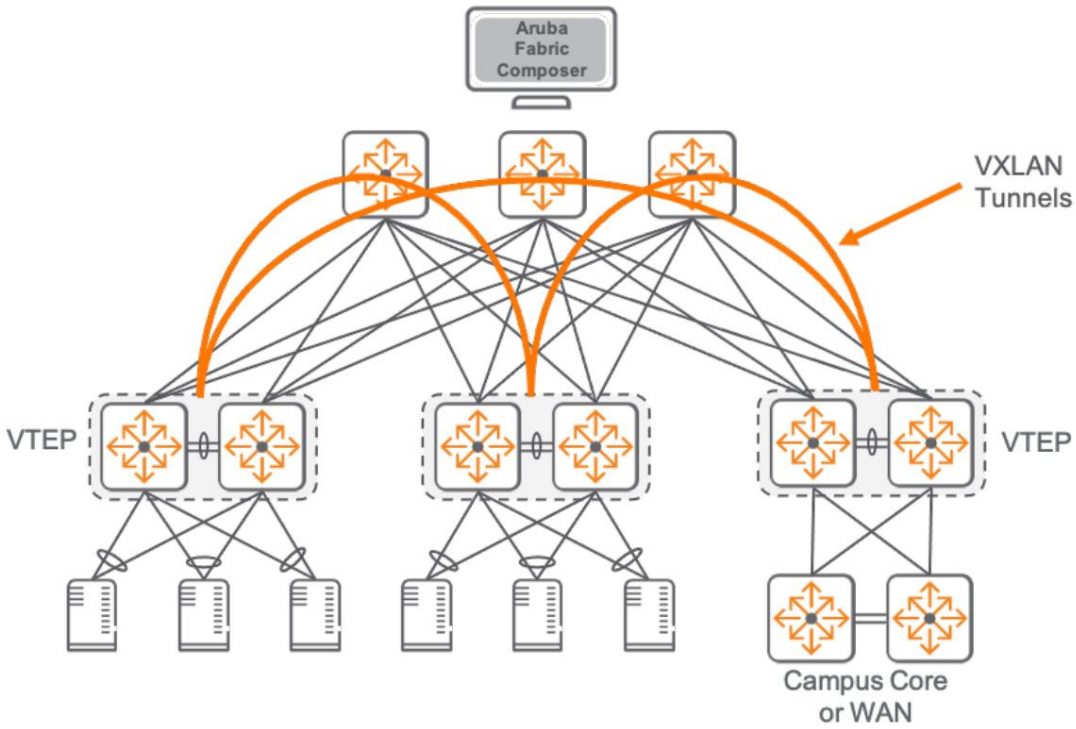

Figure 6 : Réseau superposé

Les hôtes connectés sont appris au niveau du commutateur feuille à l'aide des protocoles de couche de liaison Ethernet. L'apprentissage à distance à travers la structure VXLAN est réalisé à l'aide du protocole MP-BGP (Multiprotocol Border Gateway Protocol) comme protocole de plan de contrôle et d'une famille d'adresses de réseau privé virtuel (EVPN) Ethernet dédiée pour annoncer les préfixes IP et MAC de l'hôte. Cette approche minimise l'inondation tout en permettant une découverte efficace et dynamique des hôtes distants au sein de la structure.

Sécurité et segmentation

Dans une conception VXLAN à colonne vertébrale et feuille, une paire de commutateurs feuilles constitue le point d'entrée et de sortie unique du centre de données. Il n'est pas nécessaire que cette feuille de bordure soit dédiée à cette fonction. Des hôtes de calcul et des pare-feu peuvent également être connectés. En règle générale, la feuille frontière est l'endroit où un ensemble de politiques sont mises en œuvre pour contrôler l'accès au réseau du centre de données. Ces politiques constituent la première couche de sécurité pour les applications du centre de données. Ils limitent l'accès aux seuls réseaux et hôtes autorisés tout en surveillant également ces connexions. Le périmètre du centre de données est généralement protégé de l'une ou des deux manières suivantes :

- ACL de feuille de bordure : lorsque les sous-réseaux IP à l'intérieur du centre de données sont conçus de manière à correspondre à des groupes de sécurité ou à des fonctions commerciales, les listes de contrôle d'accès (ACL) au niveau de la feuille de bordure peuvent assurer l'application des politiques depuis les emplacements des utilisateurs jusqu'aux applications du centre de données. Si les sous-réseaux ne peuvent pas être mappés à des groupes de sécurité, les ACL peuvent devenir difficiles à gérer et à mettre à l'échelle dans des environnements plus vastes. Le principal avantage des ACL de périmètre est qu'elles peuvent être mises en œuvre directement sur l' infrastructure de commutation pour appliquer une base politique à partir de laquelle établir l'accès au centre de données. Les stratégies mises en œuvre à l'aide des ACL de commutateur ciblent spécifiquement les constructions de couche 3 et de couche 4. Les ACL de commutateur ne sont pas dynamiques ni sensibles aux applications.
- Pare-feux périmétriques : des systèmes de sécurité dédiés au périmètre peuvent offrir une surveillance avancée, une application des politiques prenant en compte les applications et une détection des menaces. Les pare-feu périmétriques sont généralement déployés en mode transparent ou routé. En mode transparent, les pare-feu se comportent comme une bosse dans le fil, ce qui signifie que tout le trafic de contrôle utilisateur et réseau autorisé les traverse de manière transparente. En mode routé, un pare-feu participera au plan de contrôle de routage et pourra être déployé dans une configuration limitant la quantité de trafic soumis à une inspection approfondie. Il est important de noter que les pare-feu avec état nécessitent un transfert symétrique pour appliquer correctement la stratégie au flux suivant.

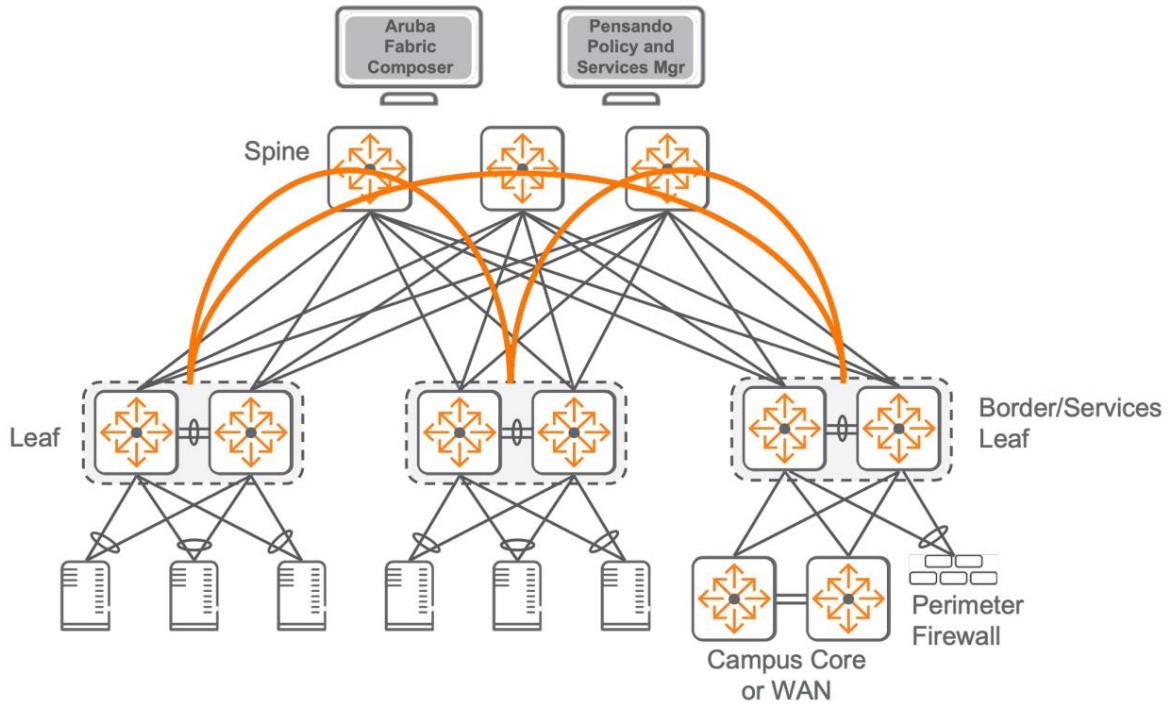

Figure 7 : Politique du centre de données

La politique au sein d'un centre de données VXLAN spine et leaf peut être mise en œuvre à l'aide de deux méthodes au niveau de la couche réseau : en ligne à l'aide de commutateurs de services distribués (DSS) ou de manière centralisée à l'aide d'un dispositif de pare-feu dans une feuille de services.

- Application des politiques de commutation de services distribués : l' unité de traitement de données programmable (DPU) Pensando étend les commutateurs Aruba série CX 10000 pour inclure des fonctionnalités de pare-feu dynamique. En tirant parti de cette fonctionnalité matérielle intégrée, l'application du pare-feu est assurée en ligne dans le cadre de la structure de commutation. Cette approche présente plusieurs avantages. La politique de pare-feu peut être granulaire pour l'hôte avec la prise en charge de la microsegmentation. Les hôtes du centre de données peuvent utiliser des passerelles locales, de sorte que les flux de trafic est-ouest sont optimisés entre les hôtes du centre de données. Il n'est pas nécessaire d'épingler les données via un pare-feu de feuille de services. Le Pensando DPU offre des performances filaires et peut réduire la consommation de ressources sur les services de pare-feu virtualisés traitant des flux de données volumineux en déplaçant les services de pare-feu vers un matériel de commutation dédié.

- Application des politiques de feuille de services : une autre approche d'application des politiques couramment déployée consiste à placer un dispositif de pare-feu dans une feuille de services. Les pare-feu connectés au niveau de la feuille des services sont utilisés comme passerelle par défaut pour les hôtes nécessitant des services spécifiques accessibles via le pare-feu. Un avantage de cette approche est la facilité avec laquelle un réseau superposé de couche 2 peut être utilisé pour transporter le trafic hôte vers le pare-feu. L'inconvénient est qu'il repose sur une passerelle centralisée et empêche l'utilisation d'une passerelle active à chaque ToR pour un transfert optimal. Semblable à une feuille de bordure, la feuille de services n'a pas besoin d'être dédiée à cette fonction.

Certains fournisseurs proposent des services de pare-feu virtualisés dans un environnement d'hyperviseur. Cette approche peut fournir une application granulaire des politiques au niveau du service tout en permettant également l'utilisation de passerelles actives. VMware NSX est un exemple de produit pouvant s'intégrer de cette manière. Les superpositions VXLAN peuvent être implémentées à la fois dans le matériel et dans les logiciels pour obtenir une virtualisation réseau optimale et des services de pare-feu distribués tout en sécurisant le trafic est-ouest à l'intérieur du centre de données.

Couche de services du centre de données Aruba ESP

Les solutions de centre de données Aruba ESP incluent des choix de plans de gestion permettant à une organisation d'appliquer l'approche la mieux adaptée à ses besoins.

- Aruba Central fournit une solution de gestion cloud pour la solution Aruba ESP de bout en bout. • Aruba Fabric Composer (AFC) est un outil d'automatisation de structure qui fournit un flux de travail simplifié.
  Une méthode basée sur la configuration de la structure est également proposée comme solution sur site.
- Aruba NetEdit fournit désormais le même éditeur de configuration multi-périphérique et le même mappeur de topologie.
  trouvé à Aruba Central dans une offre sur site.

Aruba Centre

Aruba Central est conçu pour simplifier le déploiement, la gestion et l'optimisation de l'infrastructure réseau. L'utilisation de l'apprentissage automatique (ML) intégré basé sur l'intelligence artificielle (IA) et de la gestion unifiée de l'infrastructure fournit une plate-forme globale pour la transformation numérique dans l' entreprise.

Aruba Central fournit des services avancés pour faciliter les déploiements transformationnels de centres de données. Grâce à la fonctionnalité NetEdit MultiEditor désormais intégrée à Central, il est possible de déployer des configurations complexes, multipériphériques et multicouches depuis le cloud vers votre centre de données. Le moteur Network Analytics fournit des alertes en temps réel sur l'état de vos commutateurs et permet une analyse rapide des problèmes intermittents. Aruba Central est hébergé dans le cloud pour plus d'élasticité et de résilience, ce qui signifie également que les utilisateurs n'ont jamais à se soucier de la maintenance du système ou des mises à jour des applications.

Les configurations basées sur les workflows dans Central permettent des déploiements efficaces et sans erreur des solutions Aruba partout dans le monde. Les flux de travail sont basés sur des approches de bonnes pratiques communes en matière de configuration réseau. Ils permettent de mettre rapidement en ligne de nouveaux appareils en utilisant des configurations réseau nouvelles ou existantes.

AIOps

Selon le glossaire Gartner, « L'AIOps combine le Big Data et l'apprentissage automatique pour automatiser les processus opérationnels informatiques, notamment la corrélation des événements, la détection des anomalies et la détermination de la causalité. »

Aruba AIOps, piloté par Aruba Central, élimine les tâches de dépannage manuelles, réduit le temps de résolution moyen et découvre automatiquement les optimisations du réseau. L'IA de nouvelle génération d'Aruba combine de manière unique des analyses centrées sur le réseau et l'utilisateur pour identifier et informer le personnel des anomalies. Il applique également des décennies d'expertise en matière de réseautage pour analyser et proposer des actions prescriptives.

AI Insights est disponible pour surveiller les performances de connectivité, la gestion des radiofréquences (RF), l'itinérance des clients, l'utilisation du temps d'antenne et les performances filaires et SD-WAN. Chaque information est conçue pour réduire les tickets d'incident et garantir les accords de niveau de service (SLA) en répondant aux défis de connectivité, de performances et de disponibilité du réseau.

AI Assist utilise l'automatisation basée sur les événements pour déclencher la collecte d'informations de dépannage, identifier les problèmes avant qu'ils n'affectent l'entreprise et éliminer pratiquement le processus fastidieux de collecte et d'analyse des fichiers journaux. Une fois les informations des journaux collectées automatiquement, le personnel informatique est alerté avec des journaux pertinents qui peuvent être consultés et même partagés avec Aruba TAC, qui peut aider plus rapidement à déterminer la cause première et à y remédier.

Compositeur de tissus d'Aruba

AFC fournit des fonctionnalités d'automatisation et d'orchestration basées sur des API pour le centre de données Aruba ESP. AFC découvre et interroge l'infrastructure du centre de données pour automatiser et accélérer le provisionnement de la structure spine-and-leaf ainsi que les opérations quotidiennes sur l'infrastructure de calcul et de stockage à l'échelle du rack.

AFC orchestre un ensemble de commutateurs comme une entité unique appelée structure et permet à l'opérateur d'orchestrer les ressources du centre de données en utilisant une approche centrée sur les applications pour visualiser l'infrastructure réseau et hôte.

La visualisation de la structure réseau du centre de données inclut les topologies de réseau physiques et virtuels ainsi que l'infrastructure hôte grâce à l'intégration avec ArubaOS-CX, HPE iLO Amplifier, HPE SimpliVity, VMware vSphere et d'autres produits leaders du centre de données. En plus de fournir une vue complète de l'ensemble de la structure, AFC rend le provisionnement du réseau accessible à bien plus que le simple personnel du réseau. Il fournit une plate-forme pour le déploiement orchestré des ressources hôte et réseau à travers la structure via une interface utilisateur de flux de travail guidée. AFC garantit une configuration cohérente et précise d'un centre de données en forme de colonne vertébrale, qu'un réseau superposé soit également déployé ou non.

AFC est un outil de gestion de réseau de centre de données de bout en bout recommandé pour les nouveaux déploiements de centres de données basés sur une topologie de structure spine-and-leaf. Cela s'avère particulièrement utile lors du déploiement d'une topologie de superposition à l'aide de VXLAN-EVPN. AFC configurera automatiquement le routage sous-couche et superposé à l'aide des informations IP de base fournies par l'opérateur.

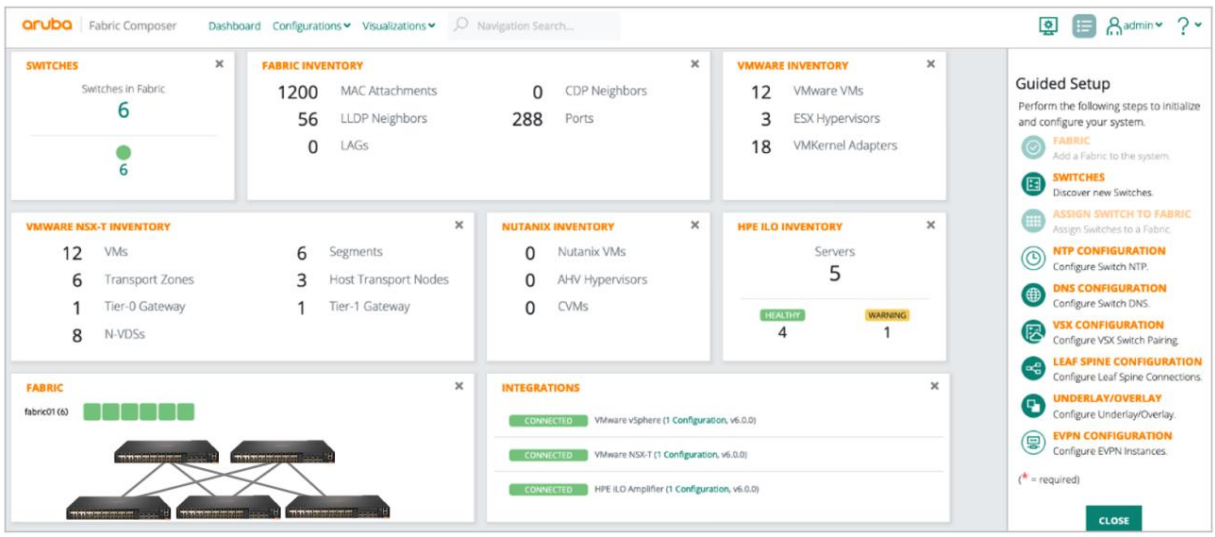

Figure 8 : Compositeur de tissu Aruba

Responsable des politiques et des services Pensando

Le Pensando Policy and Services Manager (PSM) fournit une plate-forme de gestion basée sur une API pour programmation et surveillance des DPU Pensando intégrés aux commutateurs Aruba CX 10000. AFC fournit une configuration et une orchestration à partir d'un seul panneau de verre pour la matrice de commutation et les systèmes gérés par PSM. services.

Aruba Net

Aruba NetEdit permet aux équipes informatiques d'automatiser la configuration de plusieurs commutateurs pour garantir que les déploiements sont cohérents, conformes et sans erreur. Il permet des flux de travail d'automatisation sans le surcharge de programmation en fournissant aux opérateurs une interface conviviale similaire à la commande doubler. NetEdit fournit également une vue dynamique de la topologie du réseau pour garantir une vue à jour de réseau.

Lors du déploiement d'un réseau de centre de données Aruba ESP à l'aide d'outils sur site, NetEdit doit être déployé pour une gestion détaillée de la configuration. Alors qu'Aruba Fabric Composer permet des implémentations rapides et sans erreurs , NetEdit offre la possibilité d'adapter cette configuration si nécessaire.
Ensemble, Fabric Composer et NetEdit offrent un réseau automatisé, intégré et validé configuration prête à répondre aux besoins de tout réseau de centre de données.

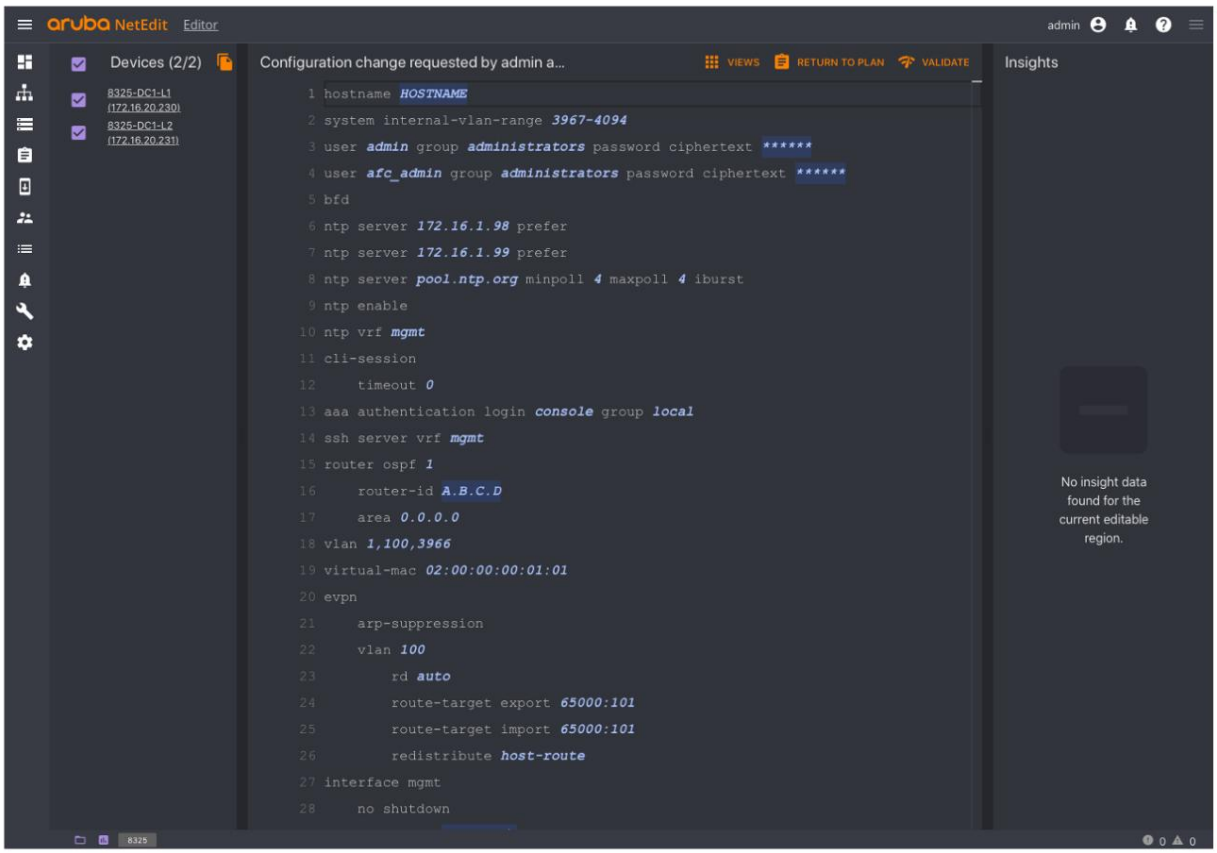

Figure 9 : NetEdit

Moteur d'analyse de réseau Aruba

Aruba Network Analytics Engine (NAE) fournit un cadre intégré pour la surveillance et le dépannage des réseaux. Il interroge et analyse automatiquement les événements du réseau pour offrir une visibilité sans précédent sur les pannes et les anomalies. Grâce à ces informations, le service informatique peut détecter les problèmes en temps réel et analyser les tendances pour prédire, voire éviter, les futurs problèmes de sécurité et de performances.

Une base de données de séries chronologiques intégrée fournit un historique des événements et des corrélations ainsi qu'un accès en temps réel à des informations à l'échelle du réseau pour aider les opérateurs à offrir de meilleures expériences. La surveillance en temps réel basée sur des règles et les notifications intelligentes sont automatiquement corrélées aux modifications de configuration. Les intégrations avec Aruba NetEdit et des outils tiers tels que ServiceNow et Slack offrent la possibilité de générer des alertes pour déclencher des actions au sein d'un processus de gestion de services informatiques.

NAE fonctionne dans le système d'exploitation AOS-CX dans les séries de commutateurs Aruba CX 6xxx, CX 8xxx et CX 10000. Les agents NAE testent les conditions sur le commutateur, ses appareils voisins ou sur le trafic traversant le réseau, puis prennent des mesures en fonction du résultat du test.

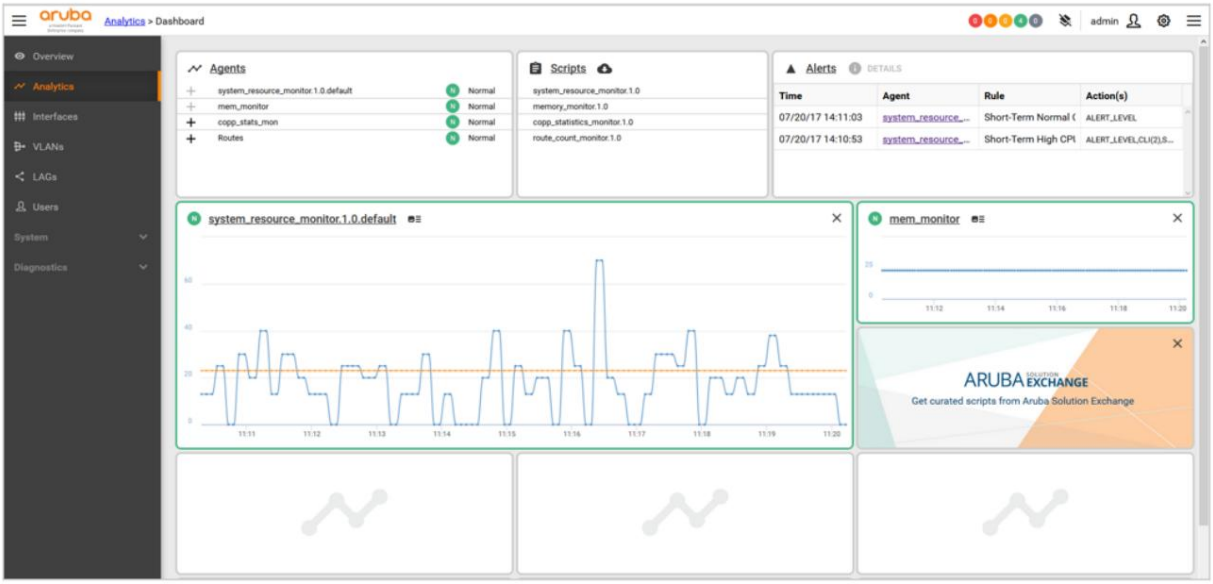

Figure 10 : Moteur d'analyse de réseau

Choisir une approche

En général, les petits centres de données connectés en périphérie sont mieux gérés à l'aide d'Aruba Central pour garantir une configuration cohérente partout dans le monde. Les centres de données plus grands et centralisés nécessiteront probablement l' utilisation d'Aruba NetEdit afin que des configurations détaillées et personnalisées puissent être écrites et déployées automatiquement sur plusieurs périphériques réseau.

Les plans visant à créer une topologie de centre de données en forme de colonne vertébrale et de feuilles devraient inclure l'AFC. Lors de la planification du déploiement d'une superposition VXLAN, AFC est fortement recommandé pour simplifier la configuration des services de sous-couche et de superposition ainsi que des segments de couche 3. Et lors du déploiement de PSM avec des commutateurs Aruba CX 10000, il est recommandé d'utiliser AFC pour gérer la création de règles et de politiques de pare-feu.

Services de centre de données supplémentaires

La planification d'un réseau de centre de données implique bien plus qu'une simple infrastructure réseau. Il est également nécessaire de garantir que les services sont disponibles pour mettre les commutateurs et les hôtes en ligne et que les appareils peuvent envoyer des messages de journal à un serveur Syslog accessible aux personnes et aux applications.

Il peut être utile d'exploiter les capacités Zero Touch Provisioning (ZTP) des commutateurs Aruba. Pour ce faire, le réseau doit fournir un serveur DHCP (Dynamic Host Configuration Protocol) sur un réseau local de gestion avec une route vers Internet. En plus de l'adresse de passerelle par défaut, les appareils auront également besoin d'au moins un serveur de service de nom de domaine (DNS) pour résoudre les noms d'hôte requis pour la connectivité à Aruba Central et au service Aruba Activate.

Network Time Protocol (NTP) garantit que les données des journaux provenant du réseau et du cloud sont correctement horodatées pour une analyse ultérieure. NTP est également requis pour que l'infrastructure à clé publique (PKI) fonctionne correctement. La PKI est aujourd'hui requise pour diverses approches de sécurité d'accès. Une solution de gestion des journaux ou de gestion des informations et des événements de sécurité (SIEM) fait aujourd'hui partie de la plupart des centres de données.

Savoir lequel sera implémenté aidera à établir une base de configuration pour tous les commutateurs du réseau.

Conception de centre de données Aruba ESP pour Spine and Leaf

Pour réussir la conception d'un centre de données en forme de colonne vertébrale, il est important de prendre en compte toutes les couches du réseau du centre de données. Cette section fournit des considérations générales sur la conception des différentes couches du centre de données Aruba ESP. La section Architecture de référence comprendra des recommandations spécifiques au matériel que vous pourrez utiliser pour finaliser votre conception.

Conception de la couche de connectivité

Cette section fournit des recommandations de conception et des bonnes pratiques pour la connectivité physique de l'infrastructure de calcul et de réseau.

Connectivité de l'hôte de calcul

La première étape de la conception d'un centre de données consiste à identifier les types de connectivité requis par les hôtes de calcul. Le matériel du serveur dispose généralement d'un port Ethernet RJ45 pour un périphérique de gestion des lumières telles que HPE iLO. La connectivité des applications s'effectue généralement via des liaisons redondantes utilisant des ports RJ45 ou SFP (Small Form Factor Pluggable).

Le port d'extinction est généralement connecté à l'aide d'un câble de raccordement en cuivre Cat5e ou Cat6 à un commutateur du réseau local de gestion. En règle générale, les connexions hôte-feuille seront de 10 Go ou 25 Go à l'aide de modules fibre SFP+/SFP28, de câbles en cuivre à connexion directe (DAC) ou de câbles optiques actifs (AOC). Les DAC ont une prise en charge de distance limitée et peuvent être plus difficiles à gérer en raison du calibre de fil plus épais par rapport aux câbles optiques. Les AOC prennent en charge des distances plus longues que les DAC, sont plus fins et plus faciles à gérer. Les DAC et les AOC coûtent moins cher que les câbles de raccordement à fibre optique et les émetteurs-récepteurs optiques séparés, mais ne fonctionnent qu'à une seule vitesse.

Il est important de vérifier que le contrôleur d'interface réseau (NIC) hôte et le commutateur ToR sont compatibles avec le même DAC ou AOC. Lorsque des émetteurs-récepteurs et des câbles optiques distincts sont utilisés, il est également important de vérifier la compatibilité de l'émetteur-récepteur avec la carte réseau hôte, le commutateur ToR et le type de câble optique. L'émetteur-récepteur pris en charge sur l'hôte sera généralement différent de l'émetteur-récepteur pris en charge sur le commutateur. Consultez toujours un professionnel du câblage structuré lors de la planification d'un système de données nouveau ou mis à niveau. centre.

Lors du déploiement d'un réseau convergé pour le trafic de stockage IP, recherchez les cartes NIC prenant en charge la charge de protocoles de stockage. De même, assurez-vous que le matériel prend également en charge le chargement VXLAN. Ces fonctionnalités contribueront à minimiser la latence du trafic de stockage en réduisant la charge sur un processeur hôte.

Les applications peuvent être hébergées directement sur un serveur à l'aide d'un seul système d'exploitation. C'est ce qu'on appelle communément un serveur nu. Plusieurs hôtes peuvent être virtualisés sur un seul serveur physique à l'aide d'une couche logicielle hyperviseur. Des exemples seraient VMware ESXi ou Microso Hyper-V.

Les hyperviseurs contiennent généralement une forme de commutateur virtuel qui fournit une connectivité à chaque machine virtuelle (VM) à l'aide de VLAN de couche 2 ou de tunnels VXLAN pour la segmentation. Une conception spine-and-leaf réussie doit prendre en charge la connectivité de couche 2 et de couche 3 à l'aide de ports non balisés et balisés VLAN pour correspondre à la connectivité requise pour le serveur et/ou le commutateur virtuel à l'intérieur du serveur. AFC offre une visibilité et une orchestration de la configuration requise pour garantir que la connectivité entre le serveur et les commutateurs Aruba ToR est correctement établie.

Gestion hors bande

La conception en forme de colonne vertébrale du centre de données Aruba ESP utilise un réseau local de gestion dédié se connectant aux ports de gestion des commutateurs et aux ports de gestion des lumières extérieures (LOM) de l'hôte. En règle générale, un seul commutateur de gestion est déployé sur chaque rack pour la gestion OOB. Un commutateur de gestion dédié garantit une connectivité fiable à l'infrastructure du centre de données pour l'automatisation, l'orchestration et l'accès à la gestion traditionnelle.

Conception haut de gamme

Le déploiement des commutateurs en position ToR permet des parcours de câbles plus courts entre les hôtes et les commutateurs. Le résultat est une solution plus modulaire avec un câblage hôte-commutateur contenu dans un boîtier rack et uniquement des liaisons montantes de commutateur sortant du boîtier. Cette approche permet de réduire la complexité lors de l'ajout de racks au centre de données.

Dans le centre de données Aruba ESP, chaque rack est desservi par une paire redondante de commutateurs configurés VSX. Cela permet aux hôtes à double hébergement d'être connectés à deux commutateurs physiques à l'aide d'un ensemble d'agrégation de liens pour une tolérance aux pannes et une bande passante accrue.

VSX permet une architecture distribuée et redondante hautement disponible lors des mises à niveau. Il virtualise le plan de contrôle de deux commutateurs pour fonctionner comme un seul périphérique au niveau de la couche 2 et comme des périphériques indépendants au niveau de la couche 3. Du point de vue du chemin de données, chaque périphérique effectue une recherche de transfert indépendante pour décider comment gérer le trafic. Certaines bases de données de transfert, telles que les tables MAC et ARP, sont synchronisées entre les deux appareils via le plan de contrôle VSX sur une liaison inter-commutateurs (ISL) dédiée. Chaque commutateur crée indépendamment les bases de données de transfert de couche 3.

Lors du déploiement d'une paire de commutateurs en mode VSX, assurez-vous qu'au moins trois ports connectent les commutateurs les uns aux autres. Au moins deux ports sont membres d'un chemin de données d'agrégation de liens entre la paire de commutateurs et doivent avoir la même vitesse que les ports de liaison montante. Un troisième peut être n'importe quel port disponible à vitesse inférieure pour préserver les liaisons montantes pour la future connectivité d'agrégation de liens VSX et Spine.

Pour une compatibilité ascendante et pour prendre en charge la croissance future, choisissez un commutateur ToR prenant en charge des taux de connectivité de 1, 10 ou 25 Gbit/s. Ces vitesses de connexion peuvent être mises en œuvre en utilisant les mêmes types de supports à fibre optique, ce qui facilite l'augmentation de la bande passante en mettant simplement à niveau les émetteurs-récepteurs ou les DAC/AOC. Gardez les points suivants à l'esprit lors de la sélection d'un commutateur ToR :

- Exigences des fonctionnalités DSS : Aruba CX 10000 est requis dans une conception de centre de données qui exploite l'inspection du pare-feu dynamique en ligne effectuée par l'ASIC Pensando Elba.
- Nombre et type de connexions au serveur : les configurations de serveur rack typiques prennent en charge 48 ports côté hôte, mais des options ToR de densité inférieure sont disponibles dans la série Aruba CX 8360.

- Vitesse de connectivité des hôtes : pour simplifier la gestion, consolidez les hôtes se connectant aux mêmes vitesses aux mêmes racks et commutateurs. L'adaptation des paramètres de vitesse du port d'une interface particulière entre 25 et 10 Go peut avoir un impact sur un groupe d'interfaces adjacentes. Tenez compte de la taille du groupe d'interfaces lors de la planification d'un rack nécessitant plusieurs vitesses de connexion. • Nombre de ports de liaison montante : les modèles de commutateurs ToR prennent en charge une gamme de densités de ports de liaison montante. Lors de l'utilisation de VSX pour la redondance, deux ports de liaison montante sont utilisés pour les ISL fournissant une redondance du chemin de données et ne peuvent pas être utilisés pour la connectivité spine.
- Connectivité ToR-to-Spine : le volume et la vitesse du port des liaisons montantes définiront le taux de surabonnement des hôtes vers la structure du centre de données. A titre d'exemple, dans un déploiement à quatre spines à 100 Go, une structure non sursouscrite peut être implémentée pour des racks de 40 serveurs connectés à 10 Go.
- Conception de refroidissement : différents modèles ToR sont disponibles pour le refroidissement port-alimentation et alimentation-port. Dans les configurations alimentation-port, un kit de conduits d'air en option peut isoler l'air chaud des serveurs à l'intérieur du rack. Le câblage peut absorber la chaleur et restreindre la circulation de l'air. Des chemins de câbles courts et une bonne gestion des câbles amélioreront l'efficacité du flux d'air.

Conception de la colonne vertébrale

La couche spine fournit l'agrégation pour les commutateurs feuilles. Dans une conception spine-and-leaf, chaque commutateur ToR est connecté à chaque commutateur spine. Chaque connexion feuille à colonne doit utiliser la même vitesse de liaison pour garantir plusieurs chemins de coût égal au sein de la structure. Cela permet au routage basé sur ECMP de garantir la connectivité en cas de panne d'une liaison.

La capacité des ports des commutateurs spine définira le nombre maximum de racks que le centre de données peut connecter. Dans le cas d'une conception ToR redondante, le nombre maximum de racks sera la moitié du nombre de ports sur le commutateur spine. Deux colonnes constituent le minimum recommandé pour une haute disponibilité. Des épines supplémentaires augmentent la capacité globale de la structure et réduisent la taille du domaine de pannes au cas où une épine serait hors de porté service.

- Déterminer les besoins en matière de support rack et de bande passante.
- Déterminez si des commutateurs ToR simples ou redondants seront installés. • Déterminez le nombre de racks nécessaires pour répondre aux besoins actuels en matière de calcul et de stockage. • Déterminez les commutateurs spine requis pour prendre en charge les racks prévus. • Concevez le réseau du centre de données pour une capacité ne dépassant pas 50 % afin de laisser de la place à la croissance.

Si le réseau dispose de plus de deux commutateurs spine, faites attention au nombre de ports de liaison montante disponibles sur le commutateur ToR choisi. Chaque commutateur ToR doit se connecter à chaque colonne vertébrale pour qu'ECMP fonctionne efficacement.

Lorsque vous décidez où placer vos commutateurs spine, tenez également compte de leur distance par rapport aux commutateurs feuilles et du type de support que vous utiliserez pour les connecter. Les connexions feuille à colonne seront constituées de fibre de 40 ou 100 Go utilisant des émetteurs-récepteurs quad SFP (QSFP) ou AOC, dans lesquels, à l'instar des DAC, le câble et l'émetteur-récepteur sont intégrés.

Conception IP sous-jacente

La sous-couche d'un réseau de centre de données spine-and-leaf est la couche qui fournit la connectivité IP entre les commutateurs spine-and-leaf. La sous-couche est la partie du réseau qui garantit que le trafic tunnelisé VXLAN (le réseau superposé) peut être transmis à travers la structure.

Le centre de données Aruba ESP utilise OSPF comme protocole de routage sous-jacent. OSPF est un protocole IGP (Interior Gateway Protocol) largement utilisé et bien compris qui offre une configuration simple et une convergence rapide. Une seule zone OSPF et des interfaces point à point sont recommandées pour minimiser la complexité et le temps requis pour établir des contiguïtés voisines.

Configurez les commutateurs du centre de données pour une unité de transmission maximale (MTU) géante de 9 198 octets. Cela prend en charge les protocoles de stockage susceptibles d'être déployés et l'en-tête de trame étendu utilisé par VXLAN.

Conception de la couche de politique

Cette section fournit des recommandations de conception et des bonnes pratiques pour la conception de la couche de stratégie du réseau du centre de données.

Réseau de gestion

Les organisations doivent prévoir de créer un réseau local de gestion physiquement séparé et un contrôle d'accès basé sur les rôles sur les périphériques réseau. Cela signifie que la connexion à un commutateur nécessite une authentification auprès d'un annuaire d'entreprise. Cela serait généralement accompli à l'aide du protocole TACACS+ et d'un serveur de politiques tel qu'Aruba ClearPass Policy Manager. Installations de journalisation, gestion des journaux et analyse des journaux devrait également être envisagée.

L'établissement d'un réseau de gestion distinct garantit que l'accessibilité des commutateurs du centre de données n'est pas involontairement bloquée lors de la modification de la politique du plan de données.

Objectif de la politique et de la segmentation

La politique de sécurité joue un rôle clé en réduisant la surface d'attaque exposée par les hôtes du centre de données, en limitant les options de déplacement latéral des menaces une fois qu'un hôte a été compromis et en empêchant l'exfiltration de données. Le blocage des protocoles inutiles limite les tactiques disponibles qu'un acteur malveillant peut utiliser pour exploiter l'hôte, qui peuvent être appliquées au trafic nord-sud et est-ouest des centres de données. La portée autorisée du trafic sortant inhibe les structures de commandement et de contrôle et bloque les méthodes courantes de data exfiltration.

Conception du plan de contrôle de superposition

La mobilité des hôtes fait référence à la possibilité de déplacer des hôtes physiques ou virtuels au sein d'un réseau de centre de données sans modifier la configuration du réseau hôte. Cette flexibilité est puissante lorsqu'elle est associée à des hôtes virtualisés et peut garantir des ressources de calcul optimisées, une haute disponibilité des applications et une connectivité efficace pour les charges de travail distribuées.

Pour maintenir une superposition de centre de données et transmettre avec succès le trafic à travers celle-ci, les VTEP au sein de la structure nécessitent des informations d'accessibilité sur les points de terminaison connectés à la structure. Un plan de contrôle distribué et dynamique est recommandé pour les raisons suivantes :

- Les techniques traditionnelles d'inondation et d'apprentissage peuvent consommer de grandes quantités de bande passante en raison de la réplication du traic dans un grand environnement de colonne vertébrale et de feuille.
- La configuration du réseau est simplifiée car les commutateurs ToR apprendront automatiquement les autres ToR. interrupteurs à l'intérieur du tissu.
- Un plan de contrôle distribué fournit une redondance et un état topologique cohérent sur l'ensemble des commutateurs de structure du centre de données.
- Un plan de contrôle distribué permet un transfert optimal via l'utilisation de passerelles distribuées au niveau des commutateurs ToR. Cela permet à l'adresse de passerelle par défaut de rester la même dans toute la structure.

L'utilisation de MP-BGP avec les familles d'adresses EVPN entre les VTEP fournit un plan de contrôle basé sur des normes et hautement évolutif pour le partage des informations d'accessibilité des points de terminaison avec une prise en charge native de la multi- location. MP-BGP est utilisé depuis de nombreuses années par les fournisseurs de services pour offrir des services VPN sécurisés de couche 2 et de couche 3 à très grande échelle. Les opérations réseau sont simplifiées grâce à l'utilisation d'une conception iBGP avec des réflecteurs de route afin que le peering ne soit requis qu'entre les commutateurs feuilles et la colonne vertébrale. Certaines des constructions du plan de contrôle BGP que vous devriez connaître sont les suivantes :

- Virtual Routing & Forwarding (VRF) : un VRF est une instance de routage virtualisée de couche 3, qui se compose d'une table de routage unique, d'interfaces membres qui transfèrent le trafic en fonction de la table de routage et de protocoles de routage qui construisent la table de routage. Un VRF peut contenir des adresses IP qui se chevauchent avec un autre VRF, car les tables de routage individuelles sont discrètes.

- Distinguateur de route (RD) : afin de prendre en charge la multilocation et la probabilité de chevauchement des adressages IP, une valeur RD est ajoutée au préfixe IPv4 ou IPv6 lors de l'exportation vers BGP à partir d'un VRF. La valeur combinée du préfixe RD + IPv4/IPv6 crée un nouveau préfixe unique qui permet à une seule famille d'adresses BGP de transporter des préfixes IPv4/IPv6 qui se chevaucheraient autrement. Le RD doit être unique pour chaque VRF, qui est mappé à un VNID VXLAN Layer 3.

- Cible de route (RT) : les cibles de route sont utilisées comme attribut pour identifier le réseau VRF associé à un préfixe lors de l'exportation et comme critère d'importation de préfixes dans une table de routage VRF. Les cibles de route de la famille d'adresses IPv4 sont utilisées pour effectuer une fuite de route entre les VRF en important des préfixes avec des cibles de route exportées par d'autres VRF. • Réflecteur de route (RR) : pour optimiser le processus de partage des informations d'accessibilité
entre les VTEP, l'utilisation de réflecteurs de route au niveau de la colonne vertébrale permet un peering iBGP simplifié. Cette conception permet à tous les VTEP d'avoir la même configuration de peering iBGP et élimine le besoin d'un maillage complet de voisins iBGP.

- Famille d'adresses (AF) : différents types de tables de routage (tels que la monodiffusion IPv4, la monodiffusion IPv6 et le VPN de couche 3) sont pris en charge dans MP-BGP. La famille d'adresses VPN de couche 2 (AFI=25) et la famille d'adresses EVPN (SAFI=70) sont utilisées pour annoncer les informations d'adresse IP et MAC entre les haut-parleurs BGP . La table de routage de la famille d'adresses EVPN contient des informations d'accessibilité pour l'établissement de tunnels VXLAN entre les VTEP.

La conception du centre de données Aruba ESP utilise deux commutateurs de couche vertébrale comme réflecteurs de route iBGP. Le nombre de préfixes de destination et de réseaux superposés consomme des ressources physiques sous forme de tables de transfert et doit être pris en compte lors de la conception du réseau. La section Architecture de référence fournit des directives matérielles pour faire évoluer la conception du réseau du centre de données.

Conditions préalables à la politique de segmentation

Les applications de centre de données sont déployées de différentes manières. Les applications peuvent être implémentées sous forme de machines virtuelles à l'aide d'hyperviseurs ou hébergées sur des serveurs nus. Les applications conteneurisées sont hautement distribuées et nécessitent généralement une connectivité entre plusieurs nœuds de calcul et de service. Dans certains cas, un seul centre de données hébergera des applications pour plusieurs locataires tout en offrant un ensemble de services partagés entre eux. En raison de la manière dont les applications sont déployées dans un centre de données moderne (avec la majorité du trafic contenu dans le centre de données), il serait incorrect de supposer que toutes les menaces de sécurité sont externes.

Une conception réussie d'une politique de centre de données commence par la compréhension des exigences des applications qui s'exécuteront dans l'environnement. Il est souvent nécessaire de reprofiler les applications existantes lorsqu'il n'existe pas de documentation suffisante sur les exigences. Du point de vue du réseau, le profilage des applications doit documenter toutes les connexions réseau requises pour que cette application s'exécute correctement. Il peut s'agir de bases de données back-end ou de services hébergés dans le cloud. Pour définir correctement la politique concernant les connexions qui doivent être autorisées et celles qui seront refusées, il est d'abord nécessaire de connaître le profil de l'application.

De même, un profil des utilisateurs accédant aux applications et aux données est généralement requis. Ne laissez jamais un centre de données grand ouvert sur un campus, même s'il est supposé être un environnement sécurisé. Pour restreindre l'accès, comprenez les différents profils d'utilisateurs associés aux applications et aux données requises. Il est important d'identifier les exigences des campus, des succursales distantes, des travailleurs mobiles sur le terrain et de l'Internet public afin que des profils d'accès aux centres de données appropriés puissent être développés pour représenter leurs besoins uniques.

Segmentation du domaine de routage virtuel

La meilleure pratique courante consiste à utiliser le nombre minimum de VRF requis pour atteindre des objectifs organisationnels clairement définis, car chaque VRF supplémentaire augmente la complexité d'un réseau. Les VRF sont utilisés pour prendre en charge les cas d'utilisation suivants :

- Environnements d'applications de production et de développement séparés. Cela fournit un bac à sable de développement tout en minimisant les risques liés à la disponibilité des applications de production, et prend en charge le chevauchement de l' espace IP lorsque cela

est nécessaire. • Appliquez une politique au trafic segmenté exigeant une conformité réglementaire stricte, telle que PCI ou HIPAA. • Appliquer une politique au trafic segmenté provenant d'hôtes identifiés par la politique de l'organisation comme nécessitant une segmentation et possédant un ensemble commun d'exigences de sécurité. Ces ensembles d'hôtes partagent souvent un domaine administratif commun.

- Isoler l'accessibilité des routes de couche 3 dans un centre de données multi-tenant, tout en prenant en charge le chevauchement des adresses IP. espace.

Les itinéraires des centres de données devront probablement être partagés avec les segments du réseau du campus. Une méthode consiste à effectuer un peering VRF du centre de données avec l'instance de routage principale du campus. La segmentation au sein du campus peut être réalisée à l'aide d'un hando VRF-lite, où un peering direct VRF à VRF est effectué entre un VRF frontalier du centre de données et son voisin VRF du campus.

Le transfert de route inter-VRF (IVRF) peut être utilisé au sein d'un centre de données pour partager des préfixes IP entre les VRF. Par exemple, pour fournir des services partagés dans un centre de données, un VRF de services peut être créé pour offrir un ensemble commun de ressources et l'IVRF permet l'accessibilité entre l'application et les VRF de services.

Segmentation VLAN

En plus de limiter la taille du domaine de diffusion, un VLAN et son sous-réseau IP associé sont utilisés pour regrouper des ensembles d'hôtes de centre de données par rôle, application et domaine administratif.

Les VLAN membres du même VRF ont une accessibilité de couche 3 entre les sous-réseaux. Ces limites de couche 3 deviennent alors un point clé de l'application des politiques. Les ACL VLAN sont généralement utilisées pour appliquer une stratégie de base entre les sous-réseaux d'un VRF. Lorsque des exigences politiques plus sophistiquées surviennent, la solution courante consiste à déployer un pare-feu centralisé et à en faire la passerelle par défaut pour les sous-réseaux d'applications. Cela se traduit généralement par des schémas de circulation sous-optimaux et inefficaces. Le centre de données Aruba ESP offre la possibilité de déployer des commutateurs CX 10000 ToR qui offrent des capacités de pare-feu de couche 4 basées sur le matériel au niveau du commutateur de liaison montante de l'hôte, réduisant ainsi le besoin de suivre le trafic en épingle.

Microsegmentation

La microsegmentation étend l'application des politiques jusqu'au niveau de la charge de travail individuelle et de l'hôte réseau. Le commutateur Aruba série CX 10000 offre une stratégie de microsegmentation complète et cohérente qui peut être appliquée à un large éventail d'hôtes de centres de données. Semblable à un pare-feu basé sur un hyperviseur, le CX 10000 offre la possibilité de segmenter entre les invités de VM sur le même hôte de VM à l'aide d'un mécanisme de VLAN privé (PVLAN). Le CX 10000 fournit une stratégie unique de microsegmentation des centres de données prenant en charge tous les types d'hyperviseurs (VMware, Microso Hyper-V, KVM, etc.) et les serveurs nus. L'utilisation du CX 10000 à la place d'une implémentation basée sur un hyperviseur charge les cycles d'application des politiques depuis le processeur hôte d'une machine virtuelle vers le matériel de commutation dédié.

La microsegmentation peut être appliquée à un sous-ensemble d'hôtes nécessitant un niveau de surveillance élevé, ou elle peut être appliquée plus largement pour maximiser la sécurité d'un centre de données.

Utilisation de la politique Aruba CX 10000

L'Aruba CX 10000 avec Pensando fournit un puissant moteur d'application des politiques. Cette section fournit des informations générales et des détails sur la manière de mettre en œuvre la stratégie de pare-feu CX 10000.

Environnements CX 10000

L'application d'une politique cohérente basée sur PSM dans une structure de centre de données est plus facile à réaliser lorsque tous les commutateurs feuilles sont des CX 10000. Un environnement mixte de commutateurs compatibles DSS et non DSS est pris en charge, cependant, les administrateurs doivent garder à l'esprit ces considérations :

- Les machines virtuelles et les hôtes nus nécessitant une politique de pare-feu doivent être câblés aux commutateurs CX 10000. • Des procédures doivent être créées pour empêcher la migration automatique et manuelle d'invité de VM depuis un hôte de VM connecté au CX 10000 vers un hôte de VM connecté à un commutateur non DSS, lorsque l'invité de VM nécessite l'application d'une stratégie basée sur DSS.
- Un ensemble combiné de politiques de sortie et d'entrée doit souvent être créé pour atteindre des objectifs définis. objectifs de sécurité.

Implications sur la mobilité des hôtes

La mobilité omniprésente des hôtes au sein d'une structure nécessite que tous les commutateurs feuilles prennent en charge les mêmes fonctionnalités. Les politiques de sécurité du pare-feu avec état prises en charge sur un commutateur DSS ne sont pas disponibles sur les commutateurs non DSS. La mobilité des machines virtuelles doit être limitée en conséquence. Par exemple, lors de l'utilisation d'outils dynamiques tels que le planificateur de ressources distribuées (DRS) de VMware , il faut veiller à ce que les ressources du commutateur virtuel et du groupe de ports soient définies pour empêcher le déplacement automatisé d'un invité de machine virtuelle nécessitant des services de pare-feu vers un hôte de machine virtuelle qui n'est pas activé. connecté à un commutateur DSS.

Réseaux MSP et principes de base des politiques

PSM associe un objet Réseau à un VLAN configuré sur un commutateur CX 10000. La définition d'un réseau indique au commutateur de transférer le trafic routé associé au VLAN vers le pare-feu basé sur DSM pour

Application des politiques de couche 4.

La politique de pare-feu PSM est un ensemble de règles qui spécifient les adresses source et de destination, ainsi que le type de trafic autorisé à l'aide du protocole IP et du numéro de port. La stratégie est appliquée à un réseau dans le sens de sortie ou d'entrée . La direction est du point de vue de l'hôte connecté. Le trafic provenant de l'hôte est considéré comme une sortie, et le trafic destiné à l'hôte est considéré comme une entrée.

Une règle d'entrée est appliquée au trafic acheminé vers le CX 10000 à partir d'autres commutateurs du réseau. Une stratégie d'entrée ne peut pas être appliquée entre deux hôtes connectés au même commutateur Aruba CX 10000. Lors de l'utilisation d'une superposition de structure EVPN, la stratégie est appliquée au trafic arrivant des hôtes qui sont adjacents à la couche 2 dans la superposition de structure, mais résident sur des commutateurs discrets au sein de la structure. La stratégie d'entrée ne s'applique pas au trafic de couche 2 qui est ponté via une liaison de couche 2 à partir d'un commutateur adjacent.

Le trafic de sortie acheminé est toujours transmis au DSM pour l'application de la politique, lorsqu'une politique est appliquée à un réseau. Une politique de sortie est requise pour filtrer le trafic entre les hôtes connectés au même commutateur CX 10000.

Le trafic ponté de couche 2 n'est pas inspecté par le DSM, à l'exception du trafic de couche 2 transmis à un autre commutateur de structure dans une superposition de structure EVPN.

Dans un environnement CX 10000 uniquement, un ensemble de politiques de sortie peut être utilisé pour spécifier le trafic autorisé du centre de données est-ouest, tout en laissant le rôle principal d'application des politiques entrantes nord-sud au centre de données situé à la frontière. Dans un environnement mixte de commutateurs DSS et non DSS, des règles d'entrée sont requises pour une application complète de la politique du centre de données est-ouest, ce qui étend les sessions entrantes au réseau où la politique PSM d'entrée est appliquée.

Considérations politiques en matière de MSP

La stratégie est appliquée au niveau de la couche VLAN, de sorte que les exigences réseau de tous les membres du VLAN doivent être prises en compte lors de la création d'un ensemble de règles de stratégie. Lorsqu'une règle d'entrée est appliquée, tout le trafic acheminé destiné aux hôtes du VLAN à partir d'autres commutateurs doit être pris en compte, y compris tout le trafic transféré EVPN de couche 2. Lors de la définition d'une règle de sortie, toutes les communications provenant des hôtes sur le VLAN doivent être prises en compte. Des règles autorisant les services sous-jacents sont requises lors de l'application d'une politique de sortie à un réseau, car le trafic dont la source n'est pas explicitement autorisée par les hôtes sera bloqué par la règle de refus implicite. Les règles prenant en charge les services tels que DNS, la journalisation et l'authentification doivent être définies.

Les règles d'une stratégie sont appliquées dans l'ordre dans lequel elles apparaissent dans la liste. Une règle de refus implicite est appliquée à la fin d'un ensemble de règles. Les règles les plus utilisées devraient apparaître plus haut dans la liste.

Il est recommandé de définir un ensemble complet de règles avant d'appliquer une politique à un réseau. Si l'ensemble complet des règles est inconnu, une règle d'autorisation totale peut être appliquée pour collecter des données de journal sur le trafic observé. Un ensemble complet de règles peut être construit en insérant des règles pour autoriser un trafic plus spécifique au-dessus de la règle d'autorisation totale. Lorsqu'aucun trafic recherché n'atteint la règle d'autorisation totale en bas de l'ensemble de règles, supprimez-le.

Architecture de référence Aruba pour les données Centre

L'architecture de référence du centre de données Aruba ESP (Edge Services Platform) prend en charge les racks de calcul à haute disponibilité à l'aide de commutateurs Top-of-Rack (ToR) redondants connectés dans une topologie spine-and-leaf de couche 3 . La topologie en forme de colonne vertébrale optimise les performances et offre une conception évolutive horizontalement qui peut s'étendre pour s'adapter à un centre de données en pleine croissance sans perturber les composants réseau existants. Un centre de données peut démarrer avec seulement deux commutateurs spine. Lorsqu'une capacité supplémentaire est requise, jusqu'à quatre commutateurs spine peuvent être déployés dans une seule structure. La figure suivante montre l'architecture de référence avec trois commutateurs spine.

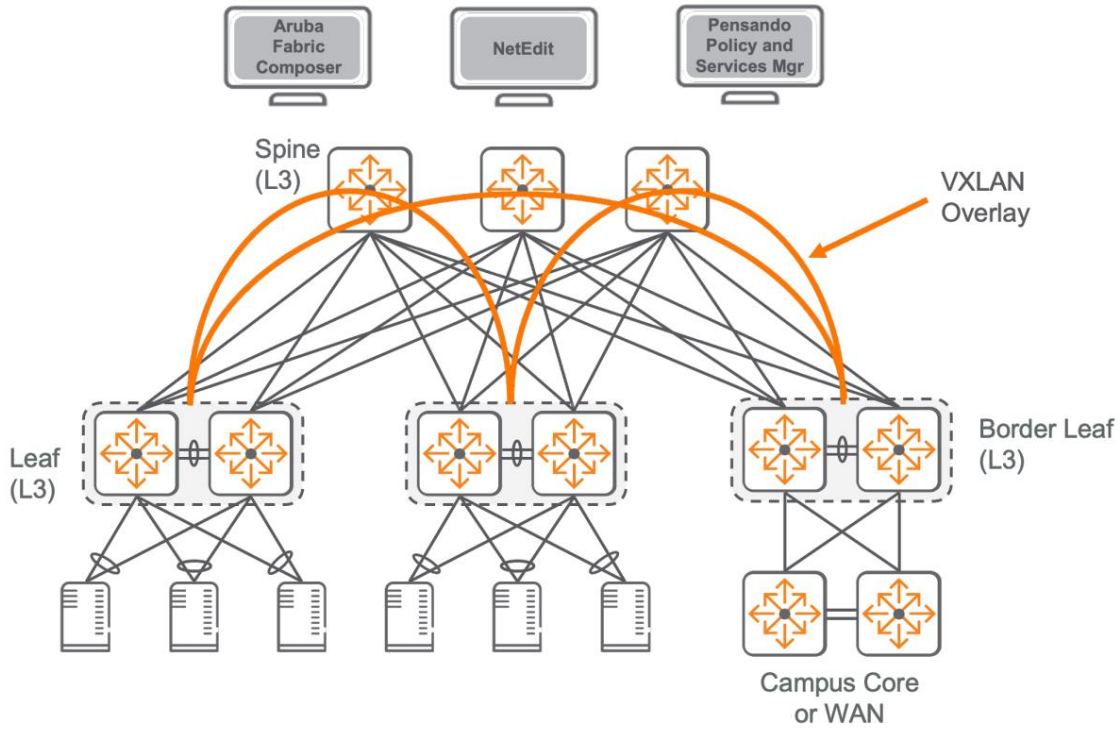

Figure 11 : Dos et feuille : double dessus du rack

Certains environnements d'application ne nécessitent pas de haute disponibilité sur l'hôte de calcul individuel. Dans ce cas, un seul commutateur ToR par rack fournira un réseau de centre de données plus rentable. Dans ce type de mise en œuvre, le nombre d'hôtes de calcul déployés par rack doit rester faible, car un commutateur ToR en cours de maintenance a un impact sur la connectivité à tous les hôtes de calcul du rack. La topologie suivante montre une conception ToR unique avec deux commutateurs spine.

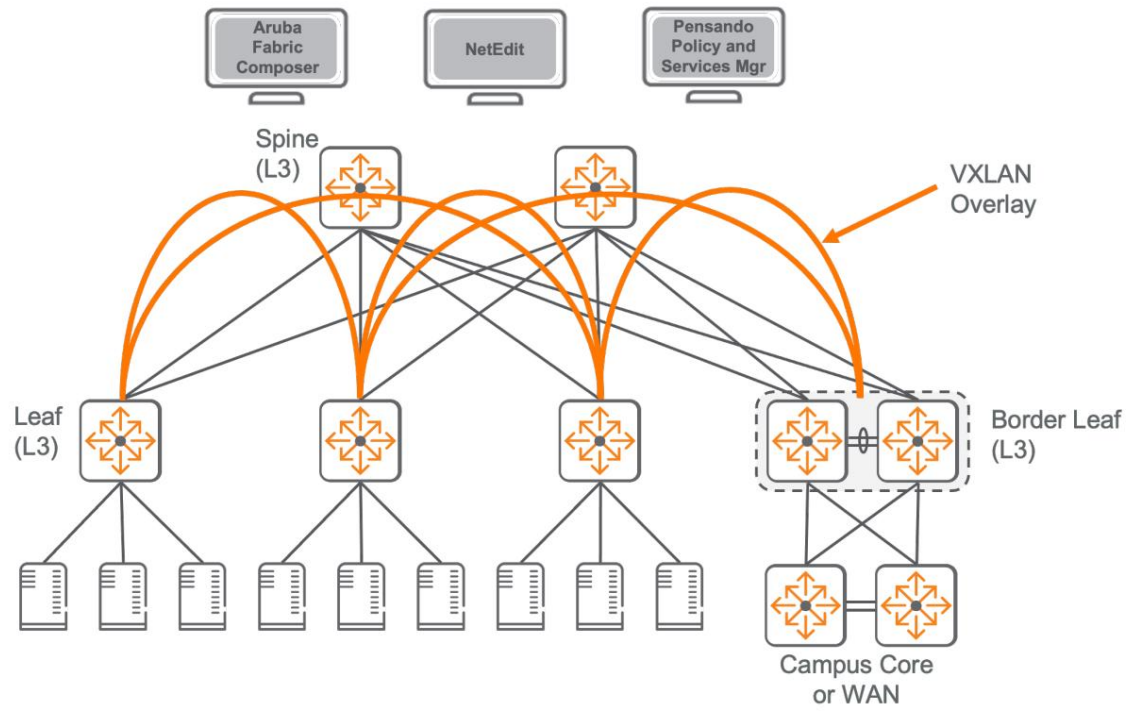

Figure 12 : Dos et feuille : haut unique du rack

Sélection des composants de l'architecture de référence

La section suivante fournit des conseils pour la sélection du matériel en fonction de votre hôte de calcul, de sa disponibilité et de vos exigences en matière de bande passante.

Commutateurs de centre de données Aruba CX

La gamme Aruba CX propose trois modèles de commutateurs de centre de données à configuration fixe. Les modèles CX 10000 et 8325 offrent une densité de ports élevée, tandis que le modèle CX 8360 offre une variété de configurations de ports pour les topologies spine-and-leaf de petite et moyenne taille. Tous les modèles offrent les capacités de commutation de centre de données suivantes :

- Architecture haut débit entièrement distribuée avec transfert à débit linéaire • Haute disponibilité et mises à niveau des ToR en service avec VSX • Système d'exploitation moderne natif cloud et entièrement programmable, construit sur une architecture de microservices. tecture
- Configuration réseau sans erreur avec des outils d'orchestration définis par logiciel • Analyses distribuées et dépannage guidé offrent une visibilité complète et une résolution rapide des problèmes • Ventilateurs et blocs d'alimentation à partage de charge remplaçables à chaud et redondants • Alimentation vers port et port vers alimentation options de refroidissement pour différentes conceptions de centres de données • Prise en charge des trames Jumbo pour les trames de 9 198 octets

- Fonctionnalités avancées de couche 2 et de couche 3 pour prendre en charge le spine et la feuille VXLAN avec MP-BGP/EVPN plan de contrôle •
- Passerelles actives distribuées pour prendre en charge la mobilité des hôtes

Le commutateur de services distribués Aruba CX 10000 prend en charge des fonctionnalités supplémentaires à prendre en compte lors de la sélection d'un modèle de commutateur feuille. Le DPU Pensando intégré prend actuellement en charge l'application d'un pare-feu dynamique en ligne et une visibilité améliorée du trafic. Les futures fonctions incluront les services de chiffrement, la protection DDoS, l'équilibrage de charge et le NAT.

Commutateurs de colonne vertébrale

L'architecture de référence du centre de données Aruba ESP est construite autour de deux commutateurs spine haute densité 1RU dotés de ports QSFP capables d'atteindre des vitesses de 40/100 GbE. L'Aruba CX 8325 peut prendre en charge jusqu'à 32 racks de calcul dans une topologie de commutateur ToR unique ou jusqu'à 16 racks de calcul dans une topologie de commutateur ToR double. L'Aruba CX 8360 peut prendre en charge jusqu'à 12 racks de calcul dans une topologie de commutateur ToR unique ou jusqu'à 6 racks de calcul dans une topologie de commutateur ToR double.

La fonction principale des commutateurs spine est de prendre des décisions de routage pour la superposition. Les principales considérations de conception lors du choix d'un commutateur spine sont :

- Densité des ports
- Vitesses des ports
- Tailles des tables de routage

Tableau 1 : Commutateurs de colonne vertébrale

Description de l'article	Capacité maximale des racks
JL626A 8325 : 32 ports 40/100 GbE QSFP+/QSFP28, port vers alimentation flux d'air	32 TdR simples / 16 TdR doubles
JL627A 8325 : 32 ports 40/100 GbE QSFP+/QSFP28, alimentation vers port flux d'air	32 TdR simples / 16 TdR doubles
JL708A 8360 : 12 ports 40/100 GbE QSFP+/QSFP28, port vers alimentation flux d'air	12 ToR simples / 6 ToR doubles
JL709A 8360 : 12 ports 40/100 GbE QSFP+/QSFP28, alimentation vers port flux d'air	12 ToR simples / 6 ToR doubles

Interrupteurs à feuilles

Il existe trois modèles de commutateurs à feuilles parmi lesquels choisir dans l'architecture de référence du centre de données Aruba ESP. Tous les modèles sont des commutateurs ToR 1RU qui prennent en charge les racks haute densité utilisant des ports cuivre 10GbE ou SFP+. Les ports SFP du modèle Aruba CX 8360 prennent également en charge les émetteurs-récepteurs 10GBASE-T.

Pour les conceptions ToR redondantes, les SKU haute et moyenne densité fournissent le minimum de quatre ports de liaison montante requis pour une topologie à deux commutateurs. Pour une conception ToR non redondante, les SKU de densité moyenne et faible fournissent le minimum de deux ports de liaison montante requis pour une topologie à deux commutateurs.

Le commutateur de services distribués Aruba CX 10000 ajoute des fonctionnalités de pare-feu généralement fournies par des appareils dédiés dans une feuille de services ou des hôtes de calcul connectés en tant que fonctionnalités de structure de commutation en ligne. Le commutateur Aruba CX 10000 doit être sélectionné lorsque ces fonctionnalités sont requises par les hôtes en aval ou pour répondre à d'autres objectifs du centre de données. Ces fonctionnalités ne sont pas disponibles sur les autres modèles de commutateurs CX. Un mélange de différents modèles de commutateurs à feuilles ToR peut se connecter à une colonne vertébrale commune. Les CX 10000, 8325 et 8360 peuvent être installés dans des racks feuilles qui ne nécessitent pas de fonctionnalités de commutateur de service distribué.

Le tableau suivant résume les SKU feuilles disponibles avec leurs conceptions prises en charge correspondantes.

Tableau 2 : interrupteurs à feuilles

Description de l'article	Conception de racks	Colonne vertébrale Conception
R8P13A 10 000 : 48 ports 1/10/25 GbE SFP/SFP+/SFP28, 6 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	Haute densité / Double ToR 2 à 3	commutateurs
R8P14A10000 : 48 ports 1/10/25 GbE SFP/SFP+/SFP28, 6 ports 40/100 GbE QSFP+/QSFP28, flux d'air alimentation vers port	Haute densité / Double ToR 2 à 3	commutateurs
JL624A 8325 : 48 ports 1/10/25 GbE SFP/SFP+/SFP28, 8 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	Haute densité / double ToR 2–4	commutateurs
JL625A 8325 : 48 ports 1/10/25 GbE SFP/SFP+/SFP28, 8 ports 40/100 GbE QSFP+/QSFP28, flux d'air alimentation vers port	Haute densité / double ToR 2–4	commutateurs
JL706A 8360 : 48 ports 100 M/1 GbE/10 GbE 10GBASE-T, 4 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	Haute densité / double ToR 2	commutateurs
JL707A 8360 : 48 ports 100 M/1 GbE/10 GbE 10GBASE-T, 4 ports 40/100 GbE QSFP+/QSFP28, flux d'air alimentation vers port	Haute densité / double ToR 2	commutateurs
JL700A 8360 : 32 ports 1/10/25 GbE SFP/SFP+/SFP28, 4 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	Densité moyenne / double Tor	2 commutateurs
JL701A 8360 : 32 ports 1/10/25 GbE SFP/SFP+/SFP28, 4 ports 40/100 GbE QSFP+/QSFP28, flux d'air alimentation vers port	Densité moyenne / double Tor	2 commutateurs
JL710A 8360 : 24 ports 1/10 GbE SFP/SFP+, 2 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	Densité moyenne / ToR unique	2 commutateurs
JL711A 8360 : 24 ports 1/10 GbE SFP/SFP+, 2 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	Densité moyenne / ToR unique	2 commutateurs
JL702A 8360 : 16 ports 1/10/25 GbE SFP/SFP+/SFP28, 2 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	Faible densité / simple Tor	2 commutateurs

Description de l'article	Conception de racks	Colonne vertébrale Conception
JL703A 8360 : 16 ports 1/10/25 GbE SFP/SFP+/SFP28, 2 ports 40/100 GbE QSFP+/QSFP28, flux d'air alimentation vers port	Densité moyenne / mandat unique	2 commutateurs

Commutateurs de gestion hors bande

L'architecture de référence du centre de données Aruba ESP utilise un réseau local de gestion basé sur une commutation dédiée. infrastructure pour garantir une connectivité fiable à l'infrastructure du centre de données pour l'automatisation, l'orchestration, et accès à la gestion traditionnelle. Le tableau suivant répertorie les modèles de commutateurs recommandés.

Tableau 3 : commutateurs de gestion hors bande

UGS	Description	Ports hôtes
JL667A	Aruba CX 6300F commutateur 48 ports 1 GbE et 4 ports SFP56 48	
JL668A	Aruba CX 6300F commutateur 24 ports 1 GbE et 4 ports SFP56 24	
JL663A	Commutateur Aruba CX 6300M 48 ports 1 GbE et 4 ports SFP56 48	
JL664A	Aruba CX 6300M 24 ports 1 GbE et 4 ports SFP56 Switch 24	
Commutateur JL724A	Aruba 6200F 24G 4SFP+	24
Commutateur JL726A	Aruba 6200F 48G 4SFP+	48
JL678A	Commutateur Aruba 6100 24G 4SFP+	24
JL676A	Commutateur Aruba 6100 48G 4SFP+	48

Compositeur de tissus d'Aruba

Aruba Fabric Composer (AFC) est proposé sous la forme d'un ISO autonome ou d'une machine virtuelle OVA et peut être installé dans des environnements hôtes virtuels et physiques en tant qu'instance unique ou en haute disponibilité, cluster à trois nœuds. AFC est disponible sous forme d'abonnement annuel au logiciel par commutateur.

AFC prend en charge les commutateurs Aruba CX 10000, 8325 et 8360 recommandés pour Spine et Leaf. rôles. Il prend également en charge les commutateurs Aruba CX 6300, 6400 et 8400.

Les informations de commande pour AFC se trouvent à la fin de l' aperçu des solutions.

Responsable des politiques et des services Pensando

Le Pensando Policy and Services Manager (PSM) s'exécute en tant que machine virtuelle OVA sur un hôte. Le MSP exige vCenter pour l'installation, et il est déployé en tant que cluster haute disponibilité basé sur quorum de trois machines virtuelles.

PSM prend en charge les commutateurs Aruba CX 10000. La gestion du PSM est intégrée à l'AFC.

PSM peut être téléchargé à partir du portail d'assistance Aruba. Le droit à PSM est inclus à l' achat d'un commutateur Aruba CX 10000 en ajoutant le SKU R9H25AAE.

Net

NetEdit s'exécute en tant que VM OVA sur un hôte. Aruba NetEdit est disponible sur le portail de services Aruba. Clients devez visiter la communauté Aruba Airheads et créer un compte Airheads afin de télécharger le Logiciel NetEdit.

Les informations de commande d'Aruba NetEdit se trouvent à la fin de cette fiche technique.

Planification de la couche physique de l'architecture de référence

La section suivante fournit des conseils pour la planification de la couche physique des commutateurs de votre centre de données.

Câbles et émetteurs-récepteurs

Veuillez vous référer aux documents suivants pour vous assurer que vous sélectionnez les câbles et émetteurs-récepteurs pris en charge lorsque vous planifiez la connectivité physique à l'intérieur de votre centre de données :

Matrice de compatibilité des émetteurs-récepteurs et des câbles HPE Server Networking

Guide des émetteurs-récepteurs ArubaOS-Switch et ArubaOS-CX

Groupes de vitesse portuaire

Lors de la planification de configurations ToR qui nécessitent une connectivité de serveur à plusieurs vitesses, il est important de noter que la définition de la vitesse d'un port peut nécessiter que les ports adjacents fonctionnent ensuite à cette même vitesse.

Les commutateurs Aruba CX 8325 et Aruba CX 10000 ont une vitesse par défaut de 25 GbE. Le changement de vitesse à 10 GbE aura un impact sur les groupes de 12 ports sur l'Aruba CX 8325 et les groupes de quatre ports sur l'Aruba CX 10000. Les commutateurs Aruba CX 8360 permettent à des ports individuels de fonctionner à des vitesses différentes sans affecter les ports adjacents, sauf si la sécurité du contrôle d'accès au support (MACSec).) est en cours d'utilisation. Les ports configurés pour utiliser MACSec doivent tous être configurés pour fonctionner à la même vitesse.

Ports divisés

Les câbles breakout peuvent être utilisés pour diviser un port 40 Gb/s ou 100 Gb/s en quatre connexions à vitesse inférieure (4x10 Gb/s et 4x25 Gb/s). Veuillez vous référer au Guide des émetteurs-récepteurs ArubaOS-Switch et ArubaOS-CX. pour sélectionner les câbles épanouis pris en charge et la prise en charge des commutateurs pour les ports divisés.

Sécurité du contrôle d'accès aux médias

MACsec est une norme définie dans IEEE 802.1AE qui étend la norme Ethernet pour fournir un cryptage au niveau de la trame sur les liaisons point à point. Cette fonctionnalité est généralement utilisée dans des environnements où des couches supplémentaires de confidentialité des données sont requises ou où il est impossible de sécuriser physiquement les liaisons réseau entre les systèmes. Veuillez vous référer au tableau suivant pour plus de détails sur la prise en charge de MACsec dans le portefeuille de commutation Aruba :

Tableau 4 : Prise en charge de MACsec dans les commutateurs Aruba

UGS	Description	Ports pris en charge
JL700A	8360 : 32 ports 1/10/25 GbE SFP/SFP+/SFP28, 4 ports 40/100 GbE QSFP+/QSFP28, flux d'air port vers alimentation	1 à 4 SFP+/SFP28
JL701A	8360 : 32 ports 1/10/25 GbE SFP/SFP+/SFP28, 4 ports 40/100 GbE QSFP+/QSFP28, flux d'air alimentation-port	1 à 4 SFP+/SFP28

Planification des capacités de l'architecture de référence

La section suivante fournit des conseils de planification de capacité pour l' architecture de référence spine-and-leaf du centre de données Aruba ESP.

Calculs de bande passante

Une conception de réseau en forme de colonne vertébrale offre une flexibilité et un débit maximum pour la mise en œuvre du centre de données Aruba ESP. Pour atteindre le plus haut niveau de performances, une topologie en forme de colonne vertébrale et de feuille peut être conçue pour éviter tout surabonnement de bande passante. Il en résulte un réseau de centre de données qui ne sera jamais encombré car la bande passante disponible pour les hôtes est égale à la bande passante entre les commutateurs feuille et colonne vertébrale.

Un avantage significatif d'une conception spine-and-leaf est qu'une capacité supplémentaire peut être ajoutée si nécessaire en ajoutant des commutateurs spine supplémentaires et/ou en augmentant la vitesse des liaisons montantes entre les commutateurs leaf-and-spine. Un rack avec 40 serveurs à double hébergement avec des cartes réseau 10 GbE pourrait théoriquement générer une charge totale de 800 Go de trafic. Pour cette configuration de densité de serveur, une structure 1:1 (non sursouscrite) pourrait être construite avec quatre commutateurs spine utilisant 4 liaisons 100 GbE sur chacun. En pratique, la plupart des topologies spine-and-leaf sont construites entre 2,4 : 1 et 6 : 1 surabonnement serveur/fabric.

Mise à l'échelle du réseau et du calcul

L'architecture de référence du centre de données Aruba ESP offre une capacité suffisante pour la plupart des déploiements. Avec les passerelles distribuées et le transfert IRB symétrique, les tables MAC et ARP sont localisées sur nœuds de calcul directement connectés et non affectés par le nombre de racks. Le nombre de préfixes IP sera fonction du nombre total de nœuds, de liens de structure, ainsi que du nombre de points physiques et/ou serveurs virtualisés. La feuille de bordure est généralement le nœud avec la charge de plan de contrôle la plus élevée car elle gère les connexions internes et externes. Le résumé d'itinéraire est une bonne pratique pour réduire le redistribution des préfixes IP entre domaines.

L'architecture de référence du centre de données Aruba ESP a été minutieusement testée dans une solution de bout en bout environnement qui intègre les meilleures pratiques de déploiement, les applications et la charge profils qui représentent les environnements de production.

Veuillez vous référer aux fiches techniques des produits sur les commutateurs Aruba Campus Core et Aggregation. pour plus de détails spécifications non incluses dans ce guide. Le tableau suivant fournit des données multidimensionnelles validées profils que vous pouvez utiliser pour la planification de la capacité de conception de la colonne vertébrale et des feuilles.

Tableau 5 : Profils multidimensionnels validés

Fonctionnalité	8325 Feuillet	8360 Feuillet	8325 Dos	8360 Dos
Échelle de l'hôte : IPv4/ARP	30 000	50 000	N / A	N / A
Échelle de l'hôte : IPv6/ND	15 000	50 000	N / A	N / A
Routage : routes IPv4	10 000	16 000	72 000	100 000
Routage : routes IPv6	1000	8000	20 000	100 000
Routage : voisins OSPF	4	4	128	64
VXLAN : VRF superposés (VNI de couche 3)	32	32	N / A	N / A
VXLAN : VLAN hôtes (VNI de couche 2)	1024	512	N / A	N / A
SVI de passerelle active	1000	512	N / A	N / A

Résumé

Les réseaux de centres de données évoluent rapidement. Le défi le plus urgent consiste à maintenir la stabilité opérationnelle, la sécurité et la visibilité tout en plaçant les ressources de calcul et de stockage là où elles servent le mieux aux utilisateurs. En outre, les équipes des centres de données sont invitées à prendre en charge le rythme rapide des environnements DevOps, notamment en se connectant directement à l'infrastructure de cloud public. Compte tenu de l'évolution rapide des exigences des centres de données, il est essentiel que les ingénieurs réseau et système disposent des outils dont ils ont besoin pour simplifier et automatiser les configurations d'infrastructure complexes.

Le centre de données ESP d'Aruba Networks s'appuie sur une technologie qui fournit des outils permettant de transformer le centre de données en une plate-forme de prestation de services moderne et agile qui répond aux exigences des organisations, grandes, petites, distribuées et centralisées. ArubaOS-CX simplifie les opérations et la maintenance grâce à un système d'exploitation de commutation commun sur le campus, la succursale et le centre de données, géré depuis le cloud ou sur site, et soutenu par une IA qui fournit des conseils sur les meilleures pratiques tout au long du cycle de vie du réseau.

Quoi de neuf dans cette version

Les modifications suivantes ont été apportées depuis la dernière publication de ce guide par Aruba : - Conception étendue de la couche de stratégie conseils. - Détails étendus sur PSM et Aruba CX 10000.

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550