Une image contenant Police, Graphique, graphisme, capture d’écran

Description générée automatiquement

Réponse appel d’offre

EDOUARD EHIANTIQUI

MADY DIABY

ISMAILA FOFANA

DIABOU BA

Table des matières

[Introduction 2](#_Toc170579105)

[Contexte et Enjeux 2](#_Toc170579106)

[Objectif de la Réponse 2](#_Toc170579107)

[Structure du Document 2](#_Toc170579108)

[Résumé Exécutif 3](#_Toc170579109)

[Compréhension des Besoins du Client 3](#_Toc170579110)

[Scénario 3](#_Toc170579111)

[Objectifs 3](#_Toc170579112)

[Contraintes Identifiées 4](#_Toc170579113)

[Solution Réseau Proposée 5](#_Toc170579114)

[Schémas d’architecture réseau WAN 6](#_Toc170579115)

[Solutions Réseau 6](#_Toc170579116)

[Solution Système Proposée 9](#_Toc170579117)

[Schémas Active Directory 9](#_Toc170579118)

[Solution 9](#_Toc170579119)

# Introduction

## Contexte et Enjeux

La société Dev-Education, spécialisée dans le déploiement et la gestion des infrastructures des centres de formation, fait face à une expansion rapide de son nombre de clients et à des évolutions technologiques importantes. À ce jour, Dev-Education dessert environ 500 clients, un nombre qui devrait doubler dans les cinq prochaines années. Pour soutenir cette croissance et répondre aux exigences de modernisation, Dev-Education a lancé un appel d'offre visant à adapter et à améliorer son infrastructure existante.

## Objectif de la Réponse

Ce document vise à répondre de manière exhaustive et structurée à l'appel d'offre de Dev-Education. Nous proposons une solution complète qui s'aligne avec les besoins et contraintes spécifiques identifiés dans le cahier des charges. Notre réponse est construite sur une analyse approfondie des besoins fonctionnels et techniques, ainsi que sur une présentation détaillée des solutions proposées pour chaque aspect du projet.

## Structure du Document

Ce document est organisé en plusieurs sections afin de couvrir de manière exhaustive les différents aspects du projet. Chaque section est conçue pour offrir une clarté maximale et démontrer notre capacité à réaliser ce projet avec succès.

1. **Introduction**
2. **Résumé Exécutif**
3. **Compréhension des Besoins du Client**
4. **Solution Réseau Proposée**
5. **Solution Système Proposée**
6. **Gouvernance et Conformité**
7. **Phases du Projet**
8. **Planning et Délais**
9. **Coût et Financement**
10. **Conclusion**
11. **Annexes**

# Résumé Exécutif

EMID, spécialisée dans les solutions IT et les services de gestion des infrastructures, propose une réponse complète et innovante à l'appel d'offre de Dev-Education. Face à l'expansion rapide et aux besoins de modernisation de Dev-Education, notre solution se concentre sur la continuité, la sécurité, et la scalabilité des infrastructures.

Nous avons conçu une solution qui garantit des connexions sécurisées entre sites, une supervision efficace des matériels et systèmes, une sauvegarde automatisée et sécurisée des bases de données, et une migration fluide vers des services cloud publics. En utilisant des technologies éprouvées et en appliquant les meilleures pratiques de l'industrie, notre proposition assure une gestion optimale des identités et une protection renforcée contre les menaces de sécurité.

Notre plan de projet détaillé, accompagné d'une estimation budgétaire précise et d'un calendrier de déploiement rigoureux, démontre notre capacité à réaliser ce projet avec succès. Nous nous engageons à fournir un support de qualité et à respecter les délais et les exigences spécifiés par Dev-Education.

# Compréhension des Besoins du Client

## Scénario

Dev-Education est une société dédiée à la gestion des infrastructures des centres de formation. Avec une base actuelle de 500 clients, Dev-Education anticipe un doublement de ce nombre dans les cinq prochaines années. Cette croissance rapide nécessite une modernisation significative de l'infrastructure actuelle pour garantir une prestation de services optimale, sécurisée et évolutive.

## Objectifs

Les principaux objectifs identifiés pour Dev-Education sont :

1. **Connexions sécurisées entre sites** :
   * Établir des connexions sécurisées pour échanger des informations entre les sites d’un même organisme.
   * La solution doit gérer jusqu'à 20 connexions VPN simultanées
2. **Supervision des matériels et systèmes** :
   * Mettre en place une solution de supervision pour remonter des informations sur l’état des équipements.
   * Garantir que les informations ne soient pas perdues en cas de coupure de lien entre le site central et le client.
3. **Sauvegarde automatisée des bases de données** :
   * Implémenter une sauvegarde automatisée des bases de données de chaque centre avec une durée de rétention de 7 jours.
   * Assurer la redondance du service pour la pérennité.
4. **Solution de sécurité pour les serveurs et postes clients** :
   * Proposer une solution de sécurité conforme aux standards actuels pour protéger les serveurs et postes clients.
5. **Infrastructure réseau programmable** :
   * Proposer des équipements réseau programmables dans la gamme Cisco.
6. **Automatisation du déploiement des configurations** :
   * Mettre en place des solutions techniques permettant de déployer les configurations d'équipements actifs à la demande, compatibles avec les anciens et nouveaux équipements.
7. **Sécurisation des méthodes d’administration** :
   * Évoluer les méthodes d’administration pour sécuriser les identités et les communications.
8. **Transfert des services sur différents clouds publics** :
   * Migrer les applications vers le cloud tout en gardant la gestion des identités sur le site central.
   * Examiner les offres complémentaires de services après la migration.
9. **Éviter les points de défaillance unique (SPOF) dans l’infrastructure de stockage** :
   * Étudier et proposer une solution de stockage SDS (Software Defined Storage) hautement disponible.
10. **Conformité et sécurité** :
    * Proposer des solutions pérennes respectant les bonnes pratiques de sécurité définies par les éditeurs et l’ANSSI.
    * Réduire la surface d’attaque, appliquer le principe du moindre privilège, et gérer les accès administrateurs privilégiés.

## Contraintes Identifiées

1. **Capacité des équipements existants** : Les équipements actuels ne supportent que 5 connexions VPN concurrentes, alors que la nouvelle solution doit en supporter 20.
2. **Redondance et disponibilité** : La solution de sauvegarde doit être redondante pour assurer une pérennité sans faille.
3. **Compatibilité des équipements** : Les solutions proposées doivent être compatibles avec les équipements réseau existants et futurs.
4. **Sécurité accrue** : L’administration des systèmes doit être hautement sécurisée, incluant MFA et des méthodes de protection contre l’usurpation d’identité.
5. **Migration fluide** : La migration vers le cloud doit être transparente pour les utilisateurs tout en maintenant une gestion centralisée des identités.

# Solution Réseau Proposée

Pour répondre efficacement aux besoins de Dev-Education, nous avons conçu une solution réseau qui intègre les meilleures pratiques et technologies de pointe. Voici les solutions détaillées que nous proposons pour garantir la sécurité, la performance, et la résilience de l'infrastructure réseau :

## Schémas d’architecture réseau WAN Une image contenant texte, diagramme, Plan, Dessin technique Description générée automatiquement

## Solutions Réseau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Objectif | Description | Solution | Technologie utilisée | Avantages |
| Connexions VPN sécurisées | Établir des connexions sécurisées entre les sites d’un même organisme pour échanger des informations. | Utilisation de SD-WAN Cisco Meraki en topologie hub and spoke | Cisco Meraki MX series pour les sites et branches, et un hub central pour gérer toutes les connexions. | - Optimisation de l'utilisation des équipements existants - Réduction des coûts supplémentaires - Sécurité renforcée pour les communications entre sites |
| vMX pour Azure | Déploiement d'un Cisco Meraki vMX dans Azure pour gérer les connexions VPN des serveurs hébergés sur Azure et assurer l'intégration fluide avec le réseau central. | Déploiement d'un Cisco Meraki vMX dans Azure | Cisco Meraki vMX100 ou vMX200 selon la taille et les besoins du déploiement. | - Gestion des connexions VPN des serveurs hébergés sur Azure - Intégration fluide avec le réseau central |
| Supervision des matériels et systèmes | Mettre en place une solution de supervision pour les équipements clients permettant de remonter des informations sur l’état des matériels et de conserver ces informations en cas de coupure de lien. | Utilisation de PRTG pour la supervision de l'infrastructure réseau | PRTG Network Monitor | - Surveillance proactive - Détection rapide des anomalies - Amélioration de la disponibilité et de la performance des systèmes |
| Infrastructure réseau programmable | Proposer des équipements réseau programmables dans la gamme Cisco pour une meilleure gestion et optimisation des performances. | Mise en œuvre de SD-WAN Cisco Meraki | Cisco Meraki MX et MS series | - Flexibilité accrue - Simplification de la gestion réseau - Amélioration de la performance et de la résilience du réseau |
| Automatisation du déploiement des configurations | Utiliser des solutions comme Ansible pour automatiser le déploiement et la configuration des équipements réseau. | Utilisation d'Ansible pour automatiser la configuration et le déploiement des équipements réseau | Ansible, playbooks personnalisés pour les configurations spécifiques | - Réduction des erreurs humaines - Déploiement rapide et cohérent des configurations - Gain de temps et d'efficacité opérationnelle |
| Redondance des connexions réseau | Assurer la disponibilité continue des connexions réseau en cas de défaillance d'un lien principal. | Mise en place de liens redondants | Cisco Meraki MX series | - Augmentation de la disponibilité du réseau - Minimisation des interruptions de service - Continuité des opérations |
| Sécurité du réseau | Protection des données et des communications sur le réseau contre les menaces et les attaques. | Utilisation de Cisco Umbrella (SASE) avec filtrage web, DNS over HTTPS et CASB (Cloud Access Security Broker) | Cisco Umbrella et Microsoft Defender for Cloud Apps CASB (Cloud Access Security Broker) | - Sécurité renforcée contre les menaces en ligne - Protection des données avec DNS over HTTPS - Surveillance et contrôle des accès au cloud avec CASB - Amélioration de la confidentialité et de l'intégrité des communications |
| Migration vers le Cloud | Déplacement des bases de données et des applications vers le cloud pour une flexibilité accrue. | Migration des bases de données et des applications vers Azure | Azure Cloud Services | - Flexibilité et scalabilité accrues - Réduction des coûts d’infrastructure - Amélioration de la performance et de la disponibilité |
| Téléphonie sur IP | Intégration de la téléphonie sur IP via Microsoft Teams pour une communication unifiée et efficace. | Microsoft Teams avec Direct Routing | Microsoft Teams et SBC (Session Border Controller) pour Direct Routing | - Communication unifiée - Réduction des coûts de téléphonie - Intégration avec les outils de collaboration Microsoft |
| Optimisation des VPN | Assurer la haute disponibilité des connexions VPN et améliorer l'efficacité du réseau. | Mise en place de VPN Bonding et Split Tunneling | SD-WAN Cisco Meraki | - Amélioration de la disponibilité des connexions VPN - Réduction de la latence et optimisation de la bande passante - Séparation du trafic critique et non critique |

# Solution Système Proposée

Pour répondre efficacement aux besoins système de Dev-Education, nous proposons une solution qui intègre des technologies avancées et des pratiques éprouvées pour assurer la sécurité, la performance et la gestion optimale des systèmes.

## Schéma Active Directory

<Insertion plus tard du schéma>

## Solution

**Sauvegarde Automatisée :**

Nous avons choisi Veeam Backup & Replication pour la sauvegarde automatisée des bases de données. Cette solution permet de sauvegarder les données vers Azure avec une réplication dans différentes régions de France. La raison de ce choix est de garantir la sécurité des données avec des sauvegardes régulières, assurer la continuité des opérations grâce à la redondance des données et offrir une haute disponibilité via la réplication et la gestion des pannes.

**Sécurité des Serveurs :**

Pour protéger les serveurs, nous avons opté pour Microsoft Defender et Microsoft Defender for Identity. Microsoft Defender offre des mesures de sécurité robustes pour les systèmes d’exploitation des serveurs, tandis que Microsoft Defender for Identity assure la protection avancée de l'Active Directory.

**Gestion des Vulnérabilités :** Pour identifier, évaluer et atténuer les vulnérabilités sur les serveurs, nous utilisons Microsoft Defender Vulnerability Management. Cette solution permet de détecter et de corriger rapidement les vulnérabilités, réduisant ainsi le risque de failles de sécurité exploitées par des attaquants.

**Application Control et Whitelisting :** Pour restreindre l'exécution d'applications non autorisées, nous utilisons Windows Defender Application Control (WDAC). Cette solution améliore la sécurité en permettant uniquement l'exécution d'applications autorisées, réduisant ainsi les risques d'exécution de logiciels malveillants.

**Sécurité des Postes Clients :**

Pour les postes clients, nous utilisons Microsoft Defender, Bitlocker et Multi-Factor Authentication (MFA). Microsoft Defender fournit une protection complète contre les menaces, Bitlocker assure le chiffrement des disques pour protéger les données, et MFA ajoute une couche supplémentaire de sécurité pour les accès utilisateur. Cette combinaison permet de garantir une protection renforcée contre les menaces, de se conformer aux standards de sécurité et d'améliorer la résilience des postes clients.

**Hybridation des Identités :**

La gestion hybride des identités est réalisée avec Entra ID Connect (ex Azure AD Connect). Cette solution intègre les identités locales et cloud, permettant le Single Sign-On (SSO) pour les comptes Windows et Microsoft 365, ainsi que pour les applications métier. Pour les applications ne supportant pas SSO via Entra ID, nous activons l'authentification LDAPS. De plus, LAPS (Local Administrator Password Solution) est utilisé sur les postes clients, et les appareils sont inscrits dans le MDM (Mobile Device Management) par GPO. Entra ID est également intégré avec le VPN pour le SSO, renforçant ainsi la sécurité des accès et simplifiant la gestion des identités. Cette approche centralisée des identités améliore la sécurité et facilite l'administration.

**Surveillance et Réponse aux Incidents (SIEM) :**

Nous utilisons Microsoft Sentinel pour la surveillance et la réponse aux incidents (SIEM). Microsoft Sentinel collecte et analyse les journaux de sécurité pour détecter rapidement les menaces et répondre de manière proactive aux incidents. Cette solution améliore la sécurité globale du système en permettant une détection rapide des menaces et une réponse efficace aux incidents.

**Microsoft 365 :**

Pour offrir une suite de collaboration et de productivité intégrée, nous avons choisi Microsoft 365. Cette suite comprend Teams, Outlook, Word, PowerPoint et SharePoint. Microsoft 365 améliore la collaboration entre les utilisateurs, augmente la productivité et intègre de manière fluide divers outils de travail.

**MDM : Intune :**

La gestion et la sécurisation des appareils mobiles et des postes clients sont assurées par Intune. Intune permet l'analyse des journaux, la gestion des mises à jour Windows, la configuration des profils de sécurité (LAPS, Bitlocker, Security Baseline) et le déploiement ainsi que la mise à jour des applications sur les postes clients. Cette solution garantit la sécurité des appareils, centralise la gestion des mises à jour et des configurations, et améliore la conformité et la sécurité. Intune intègre également la gestion des patchs pour assurer que tous les systèmes et applications reçoivent les dernières mises à jour de sécurité et correctifs, réduisant ainsi les risques de vulnérabilités non corrigées.

**Stockage Résilient :**

Pour éviter les SPOF (Single Point of Failure), nous utilisons Microsoft Storage Spaces Direct (Azure HCI) comme solution de stockage défini par logiciel. Cette solution répartit logiquement le stockage sur plusieurs unités, offrant une haute disponibilité et une résilience améliorée contre les pannes. Elle permet également une gestion efficace et flexible du stockage.

**Reprise Après Sinistre :**

Enfin, pour garantir la continuité des services en cas de désastre, nous avons choisi Azure Site Recovery. Cette solution orchestre et automatise la récupération des services, assurant ainsi la continuité des opérations en cas de sinistre. Azure Site Recovery réduit les temps d'indisponibilité et assure une reprise rapide et efficace des services.

**Protection Avancée contre les Menaces (ATP) :**

Pour détecter, prévenir et répondre aux menaces avancées, nous utilisons Microsoft Defender for Endpoint. Cette solution fournit une protection proactive contre les menaces, incluant l'analyse comportementale, la détection des anomalies et la réponse automatisée aux incidents.

**Gestion des Droits et Privilèges (PIM) :**

Pour gérer et contrôler les accès privilégiés, nous utilisons Microsoft Entra ID Privileged Identity Management (PIM). Cette solution renforce la sécurité en assurant que les privilèges sont accordés de manière just-in-time et just-enough, réduisant ainsi les risques de privilèges excessifs.

**Solution de Sauvegarde pour les Applications SaaS :**

Pour assurer la sauvegarde et la restauration des données des applications SaaS comme Microsoft 365, nous utilisons Veeam Backup for Microsoft 365. Cette solution garantit la disponibilité des données critiques des applications SaaS, permettant une récupération rapide en cas de perte de données ou de corruption.

**Gestion des Identités et des Accès (IAM) pour les Applications Héritées :**

Pour intégrer les applications héritées qui ne supportent pas SSO ou les nouvelles technologies d'authentification, nous utilisons Azure Active Directory Application Proxy. Cette solution facilite l’intégration des applications héritées dans le nouvel environnement sécurisé sans nécessiter de modifications majeures des applications.

**Supervision avec PRTG :**

Pour la supervision de l'infrastructure, nous utilisons PRTG Network Monitor. PRTG permet de surveiller en temps réel les performances et la disponibilité des systèmes et des réseaux. Cette solution garantit une surveillance proactive, permettant une détection rapide des anomalies et une intervention immédiate pour maintenir la disponibilité et la performance des services.