

Gestion moderne :

3 bonnes raisons d'adopter la gestion déclarative des appareils dès aujourd'hui

Selon Apple, la [gestion déclarative des appareils](#) (DDM) est l'avenir de la gestion des appareils. Certes, la DDM n'en est qu'à ses débuts. Mais en investissant dès aujourd'hui dans ce domaine, vous préparez votre organisation à affronter l'avenir.

Qu'est-ce que la gestion déclarative des appareils (DDM) ?

La DDM repose sur la proaction et l'autonomie des appareils. Un appareil autonome utilise des instructions prédéterminées et applique une logique de gestion programmée pour agir sans avoir à contacter un serveur pour recevoir des instructions.

En quoi la gestion des appareils mobiles avec DDM est-elle différente de l'approche traditionnelle de la MDM ?

On peut le dire, la DDM transforme radicalement le fonctionnement de la MDM.

Comment ça marche ? Pourquoi est-elle aussi puissante ?

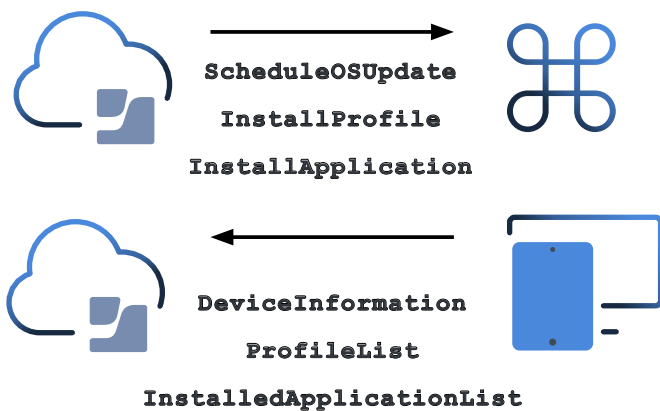
Et que pouvez-vous faire dès aujourd'hui avec la DDM ?

MDM traditionnelle

Dans le cas de la MDM seule, le serveur de gestion demande à Apple de prévenir l'appareil qu'il doit contacter le serveur pour obtenir des instructions. L'appareil reçoit un ping, demande des instructions au serveur, puis les exécute.

Pour savoir si et quand les instructions ont été suivies, le serveur demande à Apple d'envoyer une nouvelle requête à l'appareil. L'appareil répond par un rapport. Sur la base de ce rapport, le serveur peut poser de nouvelles questions ou exiger d'autres actions.

Tout cela crée un intense trafic sur le réseau et peut prendre un temps considérable.



MDM bénéficiant de la technologie DDM

La DDM établit une communication directe entre le serveur et les appareils et permet à chaque terminal de prendre des décisions de façon autonome.

L'administrateur MDM envoie aux appareils des instructions persistantes formulées selon une logique « si ceci, alors cela ». Si la condition énoncée se présente, l'appareil exécute l'action prescrite en toute autonomie et informe directement le serveur de l'événement et de sa réponse.



Un outil ultra-puissant pour les administrateurs Apple

La DDM permet aux administrateurs d'Apple de donner des instructions aux appareils et de façonner leur comportement :

- Signalement des principales valeurs d'inventaire au serveur de gestion
- Mises à jour régulières et feedback natif aux utilisateurs finaux
- Anticipation et activation de la gestion sur les nouveaux appareils susceptibles d'être jumelés à des appareils existants
- Réaction proactive aux logiciels malveillants et autres attaques



Pourquoi la DDM est-elle un fondement de la gestion moderne ?

Aujourd'hui, le lieu de travail dépasse largement le cadre des bureaux de l'entreprise, et il s'étend de plus en plus. Il ne suffit plus de réagir de plus en plus rapidement aux incidents pour préserver la sécurité des données et des réseaux : pour être à la hauteur, la cybersécurité exige de la proaction et de la vigilance. Les ordinateurs et les appareils mobiles remplissent des fonctions professionnelles de plus en plus nuancées et importantes.

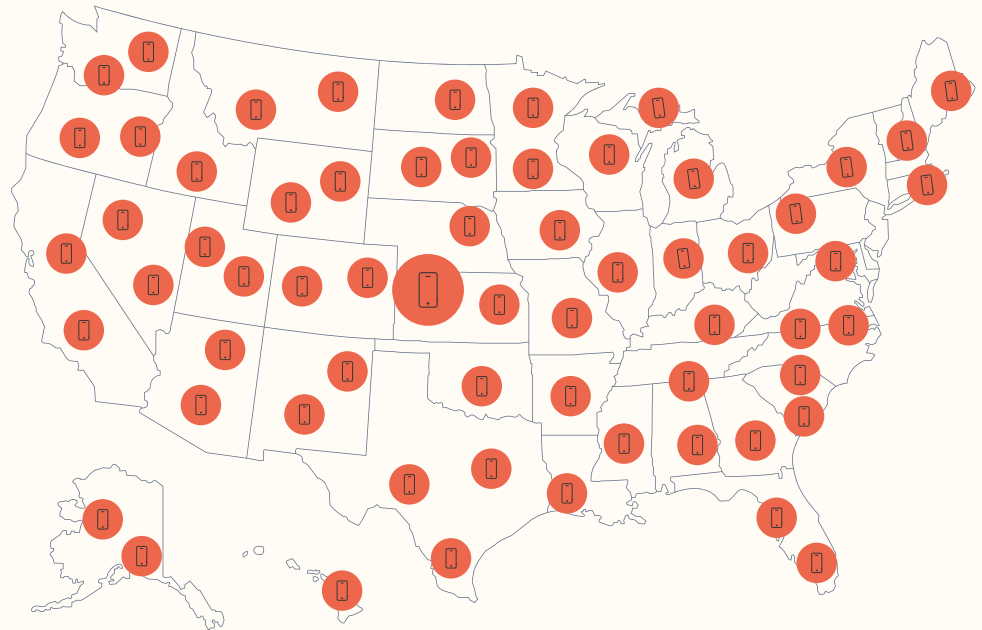
La gestion déclarative des appareils, qui donne de l'autonomie aux appareils, est absolument vitale pour toute organisation qui tient à faire face aux évolutions du marché, aux réalités des équipes et aux attentes de ses employés et ses clients.

C'est l'avenir de la gestion. Si elles ne s'y préparent pas dès maintenant, les organisations devront l'adopter dans la précipitation, ce qui les empêchera d'accomplir sereinement leurs activités essentielles de recherche de prospects et de relations client.

Apple va progressivement déployer de nouvelles fonctionnalités DDM qui vont avoir un véritable pouvoir de transformation.

Mais la DDM n'est pas seulement une technologie pour demain. Vous pouvez dès maintenant profiter de trois avantages de poids en optant pour la DDM.

1.



Inventaire réactif

Avec la DDM, les administrateurs peuvent créer une déclaration qui ordonne à l'appareil géré d'avertir spontanément le serveur de gestion lorsque des valeurs clés (la version de l'OS, par exemple) changent. Ils bénéficient ainsi d'un inventaire réactif qui garantit la conformité de manière proactive. **Prenons un exemple dans Jamf.**

Jamf compte parmi ses clients une grande entreprise américaine de services d'infrastructure.

Elle emploie des centaines de techniciens de terrain, tous équipés d'iPhone. Son service informatique soutient des équipes très vastes et dispersées.

En raison des exigences réglementaires propres à son secteur, ce client est très attentif à la conformité et surveille étroitement les **mises à jour de sécurité de l'OS.**

Mises à jour de sécurité de l'OS

En raison de ce souci de conformité, l'entreprise tient à appliquer les mises à jour logicielles dans des délais stricts. En effet, ces mises à jour apportent souvent des correctifs de sécurité essentiels.

Complications

C'est là que les choses se compliquent un peu.

L'entreprise utilise des applications personnalisées qui ne sont pas toujours immédiatement compatibles avec les dernières mises à jour de l'OS. Certains de ses utilisateurs finaux ont même pris l'habitude d'éviter les mises à jour pour éviter tout problème avec ces applications critiques dont ils ont besoin au quotidien.

Lutter contre les mauvaises habitudes

Pour lutter contre cette habitude et tenir les appareils à jour, le service informatique a créé un workflow très astucieux. Si un appareil n'est pas mis à jour dans le délai requis, le serveur :

- Ajoute l'appareil à une liste d'appareils exclus des applications gérées et exécute la commande correspondante.
- Envoie un message de fond d'écran pour demander la mise à jour
- Transmet les coordonnées du service informatique

Et en effet, c'est une approche très judicieuse. Avec ce workflow, les données de l'organisation étaient protégées, les normes de sécurité étaient respectées, et le service avait communiqué efficacement avec l'utilisateur final. Parfait !

Sauf que ça ne fonctionnait pas. Pourquoi ?

Les utilisateurs finaux téléchargeaient bien la mise à jour demandée. Mais ils n'avaient pas immédiatement accès aux applications indispensables à leur mission.

Rappelez-vous : avec l'ancien système MDM, on recommandait d'envoyer des rapports d'inventaire une fois par jour. Toutes les 24 heures, le serveur MDM contactait Apple et demandait à ce que l'iPhone réponde à une requête d'inventaire. Ce n'est qu'après qu'il rétablissait l'accès.

À moins que, par miracle, l'utilisateur ne fasse la mise à jour juste avant le rapport d'inventaire quotidien, il devait appeler l'équipe informatique pour qu'elle intervienne manuellement. Ces tâches manuelles lui prenaient beaucoup de temps

L'équipe informatique pourrait utiliser des API et des intégrations de la Marketplace de Jamf pour mettre en place un moyen de mettre à jour l'inventaire. Mais imaginez que l'appareil puisse spontanément informer le serveur de gestion que l'OS a été mis à jour.

La vraie solution : les rapports d'état.

Le client de Jamf a mis en œuvre la DDM et utilisé les rapports d'état. Une déclaration demande à l'appareil géré d'avertir spontanément le serveur de gestion en cas de changement dans des valeurs clés, comme la version de l'OS.

Désormais, une fois que les utilisateurs finaux ont fait la mise à jour conformément aux instructions, il ne faut que quelques secondes pour qu'ils puissent à nouveau utiliser toutes les fonctionnalités de leur iPhone.

En coulisses, pendant le redémarrage, l'iPhone a informé de lui-même le serveur de gestion qu'il était équipé de la nouvelle version du système d'exploitation et donc à nouveau conforme. Le serveur de gestion l'a retiré de la liste des appareils exclus des applications gérées, sans aucune intervention de l'équipe informatique.





2.

Mises à jour logicielles

L'application des mises à jour logicielles est un défi de longue date pour les nombreux administrateurs qui utilisent une technologie MDM traditionnelle.

Le problème des mises à jour logicielles

Pendant un certain temps, les workflows scriptés étaient un bon moyen d'appliquer les mises à jour logicielles. Mais Apple exige de plus en plus souvent des droits d'administrateur ou des commandes MDM pour intervenir sur les Mac, et les scripts perdent en efficacité.

N'oublions pas non plus que le service informatique peut faire perdre des heures de travail à un utilisateur s'il demande une mise à jour alors qu'il est plongé dans une tâche critique. C'est pourquoi les commandes MDM sont considérées comme le dernier recours pour imposer les mises à jour critiques.

La solution : la DDM

Heureusement, la gestion déclarative peut simplifier ce processus.

Souvenez-vous : la gestion déclarative permet de créer des instructions complexes qui façonnent le comportement d'un appareil. Celui-ci applique ensuite une logique interne pour respecter spontanément ces instructions.

Imaginons que les appareils d'une organisation doivent recevoir un correctif d'application indispensable à un moment précis. Avec une mise à jour pilotée par DDM, ils appliqueront

la mise à jour immédiatement sans qu'il faille communiquer avec les utilisateurs finaux. Personne ne perd son temps, et l'équipe informatique n'a pas besoin de courir après les retardataires.

Comment ça marche ?

La mise à jour est invoquée par une déclaration, ce qui permet au service informatique de préciser la date et l'heure d'installation de la version de l'application. Avant cette date, conformément à la logique fournie par le serveur, l'appareil communique de plus en plus fréquemment avec l'utilisateur final. Il l'avertit de l'événement à venir et lui donne la possibilité de réaliser lui-même la mise à jour sans attendre si cela l'arrange.

L'heure et la date d'exécution sont définies selon le fuseau horaire du client. Même si les utilisateurs sont répartis dans le monde entier ou en déplacement, la mise à jour se fera dans une plage pratique, en dehors des heures de travail.

Si un appareil est éteint pendant la plage prévue pour la mise à jour, celle-ci aura lieu au moment du redémarrage.

Les appareils informeront automatiquement le serveur de gestion de la nouvelle version de l'application. L'équipe informatique obtient ainsi une vue extrêmement précise de son parc géré lorsqu'il faut installer des mises à jour critiques pour éliminer des risques de sécurité.



3.

Gestion des Apple Watch

Apple a introduit de nouvelles options de gestion des appareils dans le cadre du développement de la DDM, et la gestion de l'Apple Watch est sans doute la plus prometteuse.

L'Apple Watch en entreprise ? Absolument.

Les Apple Watches sont des appareils puissants et portables. Elles soutiennent les workflows de communication, de sécurité et d'identification bien mieux que beaucoup d'autres options.

Quand elles sont gérées, le service informatique peut effacer à distance les montres perdues ou volées afin de protéger les données et les accès qu'elles contiennent. Par ailleurs, Apple prend désormais en charge la désactivation du verrouillage d'activation dans Apple Business Manager ou Apple School Manager pour les appareils d'entreprise. Les organisations peuvent ainsi profiter des avantages de la fonction Find My sans craindre qu'un appareil soit inutilisable parce que verrouillé.

Comment les entreprises utilisent-elles l'Apple Watch ?

Grâce au développement continu de la DDM, les clients de Jamf font de nombreux usages professionnels de l'Apple Watch:

- Les employés qui travaillent avec des équipements lourds ou effectuent des travaux manuels peuvent garder les mains libres et recevoir des informations sur leur Apple Watch sans se mettre en danger
- Les professionnels de santé peuvent recevoir des notifications et des alertes concernant les rendez-vous à venir ou les urgences des patients

- Des employés de secteurs variés utilisent l'Apple Watch comme badge électronique pour entrer dans des zones sécurisées

Ce qui est passionnant, c'est que ces exemples évidents ne sont qu'un début. Les clients de Jamf font preuve d'une grande créativité avec les appareils gérés, et ils nous présentent régulièrement de nouveaux cas d'utilisation. Cette liste devrait s'allonger dans les mois à venir.

Comment le service informatique gère-t-il l'Apple Watch ?

Gérer une Apple Watch, c'est en fait gérer un iPhone connecté.

Dans [Jamf Pro](#), les administrateurs utilisent les groupes d'appareils intelligents pour activer l'inscription des Apple Watches jumelées à des iPhone d'entreprise supervisés, fonctionnant sous iOS 17. Cela permet également d'obtenir une déclaration désignant comme gérée toute Apple Watch exécutant watchOS 10 ou plus et jumelée à l'un de ces appareils.

Une fois jumelées, ces Apple Watches sont supervisées et héritent automatiquement des réglages de l'iPhone : code secret obligatoire, paramètres Wi-Fi, charges utiles de certificats, etc. L'iPhone et son Apple Watch doivent être considérés comme un duo indissociable du point de vue l'inventaire, des groupes et des rapports.

L'Apple Watch offre de plus en plus d'avantages dans le monde professionnel. Chez Jamf, nous sommes impatients de voir comment nos clients vont les utiliser avec l'appui de la DDM et la puissance des services d'Apple.

Quel est le rôle de Jamf ?

Jamf Pro [active automatiquement les capacités de gestion déclarative](#) pour les appareils gérés compatibles. Et comme nous prenons en charge toutes les mises à jour d'Apple le jour de leur sortie, nous sommes toujours à la pointe de la technologie DDM.



Prenez une longueur d'avance avec la DDM

En **activant la DDM sur vos appareils Apple**, vous investissez dans l'avenir. Mais vous pouvez aller encore plus loin en exploitant dès aujourd'hui toutes ses fonctionnalités.

Vous vous demandez comment mettre en œuvre un **inventaire réactif**, améliorer les **workflows de mise à jour logicielle** ou **gérer les Apple Watches ?**

[Jamf est là pour vous aider.](#)