kyndryl

Kyndryl Multicloud Management Platform : Console d'opérations

Surveillance intelligente et gestion préventive de l'informatique hybride

Sommaire

2 Récapitulatif

3 Capacités

4 Cas pratiques

5 Pourquoi Kyndryl ?

Résumé

Alors que de plus en plus d'entreprises migrent leurs charges de travail vers des environnements informatiques hybrides, le besoin d'un accès simplifié à leurs services, avec un contrôle et une visibilité accrus de l'informatique, n'a jamais été aussi fort. Les équipes en charge des opérations informatiques doivent gérer des environnements hybrides et complexes à l'aide de multiples outils, systèmes, fournisseurs et processus. Une visibilité complète, précise et opportune sur l'ensemble de l'environnement informatique est nécessaire pour gérer la complexité, atténuer le risque d'informatique fantôme et éviter la dépendance envers un fournisseur.

Une plateforme de gestion informatique moderne, en libre-service et intelligente qui évolue avec votre entreprise.
La Multicloud Management Platform (MCMP) de Kyndryl™ est conçue pour simplifier la gestion de l'informatique hybride. MCMP propose à vos utilisateurs une expérience ouverte, en libre-service et hautement sécurisée. La plateforme s'appuie sur quatre consoles en libre-service, basées sur des "persona", pour que vos équipes d'exploitation puissent consommer, déployer, optimiser et gouverner leurs services numériques, à travers les clouds, les conteneurs et les datacenters avec un accès simplifié. Avec une visibilité approfondie

79 % des chefs d'entreprise et des responsables technologiques pensent que la visibilité sur les environnements traditionnels et cloud est une capacité importante pour un fournisseur de gestion de cloud[1]

de l'infrastructure et de la consommation cloud, les responsables IT peuvent améliorer l'efficacité et freiner l'informatique fantôme.

Prenez le contrôle de votre univers d'opérations informatiques
La console d'opérations MCMP de Kyndryl permet à votre équipe d'accéder à l'ensemble de votre périmètre numérique à partir d'une seule application. Cette plateforme d'exploitation en libre-service facilite une gouvernance efficace de la consommation cloud et un alignement plus étroit avec les priorités de votre métier, tout en renforçant l'efficacité opérationnelle.

La console d'opérations MCMP de Kyndryl utilise une interface unique pour fournir une visibilité indispensable sur les centres de données, les opérations multicloud et de conteneurs, en augmentant l'intelligence humaine par la découverte et la corrélation automatiques des évènements, et en recommandant

- Optimiser l'infrastructure informatique pour plus de flexibilité et d'évolutivité
- Obtenir une visibilité de bout en bout sur les environnements informatiques hybrides
- Affiner les processus par un contrôle intelligent
- Simplifier la gestion d'informatique hybride
- Réduire les coûts d'exploitation.

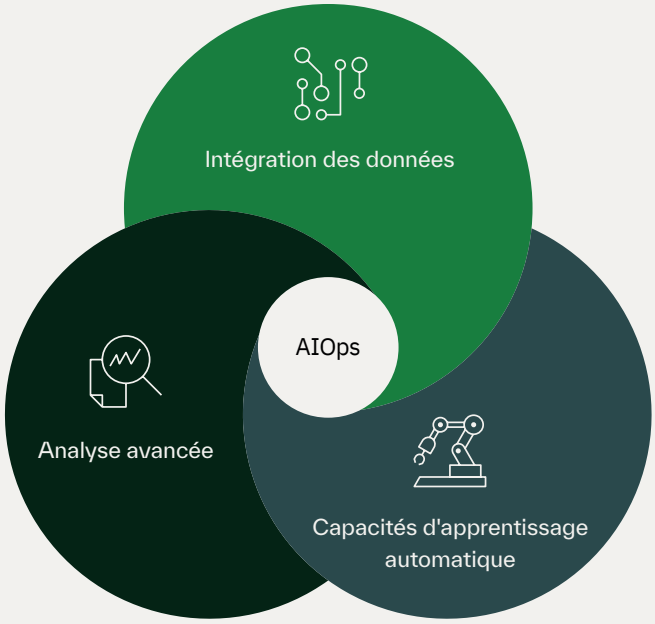
des actions correctives Au fil du temps, ces capacités d'apprentissage automatique créent des modèles d'intelligence artificielle qui aident les équipes opérationnelles à comprendre où les problèmes se développent, ce qui permet une résolution proactive.

Principaux avantages :

Fonctionalités

Au centre de l'Operations console MCMP de Kyndryl se trouve une nouvelle centrale d'applications d'IA - l'IA pour les opérations informatiques (AIOps). Grâce à l'intégration des données, aux analyses avancées et à l'apprentissage automatique, l'AIOps peut remplacer plusieurs outils manuels par une seule plateforme automatisée d'opérations informatiques. L'AIOps analyse les données, identifie les corrélations, les modèles et les tendances, ainsi que les risques potentiels, et affiche les résultats à côté des données brutes dans une interface unique.

Cette nouvelle approche de la gestion de l'informatique hybride est renforcée par l'agrégation de données, l'automatisation, les analyses avancées et l'IA. Grâce à un accès basé sur l'IA, les organisations ont une visibilité totale sur leurs environnements hybrides, ce qui permet au personnel informatique d'identifier et de résoudre les problèmes de manière proactive et plus rapidement.



L'AIOps peut remplacer de multiples outils manuels par une interface unique sur une plateforme automatisée d'opérations informatiques, pour une meilleure visibilité dans toute l'entreprise.

Cas d'usage

1

La visibilité permet des opérations informatiques proactives

Problème : les opérations informatiques ne sont pas assez réactives en cas d'interruption des accords de niveau de service et de violation de la sécurité. Elles sont incapables de passer d'un mode réactif à un mode proactif en raison du manque de données agrégées et corrélées permettant de tirer des enseignements exploitables.

Solution : l'ajout de l'IA dans le mix opérationnel informatique permet d'agréger et de corréler les informations nécessaires, et d'afficher l'état de santé de l'ensemble du patrimoine informatique hybride par le biais d'un seul et même écran : l'operations console Kyndryl, dotée de l'AIOps.

Avantage commercial : Les équipes d'exploitation peuvent corréler les incidents et les connecter aux impacts sur les services. Les problèmes hautement prioritaires sont immédiatement évidents et traçables. La vue des actifs du domaine est agrégée dans un seul système de référence.

2

La transparence est primordiale pour le succès commercial

Problème : l'informatique a toujours été considérée comme une entité vaste, complexe et opaque. À l'ère du nuage, lorsque les utilisateurs contrôlent leurs propres systèmes, que les coûts sont disponibles en ligne et que vous pouvez surveiller tout ce que vous voulez, l'opacité informatique n'est plus acceptable.

Solution : la société a besoin d'une solution multidimensionnelle pour gérer le nuage avec les bons niveaux de contrôle, le composant stratégique clé étant la transparence - AIOps. En s'appuyant sur la visibilité agrégée, l'informatique est en mesure d'exposer la santé et le bien-être de l'ensemble du patrimoine informatique hybride.

Avantage commercial : les parties prenantes comprennent la santé des systèmes clés qui font fonctionner l'entreprise. Elles sont capables de savoir quand quelque chose est défaillant et quand c'est réparé. Moins de tickets, de demandes de renseignements et de fausses alarmes sont générés de façon redondante, ce qui réduit le bruit. Et l'informatique est considérée comme un partenaire de confiance de l'entreprise.

3

L'ingénieur chargé de la fiabilité des sites s'appuie sur un continuum d'observabilité.

Problème : De nombreuses organisations adoptent le modèle d'exploitation informatique DevOps en utilisant une approche agile du développement avec des outils et des pratiques permettant une intégration et une livraison continues. Les équipes chargées des applications veulent maintenant suivre leur exemple.

Solution : AIOps assiste l'ingénieur chargé de la fiabilité du site (SRE) dans l'identification et la résolution des problèmes pour soutenir les équipes d'application. AIOps permet d'identifier rapidement les composants d'infrastructure défaillants ou d'éliminer l'infrastructure comme cause d'un problème.

Avantage commercial : Les tendances et les informations contenues dans AIOps aident les utilisateurs à savoir où concentrer leurs efforts. De plus, le tableau de bord de santé AIOps fait office de fiche de score pour que les entreprises sachent que leur participation dans le SRE est rentable grâce à des systèmes plus fiables et plus sûrs.

Pourquoi Kyndryl ?

Kyndryl possède une expertise approfondie dans la conception, l'exploitation et la gestion des infrastructures technologiques les plus modernes, efficaces et fiables dont le monde dépend chaque jour. Nous sommes profondément engagés à faire progresser l'infrastructure vitale qui alimente le progrès humain. Kyndryl compte 90 000 employés hautement qualifiés dans le monde entier, au service de 75 des 100 premières entreprises du classement Fortune.

Pour en savoir plus sur la manière dont l'Operations console de plateforme de gestion multicloud de Kyndryl peut apporter visibilité, gouvernance et automatisation à votre environnement informatique hybride de bout en bout, contactez votre représentant Kyndryl ou visitez le site Internet à l'adresse ibm.com/kyndryl

En savoir plus →

kyndryl

© Copyright IBM Corporation 2021

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes
Cedex

Produit aux États-Unis d'Amérique en juillet 2021

IBM, le logo IBM, ibm.com, Kyndryl, le logo Kyndryl, kyndryl.com, et IBM Cloud sont des marques d'International Business Machines Corp., déposées dans de nombreuses juridictions mondiales. Les autres noms de services et de produits peuvent être des marques d'IBM ou d'autres sociétés. Une liste actualisée de toutes les marques IBM est disponible sur la page Web « Copyright and trademark information » à l'adresse suivante : ibm.com/legal/copytrade.shtml.

Le présent document contient des informations qui étaient en vigueur et valides à la date de la première publication, et qu'IBM peut mettre à jour à tout moment. Les offres mentionnées dans le présent document ne sont pas toutes disponibles dans tous les pays où IBM est présent.

LES INFORMATIONS CONTENUES DANS LE PRÉSENT DOCUMENT SONT FOURNIES "EN L'ÉTAT", SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DÉCLINE NOTAMMENT TOUTE RESPONSABILITÉ RELATIVE À CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DÉFAUT D'APTITUDE À L'EXÉCUTION D'UN TRAVAIL DONNÉ. Les produits IBM sont garantis conformément aux dispositions des contrats.

Il incombe au client de s'assurer de la conformité avec la législation et les réglementations applicables. IBM ne donne aucun avis juridique et ne garantit pas que ses services ou produits sont conformes aux lois applicables.

Déclaration de pratiques de sécurité recommandées : La sécurité des systèmes informatiques inclut la protection des systèmes et de l'information par la prévention, la détection et la réponse aux accès inopportuns provenant de l'intérieur comme de l'extérieur de l'entreprise. Un accès non autorisé peut entraîner la modification, la destruction, le détournement ou l'utilisation impropre des informations, ou une détérioration ou une utilisation impropre de vos systèmes, notamment en vue de les utiliser pour attaquer autrui. Aucun système ou produit informatique ne doit être considéré comme étant complètement sécurisé et aucun produit, service ou mesure de sécurité ne peut être entièrement efficace contre une utilisation ou un accès non autorisé. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produits ou services pour optimiser leur efficacité. IBM NE GARANTIT PAS QUE TOUS LES SYSTÈMES, PRODUITS OU SERVICES SONT À L'ABRI DES CONDUITES MALVEILLANTES OU ILLICITES DE TIERS OU QU'ILS PROTÉGERONT VOTRE ENTREPRISE CONTRE CELLES-CI.

Citations

1 « Assembling your cloud orchestra, A field guide to multicloud management. » IBM Institute for Business Value, octobre 2018. ibm.com/thought-leadership/institute-business-value/report/multicloud