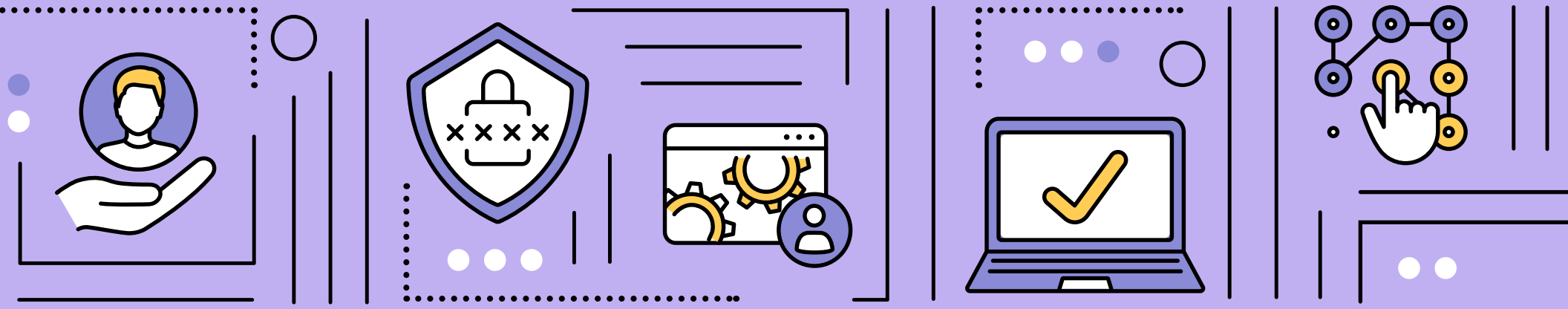
Service de notification push d'Apple

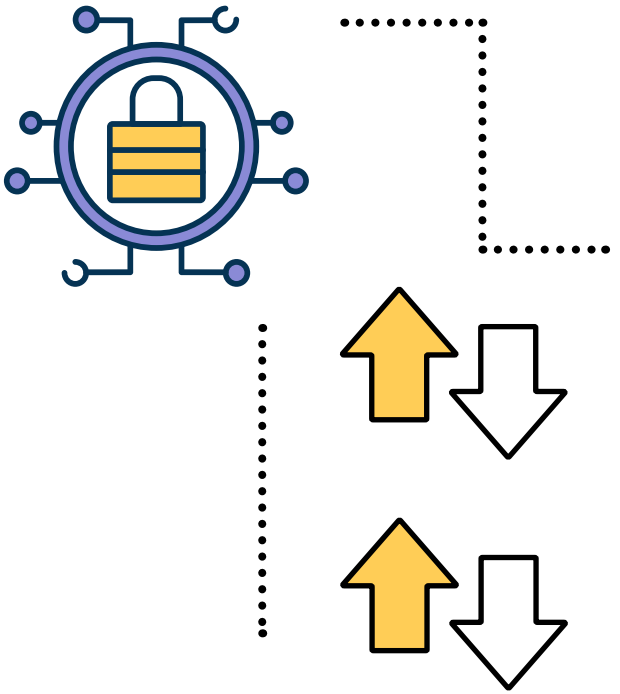
Introduction



Dans l'écosystème Apple, la gestion des appareils peut être très simple, en particulier lorsqu'il s'agit des commandes de base.

Vous souhaitez redémarrer un ordinateur à distance ? Il suffit de sélectionner l'appareil dans l'interface de votre solution de gestion des appareils mobiles (MDM) et de sélectionner le bouton « Redémarrer l'appareil ». Rien de plus facile. Mais comment cette magie opère-t-elle exactement ?

La réponse à cette question est le service de notification push d'Apple, ou APNs. Il sert de pivot à la communication entre le terminal et le serveur MDM. Et c'est précisément le sujet de ce document, des premières étapes de la mise en place jusqu'au maintien de la fonctionnalité et de la fiabilité du service de notification.



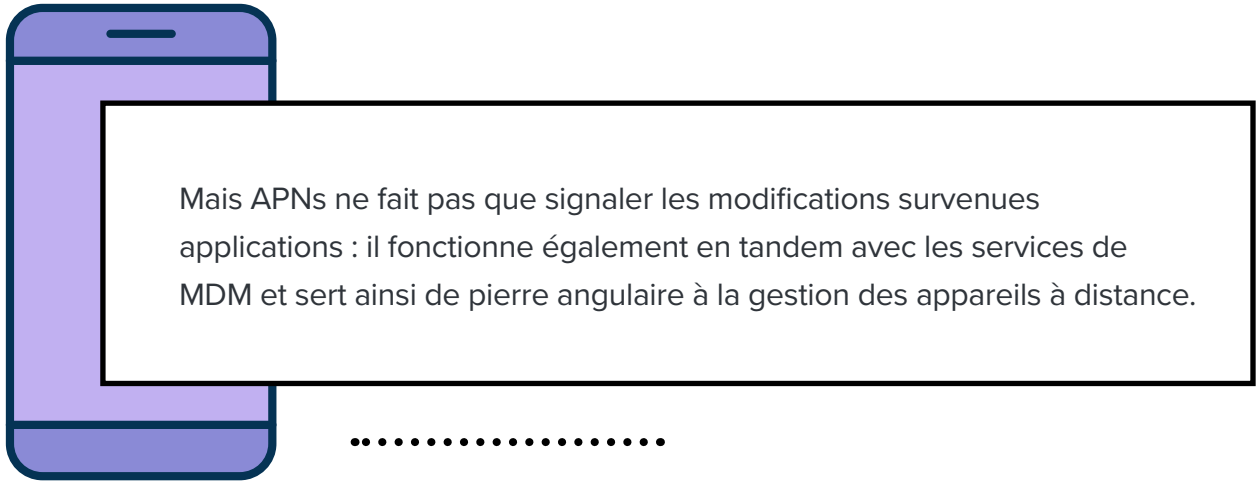
Découvrez dans cet e-book :

- Ce que fait APNs et comment fonctionne le service
- Pourquoi APNs est indispensable à la gestion des appareils
- Les bonnes pratiques pour que APNs reste pleinement opérationnel

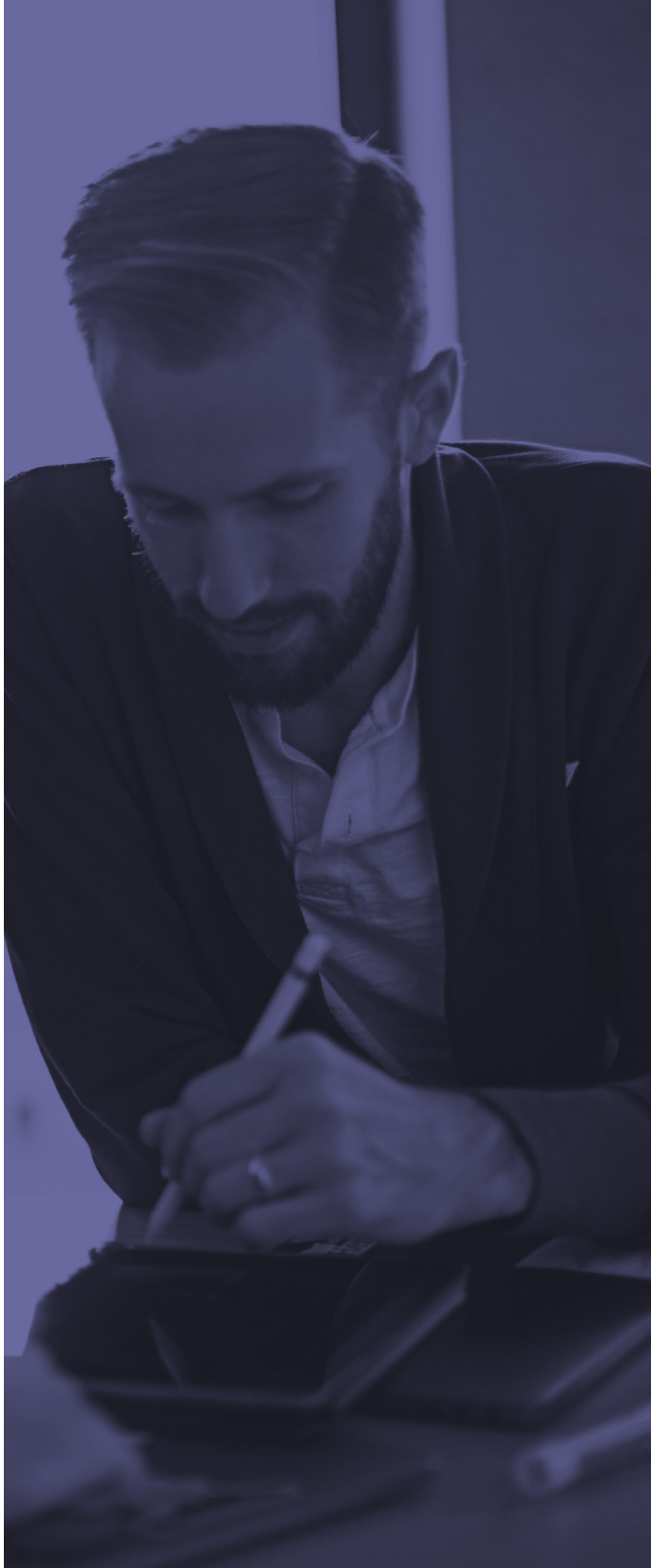
APNs : LES FONDAMENTAUX

Selon Apple, « les notifications locales et push permettent de présenter à l'utilisateur un contenu utile et pertinent quand votre app est à l'arrière-plan ou inactive. Elles peuvent prendre la forme d'un message, d'un son distinctif ou d'un badge sur l'icône de votre application. »

Pour le dire simplement, APNs est la méthode de livraison des communications envoyées aux apps. Ces notifications viennent informer l'utilisateur d'un changement d'état de l'app ou du système. Prenons l'exemple de l'arrivée d'un nouvel e-mail dans votre boîte de réception. Le serveur de messagerie signale ce changement et utilise immédiatement APNs pour vous en avertir, via l'application de votre appareil Apple.



Mais APNs ne fait pas que signaler les modifications survenues applications : il fonctionne également en tandem avec les services de MDM et sert ainsi de pierre angulaire à la gestion des appareils à distance.



La communication est essentielle

Dans le paysage informatique moderne et mondialisé, la communication est la sève de la productivité. De la même manière, APNs est indispensable pour maintenir les applications à jour sur les appareils Apple et informer les utilisateurs des messages importants. Enfin, il permet l'enrôlement des appareils dans la MDM et veille à ce qu'ils restent conformes aux profils de configuration et aux règles de sécurité.

En effet, sans ce composant fondamental, le lien entre les terminaux et le serveur MDM qui les encadre est rompu. Sans une communication directe avec le terminal, les appareils deviennent ingérables pour le service informatique.

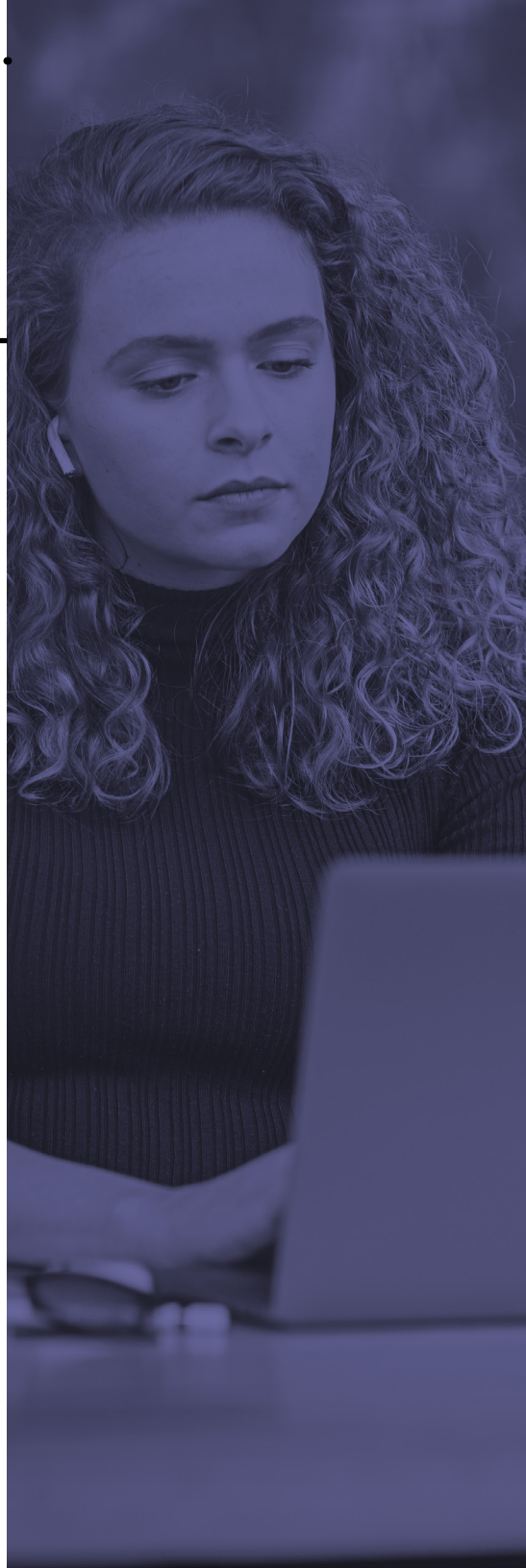
Une remarque toutefois : malgré la perte des capacités de gestion, toutes les applications et configurations déployées resteront intactes. Par contre, les appareils eux-mêmes – ainsi que leurs apps et leurs configurations – ne seront pas mis à jour tant que la connectivité à APNs ne sera pas rétablie.

Comment fonctionne APNs ?

Nous avons expliqué ce qu'est APNs et souligné son rôle crucial, mais vous vous demandez sans doute comment il fonctionne. En fait, c'est assez simple, comme l'illustre le schéma ci-dessous.

Comme vous pouvez le constater, dans ce cas de figure, le fournisseur est le développeur ou le service. Il maintient une connectivité constante avec le cloud des services de notification push d'Apple, qui agit en quelque sorte comme un proxy pour les appareils Apple. Le message initial est envoyé par le fournisseur de MDM à APNs, qui transmet ensuite le message à l'appareil lui-même. Là, il est traité par l'application qui délivre en bout de ligne la notification à l'utilisateur final.

Si l'exemple ci-dessus décrit le processus en général, il n'explique pas comment un système de gestion comme Jamf l'exploite pour gérer des appareils. Dans ce cas, l'équipe informatique se connecte à la console Jamf (Jamf Pro, Jamf School ou Jamf Now) et sélectionne les commandes qu'elle souhaite déployer auprès d'appareils explicitement ciblés. Dans un scénario de gestion, la commande ou le profil de configuration envoyé par Jamf contient une charge utile, et c'est elle qui spécifie les commandes à traiter sur les appareils ciblés. La notification est envoyée à APNs, puis acheminée vers les appareils concernés. Une fois parvenues aux appareils cibles, les commandes sont traitées par le système d'exploitation et exécutées, comme prévu.



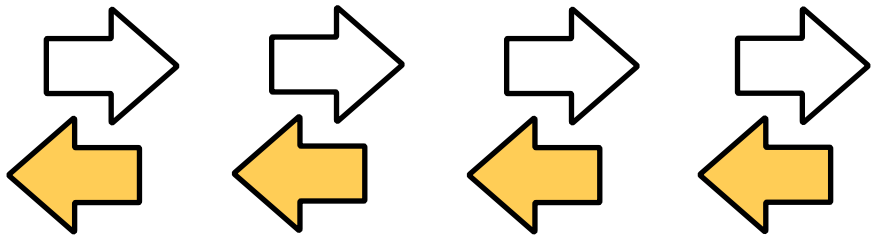
Préserver le flux d'APNs

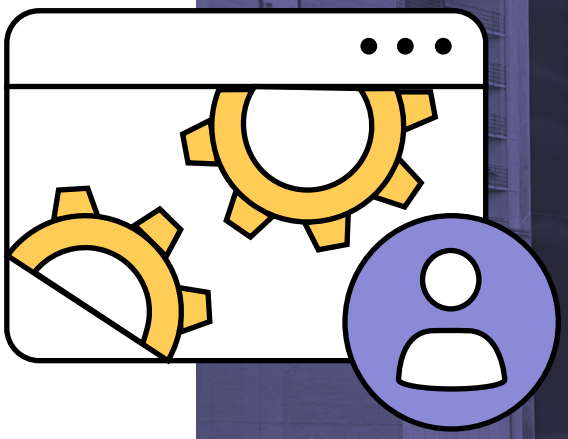
Maintenant que nous comprenons mieux le fonctionnement d'APNs et son importance, il s'agit maintenant de veiller au bon fonctionnement du service. L'objectif : minimiser les problèmes et en particulier les interruptions des services de gestion.

Première chose : il faut un identifiant Apple (Apple ID) lors de la **création d'un certificat push**, nécessaire pour établir le service de vos fournisseurs dans le cloud APNs d'Apple. Vous devez en effet générer un certificat qui sera lié à l'utilisation d'APNs par votre organisation. Que l'organisation héberge sa propre application ou son propre service, ou bien qu'elle utilise ceux d'une autre entreprise, chacune doit avoir son propre certificat push enregistré auprès d'APNs.

Ce compte doit rester privé : sécurisez-le à l'aide d'un mot de passe fort. En effet, il faut absolument éviter que ce compte soit compromis ou que les certificats générés soient modifiés de quelque manière que ce soit. Cela pourrait provoquer une perte de fonctionnalité des applications et des services reposant sur APNs – et cela englobe les appareils gérés par la MDM. Une autre mesure de sécurité consiste à activer l'authentification à deux facteurs (2FA) : vous réduirez ainsi davantage le risque que l'Apple ID ne tombe entre les mains d'utilisateurs non autorisés.

Le trafic qui entre et sort du réseau joue un rôle clé dans le maintien du flux. La circulation est souvent régulée – parfois même fortement – par des dispositifs de pare-feu qui filtrent tout trafic indésirable afin de protéger le réseau et ses utilisateurs. Et il se trouve qu'APNs s'appuie sur les ports du réseau pour acheminer correctement les données de notification. La majeure partie de ce trafic est dirigée vers le port TCP 5223 (avec des fonctions de basculement vers le port TCP 443, si nécessaire). Toutefois, Apple utilise également les ports TCP 2195-2197. Vérifiez auprès de votre administrateur de sécurité que **ces ports sont ouverts** : cela facilitera considérablement le trafic et réduira les erreurs de communication et les pertes de services.





Conseil de pro : renouvelez sans attendre les certificats utilisés par APNs. On ne soulignera jamais assez à quel point il est impératif de veiller au bon fonctionnement des notifications. Avec des certificats toujours à jour, APNs ne perdra jamais sa connexion avec le serveur MDM ou les terminaux, et vous conserverez la possibilité de gérer les appareils.

Mais que se passe-t-il en cas de perte de connectivité avec APNs ?

Dans ce cas, les terminaux conservent l'ensemble des réglages et des applications déployés avant la coupure de la connexion. Par contre, il devient impossible de les gérer. Aucune commande de gestion, aucun onboarding ni aucun approvisionnement d'appareil existant n'est réalisable. En bref, aucun changement ne peut plus être poussé du fournisseur de MDM vers les terminaux. La connexion bidirectionnelle entre le fournisseur MDM et le terminal est perdue : il faut donc créer un nouveau certificat APNs pour sécuriser à nouveau les connexions. L'introduction du nouveau certificat oblige à enrôler de nouveau tous les appareils manuellement auprès du fournisseur MDM. Et les appareils sous iOS devront même être effacés.

Apple et Jamf savent parfaitement rappeler au service informatique les dates limites de renouvellement, par e-mail et via la console Jamf. Il devrait donc avoir assez de temps pour éviter une expiration inopinée. Jamf Pro accompagne d'ailleurs l'équipe tout au long du processus, y compris dans les démarches qui se déroulent dans le portail d'Apple. La solution effectue un contrôle de hash pour s'assurer que le certificat renouvelé repose bien sur le compte utilisé lors de sa création, préservant ainsi la confiance établie entre la MDM et APNs. Grâce à cette mesure de sécurité intégrée, Jamf Pro vérifie également qu'APNs est lié au bon compte et qu'il n'a pas été détourné.

Enfin, toujours dans le portail Apple, l'équipe informatique peut révoquer les certificats inutilisés ou expirés. Pour cela, il lui suffit de localiser l'enregistrement en question, de cliquer sur le bouton de révocation correspondant et de confirmer le changement. C'est une étape essentielle si elle doit changer de certificat ou en implémenter de nouveaux. Une fois révoqués, les certificats obsolètes ne peuvent pas être réutilisés ou, pire, envoyés vers un autre système pour compromettre les appareils avec lesquels ils sont encore compatibles.

Mettez les workflows APNs à l'épreuve avec Jamf aujourd'hui.

Quel que soit votre environnement, Jamf propose une solution de gestion des appareils mobiles adaptée à vos besoins. Découvrez la **gestion des appareils mobiles**. Quand vous serez prêt, lancez-vous avec un essai gratuit.

Commencer

Ou contactez votre revendeur habituel de matériel Apple.